CAPITOL
Technology University

Bradford L. Sims, PhD
President

July 11, 2019

Dr. James D. Fielder, Jr.
Secretary of Maryland Higher Education
Maryland Higher Education Commission
6 N. Liberty Street
Baltimore, MD 21201

Dear Dr. Fielder,

Capitol Technology University is requesting approval to offer a **Master of Science (M.S.) in Construction Cybersecurity**. The degree curriculum will be taught using a significant number of existing faculty at our university and will be supported by the development of new courses for the **M.S. in Construction Cybersecurity**. The mission of Capitol Technology University is to provide a practical education in engineering, computer science, information technology, and business that prepares individuals for professional careers and affords the opportunity to thrive in a dynamic world. A central focus of the university's mission is to advance practical working knowledge in areas of interest to students and prospective employers within the context of Capitol Tech's degree programs. The university believes that a **M.S. in Construction Cybersecurity** is consistent with this mission.

There is a growing requirement within the construction industry for highly trained construction cybersecurity professionals. This program is in response to that need. The **M.S. in Construction Cybersecurity** degree is primarily for experienced construction personnel who desire to advance in their careers by earning a master's degree, but is also designed to accommodate those desiring to enter the field.

To respond to needs of the construction industry, we respectfully submit for approval a Master of Science (M.S.) in Construction Cybersecurity. The required proposal is attached as well as the letter from me as university president confirming the adequacy of the university's library to serve the needs of the students in this degree.

Respectfully,

Bradford L. Sims, PhD

CAPITOL
Technology University

Bradford L. Sims, PhD
President

July 11, 2019

Dr. James D. Fielder, Jr.
Secretary of Maryland Higher Education
Maryland Higher Education Commission
6 N. Liberty Street
Baltimore, MD 21201

Dear Dr. Fielder,

This letter is in response to the need for confirmation of the adequacy of the library of Capitol Technology University to support the proposed **Master of Science (M.S.) in Construction Cybersecurity**. As president of the university, I confirm that the library resources, including support staff, are more than adequate to support the **M.S. in Construction Cybersecurity** In addition, the university is dedicated to, and has budgeted for, continuous improvement of its library resources.

Respectfully,

Bradford L. Sims, PhD

Office Use Only: PP#

MHEC
Creating a state of achievement

Cover Sheet for In-State Institutions
New Program or Substantial Modification to Existing Program

Institution Submitting Proposal	Capitol Technology University

Each action below requires a separate proposal and cover sheet.

- (●) New Academic Program New
- ( ) Area of Concentration New
- ( ) Degree Level Approval New
- ( ) Stand-Alone Certificate
- ( ) Off Campus Program
- ( ) Substantial Change to a Degree Program
- ( ) Substantial Change to an Area of Concentration
- ( ) Substantial Change to a Certificate Program
- ( ) Cooperative Degree Program
- ( ) Offer Program at Regional Higher Education Center

Department Proposing Program	Department of Business and Information Sciences	
Degree Level and Degree Type	Master of Science (M.S.)	
Title of Proposed Program	M.S. in Construction Cybersecurity	
Total Number of Credits	36	
Suggested Codes	HEGIS: 799	CIP: 11
Program Modality	( ) On-campus (●) Distance Education (*fully online*) ( ) Both	
Program Resources	(●) Using Existing Resources ( ) Requiring New Resources	
Projected Implementation Date	(●) Fall ( ) Spring ( ) Summer	Year: 2019
Provide Link to Most Recent Academic Catalog	URL: https://www.captechu.edu/current-students/academic-resources	
Preferred Contact for this Proposal	Name: Professor Soren Ashmall	
	Title: Director, Assessment & Accreditation	
	Phone: (571) 332-4344	
	Email: spashmall@captechu.edu	
President/Chief Executive	Type Name: Dr. Bradford Sims	
	Signature: [signature]	Date: 7-11-19
Approval/Endorsement by Governing Board	Type Name: Dr. Bradford Sims	
	Signature: [signature]	Date: July 11, 2019

Revised 5/15/18

PROPOSAL FOR:

__X__NEW INSTRUCTIONAL PROGRAM

_____ SUBSTANTIAL EXPANSION/MAJOR MODIFICATION

_____ COOPERATIVE DEGREE PROGRAM

__X__WITHIN EXISTING RESOURCES or____REQUIRING NEW RESOURCES

CAPITOL Technology University

Institution Submitting Proposal

Fall 2019
Projected Implementation Date

Master of Science
Award to be Offered

Master of Science in Construction Cybersecurity
Title of Proposed Program

0799.00
Suggested HEGIS Code

11.1003
Suggested CIP Code

Cybersecurity
Department of Proposed Program

Professor William Butler
Name of Department Head

Prof. Soren Ashmall	**spashmall@captechu.edu**	**571-332-4344**
Director, Assessment and Accreditation	Contact E-Mail Address	Phone Number

7-11-19
Signature and Date

President/Chief Executive Approval

July 11, 2019
Signature and Date

Date Endorsed/Approved by Governing Board

Proposed Technical Master of Science in Construction Cybersecurity
Department of Cybersecurity
Capitol Technology University
Laurel, Maryland

A. Centrality to Institutional Mission Statement and Planning Priorities:

1. Program description and relationship to university mission and how it relates to the institution's approved mission.

Master of Science in Construction Cybersecurity Program Description:

The **Master of Science (M.S.) in Construction Cybersecurity** degree program is designed to meet the growing needs of today's business and government where construction cybersecurity is now a major consideration. The **M.S. in Construction Cybersecurity** provides advanced graduate-level management education where the latest construction cybersecurity concepts are reviewed and analyzed with a laser focus. Throughout the program, the latest technological developments, applications, and considerations in the construction industry are explored and applied to real-life industry challenges. Students will learn optimum methods and techniques in construction cybersecurity and how to define related resources and associated risks at an executive level in order to maintain profitability, manage work effectivity and efficiently, and ensure customer satisfaction.

The **M.S. in Construction Cybersecurity** will prepare students for advanced cybersecurity skills and leadership positions throughout the construction industry. The student will learn to analyze patterns, employ powerful technological tools, and to drive business decisions in the construction cybersecurity field. The student will get hands-on use of the technology in construction and construction cybersecurity.

The **M.S. in Construction Cybersecurity** provides the student with the ability to integrate decision-making skills in the technologically complex construction cybersecurity environment. Capitol Technology University graduates will be able to apply their cutting-edge construction cybersecurity skills to every day work situations in the industry. Students will learn the latest technological developments, applications, and considerations in construction cybersecurity. The required core courses will build a foundation that encompasses technology and cybersecurity.

Relationship to Institutional Approved Mission:

The **M.S. in Construction Cybersecurity** is consistent with the University mission to educate individuals for professional opportunities in engineering, computer science, information technology, and business. The University provides relevant learning experiences that lead to success in the evolving global community. Fundamental to the degrees in the Department of Business and Information Sciences are opportunities to pursue cutting-edge knowledge combined with technological applications, techniques, and procedures. The **M.S. in Construction Cybersecurity** is consistent with that philosophy. This same philosophy is supported by the University's existing degree programs and learning opportunities. The University has the following undergraduate degrees: B.S. in Astronautical Engineering, B.S. in Business Analytics and Data Science, B.S. in Computer Engineering, B.S. in Computer Engineering Technology,

B.S. in Computer Science, B.S. in Construction Management and Critical Infrastructure, B.S. Construction Safety, B.S. in Cyber Analytics, B.S. in Cybersecurity, B.S. in Electrical Engineering, B.S. in Electrical Engineering Technology, B.S. in Engineering Technology, B.S. in Facilities Management and Critical Infrastructure, B.S in Management of Cyber and Information Technology, B.S. in Mechatronics Engineering, B.S. in Mechatronics and Robotics Engineering Technology, B.S. in Mobile Computing, B.S. in Software Engineering, and B.S. in Technology and Business Management, and B.S in Unmanned and Autonomous Systems. The University also has the following degrees at the graduate level: M.S. in Aviation, M.S. in Computer Science, M.S. in Critical Infrastructure, M.S. in Cyber Analytics, M.S. in Cybersecurity, M.S. in Engineering Technology, M.S. in Information Systems Management, M.S.in Internet Engineering, M.S. in Unmanned and Autonomous Systems Policy and Risk Management, M.B.A., T.M.B.A. Business Analytics and Data Science, T.M.B.A. in Cybersecurity, D.Sc. in Cybersecurity, Ph.D. in Aviation, Ph.D. in Business Analytics and Decision Sciences, Ph.D. in Construction Science, Ph.D. in Critical Infrastructure, Ph.D. in Manufacturing, Ph.D. in Occupational Health and Safety, Ph.D. in Technology, Ph.D. in Technology/M.S. in Research Methods Combination Program, and Ph.D. in Unmanned Systems Applications. The **M.S. in Construction Cybersecurity** degree fits within University's mission framework and is an integral part of the Strategic Plan for FY 2017-2021 and succeeding years. Funding to support the new degree has been included in the institutional and departmental budgets for FY 2019-2020 and forecasted budgets going forward.

The **M.S. in Construction Cybersecurity** degree will be offered online using the Canvas Learning Management System and Zoom. The result is the convenience required by the 21st Century learner and provides the interaction with faculty and fellow students that is critical to the high-level learning experience. The curriculum provides the graduate student the necessary learning tools that the University believes critical to success as a construction cybersecurity professional. The degree is also consistent with the interdisciplinary nature of the University. .

2. Explain how the proposed program supports the institution's strategic goals and provide evidence that affirms it is an institutional priority.

Capitol Technology University operates on four strategic goals:

1. **Expand Educational Offerings, Increase Program Completion:** *Capitol Technology University is an institution that offers career-relevant curricula with quality learning outcomes. The strategy includes continuing to expand educational offerings, increasing program completion, and raising learner qualifications and outcomes.*

2. **Increase Enrollment and Institutional Awareness:** *Capitol will accelerate its goal pursuit to become more globally renowned and locally active through student, faculty and staff activities. Enrollment will grow to 650 undergraduates, 350 masters' students and 250 doctoral candidates.*

3. **Improve the Utilization of University Resources and Institutional Effectiveness While Expanding Revenue**: *Capitol will likely continue to be 80% financially dependent on student tuition and fees. We plan to enhance our resources by expanding the range and amount of funding from other streams and aligning costs with strategic initiatives.*

4. **Increase the Number and Scope of Partnerships**: *Capitol's service to our constituents and sources of financial viability both depend upon participation with continuing and new partner corporations, agencies, and schools.*

The proposed **M.S. in Construction Cybersecurity** builds upon the existing areas of undergraduate degree programs: B.S. in Astronautical Engineering, B.S. in Business Analytics and Data Science, B.S. in Computer Engineering, B.S. in Computer Engineering Technology, B.S. in Computer Science, B.S. in Construction Management and Critical Infrastructure, B.S. in Construction Safety, B.S. in Cyber Analytics, B.S. in Cybersecurity, B.S. in Electrical Engineering, B.S. in Electrical Engineering Technology, B.S. in Engineering Technology, B.S. in Facilities Management and Critical Infrastructure, B.S in Management of Cyber and Information Technology, B.S. in Mechatronics Engineering, B.S. in Mechatronics and Robotics Engineering Technology, B.S. in Mobile Computing, B.S. in Software Engineering, and B.S. in Technology and Business Management, and B.S in Unmanned and Autonomous Systems. The University also provides the following opportunities at the graduate level for a student to continue his/her academic pursuits: M.S. in Aviation, M.S. in Computer Science, M.S. in Critical Infrastructure, M.S. in Cyber Analytics, M.S. in Cybersecurity, M.S. in Engineering Technology, M.S. in Information Systems Management, M.S.in Internet Engineering, M.S. in Unmanned and Autonomous Systems Policy and Risk Management, M.B.A., T.M.B.A. Business Analytics and Data Science, T.M.B.A. in Cybersecurity, D.Sc. in Cybersecurity, Ph.D. in Aviation, Ph.D. in Business Analytics and Decision Sciences, Ph.D. in Construction Science, Ph.D. in Critical Infrastructure, Ph.D. in Manufacturing, Ph.D. in Occupational Health and Safety, Ph.D. in Technology, Ph.D. in Technology/M.S. in Research Methods Combination Program, and Ph.D. in Unmanned Systems Applications. The University's undergraduate degree programs prepare students to begin their careers, or further their careers, fully employed with enhanced leadership skills and technical expertise that meet the needs information-dependent organizations using modern technology. The University's programs have been preparing professionals for rapid advances in information and technology, intense global competition, and increasingly complex technological environments for decades. The **M.S. in Construction Cybersecurity** will contribute to that legacy and will allow students to elevate their skills and careers to the next level as a commercial pilot.

The proposed **M.S. in Construction Cybersecurity** is fully supported by the University's Vision 2025 and Strategic Plan 2017-2025. Funding to support the degree has been included in forecasted budgets going forward.

The University also has active partnerships in the private and public arenas (e.g., Parsons Corporation, Leidos, Patton Electronics, Lockheed Martin, Northrup Grumman, Cyber Security Forum Initiative, IRS, NCS, NSA and DHS). The **M.S. in Construction Cybersecurity** degree will provide new opportunities for partnerships as well as expanded research. The increase in partnerships and placement of our graduates in our partner institutions will serve to expand the University's enrollment and reputation. While additional enrollment will increase financial resources, additional partnerships and grants in the construction cybersecurity field will help diversify and increase the University's financial resources.

3. **Provide a brief narrative of how the proposed program will be adequately funded for at least the first five years of program implementation. (Additional related information is required in section L.)**

   Capitol Technology University will support the proposed program through the same process and level of support as the University's existing programs. Many of the program's courses already exist within other programs in the university. The University has also budgeted funds to support program and course development, online support, office materials, travel, professional development, and initial marketing. There is no substantial impact to the institution due to the advanced budgeting of these funds. If approved, the program is expected to be self-sustaining going forward.

4. **Provide a description of the institution's commitment to:**

   a. **Ongoing administrative, financial, and technical support of the proposed program**

      The proposed degree is an integral part of the University's Strategic Plan for FY 2017-2025 and forward. Funding for the administrative, financial, and technical support of the new degree has been included in the institutional and departmental budgets for FY 2019-2020 as well as the forecasted budgets going forward.

   b. **Continuation of the program for a period of time sufficient to allow enrolled students to complete the program.**

      Capitol Technology University is fully committed to continuing the proposed **M.S. in Construction Cybersecurity** degree program for a sufficient period to allow enrolled students to complete the program.

B. Critical and Compelling Regional or Statewide Need as Identified in the State Plan:

1. **Demonstrate demand and need for the program in terms of meeting present and future needs of the region and the state in general based on one or more of the following:**

   a. **The need for advancement and evolution of knowledge.**

      Leaders in the construction industry are facing an ever-increasing need to expand the application of new technology to their industry in order to remain competitive, efficient, and viable now and in the future. Construction companies today depend and thrive on timely, accurate and relevant information. As technology enables the creation and capture of ever-increasing amounts of data, the effective management and understanding of resource needs is becoming an enormous challenge. Construction is no longer just the task of building buildings; it is far reaching implications in the global, environmental, integration, and security aspects of society. Effective leadership in this industry can only be achieved with a holistic approach and the advanced skills that will be covered in this proposed degree.

      According to the article "Data Breaches, Cyber Security and the Construction Industry"**:**

Is cyber security a major concern for your construction business? Maybe you don't think your company is a potential target for a cyberattack. You'd be right too if your company doesn't use computers to store any information about your business and if you never connect to the internet.

As the construction industry becomes more connected through internet-connected solutions and remotely accessible systems such as Building Information Modeling (BIM), telematics and project management software it creates more opportunities for hackers to launch a cyberattack.

Construction firms have access to a wealth of information that might be desirable to hackers. Intellectual property, proprietary assets, architectural drawings and specifications as well as corporate banking and financial accounts are all prime targets. Access to employee information such as full names, Social Security numbers and bank account data used for payroll are frequently targeted in spear phishing scams. Hackers often go after general contractors and subcontractors as a means to gain access to clients' networks.

Here are a few examples of how companies in the AEC industry have become victims of cybercrime:

Turner Construction was the victim of a spear phishing scam in March when an employee sent tax information on current and former employees to a fraudulent email account. Spear phishing is an email scam targeted at a specific individual, business or organization. Hackers spoof the "From:" field in an email to make it appear to come from a trustworthy source, say from your CEO or CFO. Typical spear phishing scams include messages requesting personal information on employees such as names and Social Security number, corporate banking account information, or login credentials.

In the case of Turner Construction, the information provided to the fraudulent email account included full names, Social Security numbers, states of employment and residence as well as tax withholding data for 2015. All employees who worked for the company in 2015 were affected by the data breach. Turner, which is headquartered in New York, is one of the largest construction management firms in the U.S. with offices in 24 states.

Baltimore-based Whiting-Turner Contracting, another of the nation's top construction management and general contracting companies, may have also been the victim of a data breach. In March, the company was notified by an outside vendor that prepared W-2 and 1095 tax forms for the company's employees about suspicious activity on that vendor's systems. Around the same time, employees of Whiting-Turner were reporting fraudulent tax filings being made in their names. In addition to employee information, it is also possible that personal information on children and beneficiaries of employees who received healthcare insurance coverage through Whiting-Turner was compromised. Whiting-Turner has 31 offices in 18 states and Washington, D.C.

The construction industry is clearly not immune to cyberattacks. Central Concrete Supply Company out of California, Century Fence out of Wisconsin, Trinity Solar and Foss Manufacturing which makes nonwoven textile products for a number of industries,

including construction, were also recent victims of spear phishing scams this year involving employee W-2 tax information.

Close to 100 companies have reported data breaches where employee information was compromised. There are probably many more attacks that either have not been reported yet or have so far gone unnoticed. Targeted companies span a wide range of industries including healthcare, hospitality, financial and retail. Municipalities, school districts and universities have also reported being victims of phishing scams and data breaches this year. Some of the companies you might be familiar that have suffered data breaches this year include Advance Auto Parts, Medieval Times, Sprouts Farmers Market and Mansueto Ventures, publishers of Inc. and Fast Company.

Remember the Target data breach from a couple of years ago? The attackers got access to login credentials for Target's computer network from one of their vendors, Fazio Mechanical. An employee fell victim to a phishing scam that allowed malware to be installed on the company's computers. Fazio had access for electronic billing, project management and contract submission and not because they were remotely monitoring and controlling any of the HVAC and refrigeration systems at any of their stores.

A spear phishing attack also led to physical damage at a steel mill in Germany. Malware was downloaded onto a company computer that had access to the plant's business network. From there, the hackers were able to gain access to the production network where they compromised the control systems, resulting in a blast furnace not being able to properly shut down.

Most security experts agree that it's a matter of when, not if, your company is targeted by hackers. Even the most sophisticated networks can be breached so it is also important to have a response plan in place in the event of a cyber incident. Your company should also invest in cyber insurance since traditional insurance coverage such as commercial general liability (CGL) policy might not cover cyber and technology liability.

(Source: https://www.isqft.com/start/blog-data-breaches-cyber-security-and-the-construction-industry/)

Top 3 Cybersecurity Risks in Construction:

- Mobile Workforce – Construction has a fluid environment that changes daily and most a construction company's employees are in the field and their office is a jobsite trailer, so IT needs to fortify that trailer just like it would any office. With so many field employees, most employees use laptops, tablets, and smartphones, all of which leave the safety of the main office. You need to require all users to enter a password to access these devices and you should be able to remove access to any company data or have the ability to wipe all company data off the device remotely.
- File Sharing Outside the Company's Network – Since construction is a team sport that takes dozens of companies to complete a project, confidential data (bids, blueprints, financials, employee records) must remain secure, yet accessible.

- Mix of Users – Construction brings together people from all walks of life including different education levels, locations, languages, and more. Unlike most corporate offices, you cannot classify every employee at a construction company as an office or field worker. Add in the volatility of turnover and the reliance on subcontractors, the constant change in staff makes it difficult to consistently train everyone.

(Source: https://www.myitsupport.com/blog/construction-cybersecurity-risks)

b. Societal needs, including expanding educational opportunities and choices for minorities and educationally disadvantaged students at institutions of higher education.

Capitol Technology University is a diverse multiethnic and multiracial institution with a long history of serving minority populations. The University has a 51% minority student population with 7% undisclosed. The Black/African American population is 34%. The university has military/veteran population of 22%. The University also has a 22% female population – a significant percentage given its status as a technology institution. If approved, the proposed **M.S. in Construction Cybersecurity** will expand the field of opportunities for minorities and disadvantaged students.

Higher education and experience requirements make skills gaps hard to close. Because cybersecurity with knowledge of the construction industry jobs require years of training and relevant experience, skills gaps cannot easily be resolved though short-term solutions. Employers and training providers must work together to cultivate a talent pipeline for these critical roles.

c. The need to strengthen and expand the capacity of historically black institutions to provide high quality and unique educational programs.

While Capitol Technology University is not a historically black institution, the university is a diverse multiethnic and multiracial institution with a long history of serving minority populations. The University has a 51% minority student population with 7% undisclosed. The Black/African American population is 34%. The University has military/veteran population of 22%. The university also has a 22% female population – a significant percentage given its status as a technology institution. If approved, the proposed **M.S. in Construction Cybersecurity** will expand the field of opportunities for minorities and disadvantaged students.

A report from the Business-Higher Education Forum notes that African Americans and Hispanics represent just 6 and 7% respectively of STEM employment, even though they represent more than twice that much of the U.S. population." The U.S. Bureau of Labor Statistics also shows inequalities in the percentages of women and minorities in Construction and Information Security (the closest match to cybersecurity) when compared to the total population.

Industry	2018				
	Percent of total employed				
	Women	White	Black or African American	Asian	Hispanic or Latino
Total Population	46.9	78.0	12.3	6.3	17.3
Construction	3.4	87.5	7.1	1.6	37.0
Information Security	24.9	76.8	12.3	8.5	6.8

(Source: https://www.bls.gov/cps/cpsaat11.htm)

Given the substantial minority population of Capitol Technology University, it is reasonable to assert that the **M.S. in Construction Cybersecurity** program will add to the base of minority participation in the ranks of construction and cybersecurity professionals.

2. Provide evidence that the perceived need is consistent with the Maryland State Plan for Postsecondary Education.

The 2017-2021 Maryland State Plan for Postsecondary Education articulates three goals for postsecondary education:

1. Access
2. Success
3. Innovation

Goal 1: Access

"Ensure equitable access to affordable and quality postsecondary education for all Maryland residents."

Capitol Technology University is committed to ensuring equitable access to affordable postsecondary education for all Maryland residents. The University meets its commitment in this arena through its diverse campus environment, admissions policies, and academic rigor.

The Capitol Technology University community is committed to creating and maintaining a mutually respectful environment that recognizes and celebrates diversity among all students, faculty, and staff. The University values human differences as an asset and works to sustain a culture that reflects the interests, contributions, and perspectives of members of diverse groups. The University delivers educational programming to meet the needs of diverse audiences. We also seek to instill those values, understanding, and skills to encourage leadership and service in a global multicultural society.

The University's commitment to diversity is reflected in its student body. Capitol Technology University has a 51% minority student population with 7% undisclosed. The Black/African American population is 34%. The university has military/veteran population of 22%. The university also has a 22% female population – a significant percentage given its status as a technology university.

Achievement gaps: The University provides leveling courses in support of individuals attempting a career change to a field of study not necessarily consistent with their current

skills. There are situations where additional graduate and/or undergraduate courses best serve student needs in subject areas. The University makes those courses available.

The University engages in diversity training for its institutional population, including students. Diversity and inclusiveness are built in to the curriculum allowing graduates to operate effectively in a global environment. The University supports multiple diversity enhancing actions, including team projects and grants across degrees. This approach has proven effective at supporting multiple aspects of diversity.

Capitol Technology University does not discriminate on the basis of race, color, national origin, sex, age, sexual orientation, handicap in admissions, employment, programs, or activities.

Through its academic programs, Capitol Technology University seeks to prepare all its graduates to demonstrate four primary characteristics:

- **Employability:** *The ability to enter and advance in technical and managerial careers, appropriate to their level and area of study, immediately upon graduation.*
- **Communications:** *Mastery of traditional and technological techniques of communicating ideas effectively and persuasively.*
- **Preparation of the Mind:** *The broad intellectual grounding in technical and general subjects required to embrace future technical and managerial opportunities with success.*
- **Professionalism:** *Commitment to life-long learning, ethical practice and participation in professions and communities.*

The proposed **M.S. in Construction Cybersecurity** program and university financial aid will be available to all Maryland residents who qualify academically for admission.

The **M.S. in Construction Cybersecurity** program, with its academic rigor, will produce highly qualified construction cybersecurity professionals for this critical field of study and employment. The University has a proven record of rigorous high-quality education. The University is fully accredited by five accrediting organizations. The University receives its regional accreditation from the Middle States Commission on Higher Education (MSCHE). The University also has specialized accreditation from the International Accreditation Council of Business Education (IACBE), Accreditation Board for Engineering and Technology (ABET), and National Security Agency (NSA)/Department of Homeland Security (DHS). The proposed construction cybersecurity program is consistent with the MSCHE criteria for regional accreditation of the delivery of high quality higher education as well as the specialized National Security Agency (NSA)/Department of Homeland Security (DHS) accreditation requirements for cybersecurity programs.

Goal 2: Success

"Promote and implement practices and policies that will ensure student success."

The courses for the **M.S.in Construction Cybersecurity** will be offered online using the Canvas Learning Management System and Zoom. The University provides a tuition structure that is competitive with its competitors. The University tuition structure does not differentiate between in-state and out-of-state students. Student services are designed to provide advising,

tutoring, virtual job fair attendance, and other activities supporting student completion and employment for both on-ground and online students.

Students receive information throughout the admissions process regarding the cost to attend the University. The information is also publicly available on the University website. The University's Admissions Office and Office of Financial Aid identify potential grants, scholarships, and state plans for each student to reduce potential student debt. The net cost versus gross costs are identified clearly for the student. Students receive advising from Financial Aid Advisors prior to enrolling in classes for the first time. Admissions personnel, Student Services Counselors and Departmental Chairs advise students of the need for academic readiness as well as the degree requirements. A specific success pathway is developed for each student.

The University's tuition increases have not exceeded 3%. The University also has a tuition guarantee for undergraduates, which means full-time tuition is guaranteed not to increase more that 1% per year at the rate applied at time of enrollment. The tuition remains at this rate if the student remains enrolled full-time without a break in attendance.

The University has in place services and learning tools to guide students to successful degree completion. Programs such as Early Alert provide the University's faculty and staff opportunities for early student intervention on the pathway to graduation. This applies to all students regardless of the mode of course delivery or degree program. Capitol Technology University is also a transfer friendly institution and participates in multiple programs for government and military credit transfer. Capitol Technology University participates in the Articulation System for Maryland Colleges and Universities (ARTSYS) and has multiple transfer agreements with local institutions at all degree levels.

The University has in place services, tutoring, and other tools to help ensure student graduation and successful job placement. The University hosts a career (job) fair twice a year. The University has an online career center available to all students covering such topics as career exploration, resume writing, job search techniques, social media management, mock interviews, and assistance interpreting job descriptions, offers, and employment packages.

The University also works with its advisory boards, alumni, partners, and faculty to help ensure the degrees offered at the University are compatible with long-term career opportunities in support of the state's knowledge-based economy.

Goal 3: Innovation

"Foster innovation in all aspects of Maryland higher education to improve access and student success."

Capitol Technology University's past, present, and future is inextricably intertwined with innovation. The University has a long tradition of serving as a platform for the use of new and transformative approaches to delivering higher education. New technology and cutting-edge techniques are blended with proven strategies with the goal of enabling student success in all classroom modalities as well as in a successful career after graduation. As a small institution, Capitol Technology University has the agility to rapidly integrate new technologies into the curriculum to better prepare students for the work environment. The

University designs curriculum in alliance with its accreditation and regulating organizations and agencies.

The University also employs online virtual simulations in a game-like environment to teach the application of knowledge in a practical hands-on manner. The University is engaged with a partner creating high-level virtual reality environments for specific courses in the degree. This use of current technology occurs in parallel with traditional proven learning strategies. These elements of the University's online learning environment are purposeful and intended to improve the learning environment for both the student and faculty member. In addition, these elements are intentionally designed to increase engagement, improve outcomes, and improve retention and graduation rates. The University believes that innovation is the key to successful student and faculty engagement.

Example: The University engages its students in 'fusion' projects, which allows students to contribute their skills in interdisciplinary projects such as those in our Astronautical Engineering and Cyber Labs. In those labs, students become designers, builders, and project managers (e.g., to send a CubeSAT on a NASA rocket) and data analysts (e.g., to analyze rainforest data for NASA). The University's students recently launched another satellite aboard a NASA rocket from a location in Norway at the beginning of the 2018 Fall Semester. We are also recruiting additional partners for the proposed **M.S. in Construction Cybersecurity** for which real-world projects will provide students integrative learning opportunities.

The University also supports prior learning assessment. Portfolio analysis is available. The University accepts professional certifications for credit for specific courses. In addition, the University allows students to take a competency exam for credit for required courses up to the current state limits.

C. Quantifiable and Reliable Evidence and Documentation of Market Supply and Demand in the Region and State:

1. **Describe potential industry or industries, employment opportunities, and expected level of entry (*ex: mid-level management*) for graduates of the proposed program.**

Graduates with the **M.S. in Construction Cybersecurity** will be expected to fill mid-level management positions in existing commercial companies and government organizations with titles such as:

- Director, Cybersecurity
- Director, Construction Cyber Operations
- Senior Director, Cybersecurity
- Managing Director, Construction Information and Cybersecurity
- Managing Director, Cybersecurity
- Construction Industry Senior Cybersecurity Strategist
- Construction Cybersecurity Consultant
- Executive Director, Information Technology and Cybersecurity
- Chief Cybersecurity Officer

Graduates will also possess the required knowledge in construction cybersecurity to serve as a subject matter expert and form their own private company.

2. Present data and analysis projecting market demand and the availability of openings in a job market to be served by the new program.

According to the article "Cybersecurity in the Construction Industry: Protecting Against a Growing Threat":

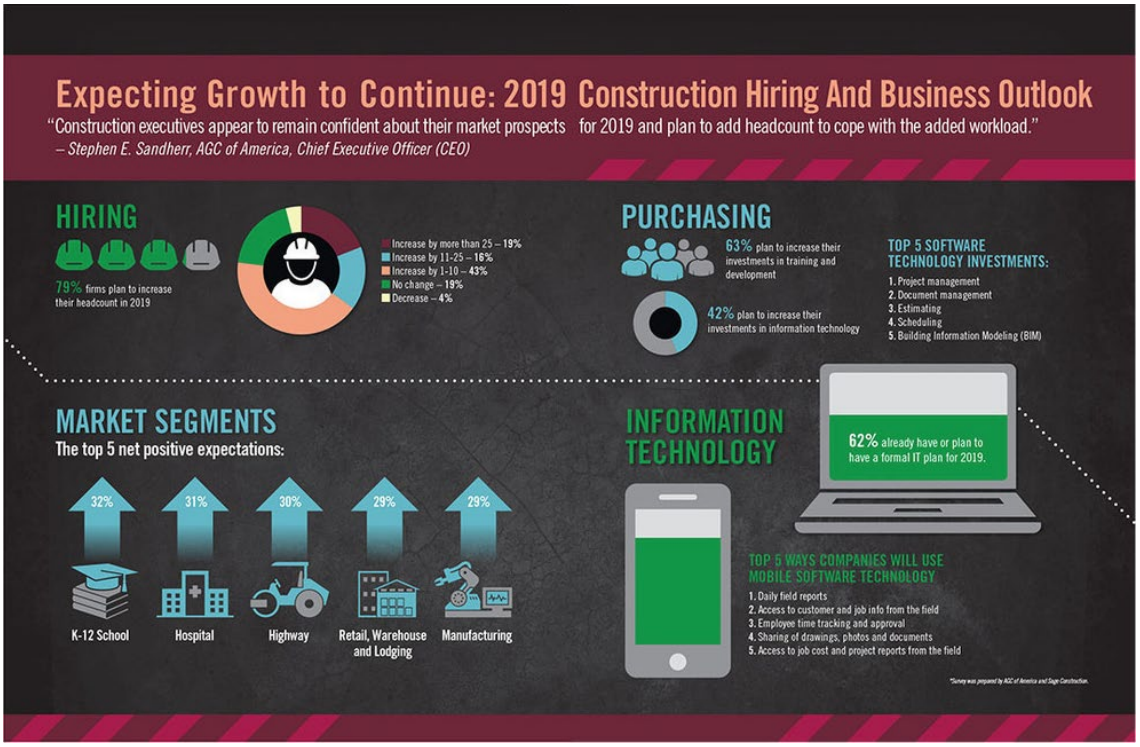
> "Why Cyber Threats to Construction are on the Rise. The construction industry, like so many other sectors of the economy, is increasingly dependent on the internet and on internet-enabled technologies. Shared resources like integrated project delivery and building information modeling increase the risk that an authorized user will unintentionally introduce malware into shared systems. The widespread use of vendors and subcontractors who have connectivity to shared information technology (IT) networks increases the risk that a cyber incident involving one company will become a vulnerability for many companies. In addition, the steady growth in connected and remote-controllable devices – broadly known as the "Internet of Things" – has vastly increased the potential attack surface for cyber threats. Perhaps the most famous example of the ways in which these threats can intersect with and magnify each other is the Target department store data breach, in which millions of Target customers' credit card information was exposed, and Target suffered millions of dollars in breach response costs, litigation fees, lost revenue, and incalculable reputational harm. The breach originated with an HVAC vendor who was responsible for managing "smart" thermostats at Target facilities. Once inside the network, the hackers were able to traverse the connected IT architecture and penetrate Target's payment card information databases.
>
> What is at Risk? Cyber threats can expose all of a company's digital assets: business plans and acquisition strategies; proprietary construction plans and designs; customer, contractor, and supplier lists and pricing; personally identifiable information of employees and contractors; protected health information of personnel; and facilities security information. Cyber risk can also cause business interruption and reputational harm: for example, a ransomware attack might not lead to a loss of information, but by shutting down a company's computer networks, and potentially destroying information, it can cause an enormous amount of lost productivity and business delay. And the ability for cyber attackers to hijack physical devices – from security cameras to vehicle telematics to industrial control systems – means that there is an ever-increasing risk of property damage and personal injury due to cybersecurity incidents."

(Source: https://www.jdsupra.com/legalnews/cybersecurity-in-the-construction-22150/#Follow Section)

The London-based digital marketers reviewed ProofPoint's cybersecurity quarterly analysis and found the construction industry is the second most targeted for email fraud with an average of 61 attacks per company over a three-month period. The real estate industry follows with an average of 54 attacks per organization in the same time frame according to a recent article by Builder Online entitled, "Cyber-Criminals Prey Heavily on Construction Pros."

(Source: https://www.builderonline.com/builder-100/it-technology/cyber-criminals-prey-heavily-on-construction-pros_o)

At the same time, Constructor magazine states software technology investments and mobile software technology use are expanding rapidly in the construction industry. The table below shows the construction industry expanding with a significant investment in more technology.



(Source: https://www.constructor-digital.com/ngcs/0119_march_april_2019/MobilePagedArticle.action?articleId=1466614#articleId1466614)

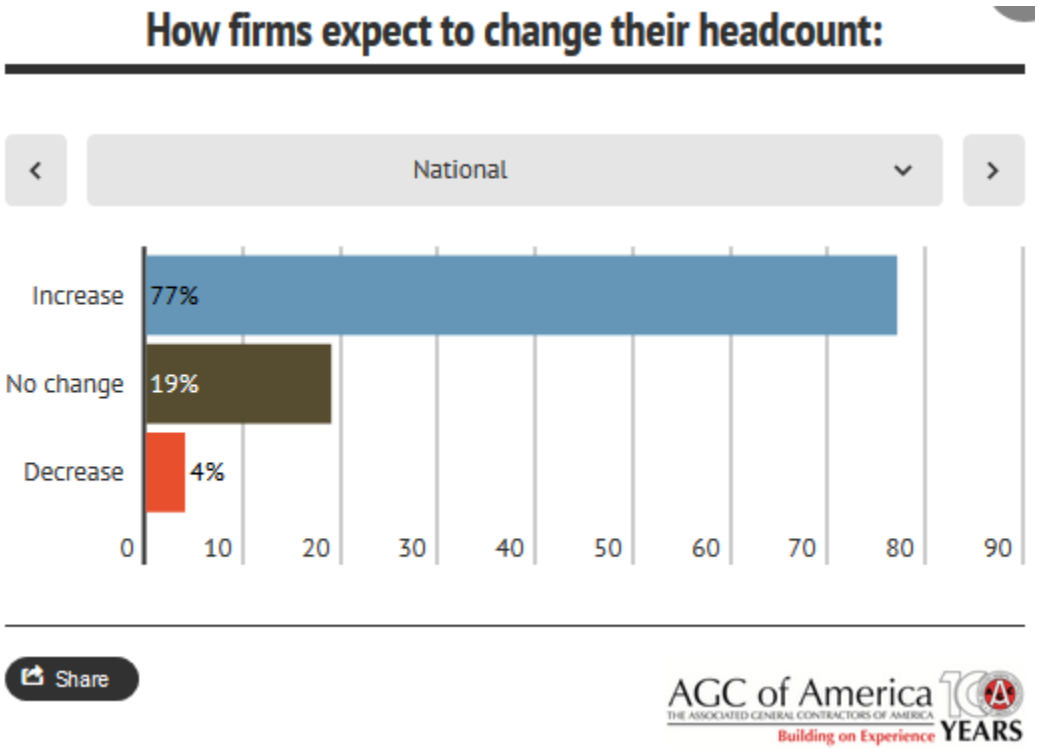
The protection of Critical Infrastructure is a mandate now permeating many sectors of the economy. One industry that spans all of the others of the economy is construction; as a result, construction firms are now finding requirements to address the cybersecurity protection of Critical Infrastructure in all of their projects while at the same time protecting their company from attacks. Cybersecurity is a key component of Critical Infrastructure protection as buildings become "smarter" and more reliant on technology.

"Security is no longer restricted to just technology companies or financial institutions… organizations in charge of critical infrastructure such as the electric grid grapple with skilled adversaries who take advantage of holes in the network defenses to cause damage."

(Source: http://burning-glass.com/average-cybersecurity-salary-over-93000/)

3. **Discuss and provide evidence of market surveys that clearly provide quantifiable and reliable data on the educational and training needs and the anticipated number of vacancies expected over the next 5 years.**

2019 Sage Construction Hiring and Business Outlook Survey



Seventy-nine percent of construction firms plan to expand their payrolls in 2019 but an almost equal percentage are worried about their ability to locate and hire qualified workers, according to survey results released today by the Associated General Contractors of America and Sage Construction and Real Estate. The findings are detailed in Contractors Remain Confident About Demand, Worried About Labor Supply: The 2019 Construction Hiring and Business Outlook Report.

“Construction executives appear to remain confident about their market prospects for 2019 and plan to add headcount to cope with the added workload,” said Stephen E. Sandherr, the association's chief executive officer. “Even as they are optimistic about growing demand, contractors are concerned about finding qualified workers to execute projects.”

(Source: https://www.agc.org/news/2019/01/02/2019-sage-construction-hiring-and-business-outlook-survey)

Employment of information security analysts is projected to grow 28 percent from 2016 to 2026 -- much faster than the average for all occupations. Demand for information security analysts is expected to be very high, as these analysts will be needed to create innovative solutions to prevent hackers from stealing critical information or causing problems for computer networks.

Quick Facts: Information Security Analysts	
2018 Median Pay	$98,350 per year $47.28 per hour
Typical Entry-Level Education	Bachelor's degree
Work Experience in a Related Occupation	Less than 5 years
On-the-job Training	None
Number of Jobs, 2016	100,000
Job Outlook, 2016-26	28% (Much faster than average)
Employment Change, 2016-26	28,500

(Source: https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm)

Employment projections data for information security analysts, 2016-26

Occupational Title	SOC Code	Employment, 2016	Projected Employment, 2026	Change, 2016-26	
				Percent	Numeric
Information security analysts	15-1122	100,000	128,500	28	28,500

SOURCE: U.S. Bureau of Labor Statistics, Employment Projections program

(Source: https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-6)

In 2018, there were 143 4-year construction-related programs at U.S. universities. Graduates from these institutions fill entry-level positions as project engineers, estimators, safety managers, superintendents, Building Information Management (BIM) managers, pre-con, document control and communication positions, schedulers, etc. A portion of those graduates who wish to advance their careers to positions of greater responsibility will also enter graduate programs. The growing cybersecurity field is looking for those persons to fill the rapidly expanding demand in the construction arena.

4. Data showing the current and projected supply of prospective graduates.

According to The Cyber Edge, the projected shortage of skilled workers is increasing to nearly 2 million for cybersecurity professionals.

> The cybersecurity workforce gap is real, and it's growing. Based on a state-by-state analysis on CompTIA's cyberstates.org, there are currently 320,000 open cyber jobs in the United States. By 2022, the projected shortage of cybersecurity professionals worldwide will reach 1.8 million, according to the Center for Cyber Safety and Education.
>
> The challenge for government agencies in the United States to recruit and retain talent is mammoth. A June 2018 report by the U.S. departments of Commerce and Homeland Security noted, "The United States needs immediate and sustained improvements in its cybersecurity workforce situation."

> Lengthy security clearance delays and onboarding processes, along with low pay and a knowledge gap about specific workforce needs and education programs, have severely impacted the total number of cybersecurity workers across the country.
>
> Shortages exist for nearly every position within cybersecurity. Most alarmingly though, the greatest need is for highly skilled technical staff. In 2010, the Center for Strategic and International Studies' (CSIS) report "A Human Capital Crisis in Cybersecurity" found that the United States "not only [has] a shortage of the highly technically skilled people required to operate and support systems already deployed, but also an even more desperate shortage of people who can design secure systems, write safe computer code and create the evermore sophisticated tools needed to prevent, detect, mitigate and reconstitute from damage due to system failures and malicious acts."

By 2016, CSIS found that things had not improved much. Information technology professionals still consider technical skills such as secure software development the most difficult to find among cybersecurity candidates.

Rob Joyce knows all too well there is not enough skilled talent for the growing need of the cyber community. As senior cybersecurity strategy advisor to the director, National Security Agency (NSA), and former cybersecurity advisor to the president, he thinks "we need to make systemic changes to address [the] gap."

Speaking to attendees at AFCEA's second annual Cyber Education Research and Training Symposium (CERTS) in January 2019 in Augusta, Georgia, Joyce emphasized the need for formal and informal education, and diversity in cybersecurity as a starting point.

A key element of his long-term national cyber strategy is formal education. "We need to get people into that education pipeline," Joyce said. "Less than 65,000 people will graduate with undergraduate degrees in computer and information science fields. That's not cybersecurity. That includes all [information technology] and computer science students across the country. That's a scary figure when we say we have more than 300,000 open jobs," Joyce stressed.

What's more alarming is that of those 65,000, only 12,000 are women. Even fewer are minorities. "I think if you are looking for a strategic lever that the nation has to pull, the first thing we have to do is balance that pipeline out to represent our population," he said.

The International Information System Security Certification Consortium (ISC)2 reported in 2017 that women continue to make up only 11 percent of the information security workforce worldwide, and only about 14 percent in the U.S. Joyce believes that needs to change if the cyber community hopes to make a dent in the skills-gap crisis.

"If we can get women into the computer science/cybersecurity field at the same level as men, we will see a substantial increase in that pipeline," Joyce stated. "It's the same for minorities. If the computer science outlook looked like the demographics of our country, we would up those numbers [in the pipeline] significantly."

Concurrently, two studies on the projected supply and demand for graduates in the construction field from accredited institutions of higher education shows a significant workforce shortage of graduates in the field that has been growing since 2000.

> In 1997 the Department of Construction Science at Texas A&M University conducted a survey of accredited construction programs and construction companies that consistently hired from these programs to identify if the demands of the industry were being met by the supply of construction graduates. A time series regression analysis was used to predict the demand for construction graduates from accredited construction programs. The model showed that there was an increase in demand for construction graduates of approximately 593 students per annum. The supply of students however was reported as remaining static for the next five years indicating the prospect of gap between supply and demand. The results of this research were presented at the annual conference of the Associated Schools of Construction in 2000. In 2005 the study was repeated to see if there had been any change in the supply and demand for construction education graduates. In the 2005 study, 64 accredited construction education programs were surveyed to quantify the number of "construction graduates" who were produced by accredited construction programs. The study surveyed 551 construction companies across the United States, who hired construction graduates to quantify the demand for construction graduates. The study then compared the supply and demand figures. In 2005, findings from the accredited universities indicated a production level of approximately 3596 construction graduates. The industry survey indicated a demand in 2005 for approximately 7877 construction graduates. The intent of the study is to provide a representation of the current production level of, and the demand for construction graduates, for the purpose of comparing supply and demand. Actual demand figures are given for the years 2000 through 2005. Demand projections are given for the years 2006, 2007, 2008, 2009, 2010. Supply figures are based upon the average production of construction graduates, from each identified university, during the years 2000 through 2005. The results of the survey data indicate an increasing demand for construction education graduates of approximately 754 students per annum. Additionally, the survey data reveals the supply of construction graduates is increasing by only 160 students annually and is not currently meeting the demands of the construction industry, nor will it be meeting the industry demands in the future.
>
> (Source: https://www.researchgate.net/publication/238071959_A_Study_ of_the_Supply _and_Demand_for_Construction_Education_Graduates_in_the_United_States [accessed Dec 20 2018].)

The **M.S. in Construction Cybersecurity** will be the first degree in the nation to address the cybersecurity needs of the construction industry. It will send its graduates to leadership positions in industry with the ability to chart the course of their organization and its success in the future. The program graduates will be in the position to earn the maximum amount of income in construction cybersecurity and fill the requirement for its leaders to possess current knowledge in cybersecurity focused on protecting the construction industry.

D. Reasonableness of program duplication:

1. **Identify similar programs in the State and/or same geographical area. Discuss similarities and differences between the proposed program and others in the same degree to be awarded.**

   There are 15 master's degrees offered by eight institutions in the broad area of cyber in the State of Maryland. Those institutions are Capitol Technology University, Hood College, Johns Hopkins University, Stevenson University, University of Maryland Eastern Shore, University of Maryland Global Campus, University of Baltimore, and University of Maryland Baltimore County. Of the 15 master's degrees, eleven of the degrees focus on cybersecurity or related aspect. However, none of the existing master's degrees is specifically focused on construction cybersecurity. Capitol Technology University's proposed **M.S. in Construction Cybersecurity** is focused only on the narrow area of construction cybersecurity. If approved, Capitol Technology University's **M.S. in Construction Cybersecurity** will position its graduates to fill the requirement for managers and senior leaders in the construction cybersecurity industry in Maryland and the region.

2. **Provide justification for the proposed program.**

   The program is strongly aligned with the University's strategic priorities and is supported by adequate resources. The new **M.S. in Construction Cybersecurity** will strengthen and expand upon existing graduate degree programs at the University. The degree will represent study in a rapidly changing and expanding discipline. Research shows a current and growing shortage of construction cybersecurity leaders. There is a thorough discussion of the need in sections B and C of this document.

E. Relevance to high-demand programs at Historically Black Institutions (HBIs):

1. **Discuss the program's potential impact on the implementation or maintenance of high-demand programs at HBIs.**

   The University does not anticipate any impact on the implementation or maintenance of high-demand programs at HBIs. There are 15 master's degrees offered by eight institutions in the broad area of cyber in the State of Maryland. However, none of the existing master's degrees is specifically focused on cybersecurity in the construction industry. Only one HBI, University of Maryland Eastern Shore (UMES), offers a master's degree in cyber: a M.S. in Cyber Engineering Technology. **Capitol Technology University's proposed degree is different in scope than all existing master's programs in the state; Capitol Technology University's M.S. in Construction Cybersecurity is focused only on the narrow area of construction cybersecurity.**

F. Relevance to the identity of Historically Black Institutions (HBIs):

1. **Discuss the program's potential impact on the uniqueness and institutional identities and missions of HBIs.**

   The University does not anticipate any impact on the uniqueness and institutional identities and missions of HBIs. There are 15 master's degrees offered by eight institutions in the broad area of

cyber in the State of Maryland. However, none of the existing master's degrees is specifically focused on cybersecurity in the construction industry. Only one HBI, University of Maryland Eastern Shore (UMES), offers a master's degree in cyber: a M.S. in Cyber Engineering Technology. **Capitol Technology University's proposed degree is different in scope than all existing master's programs in the state; Capitol Technology University's M.S. in Construction Cybersecurity is focused only on the narrow area of construction cybersecurity.**

G. Adequacy of Curriculum Design, Program Modality, and Related Learning Outcomes (as outlined in COMAR 13B.02.03.10):

1. **Describe how the proposed program was established, and also describe the faculty who will oversee the program.**

   The proposed program was established through a rigorous review of unmet needs by the University's New Programs Group. The group includes selected representation from the faculty, administrators, and Executive Council. The program will be overseen by a diverse group of faculty members with backgrounds in civil engineering, cybersecurity, construction management, mechanical engineering, environmental engineering, architectural engineering, strategic studies, technology, and business. Please see Section I for a detailed list of the faculty's backgrounds.

2. **Describe educational objectives and learning outcomes appropriate to the rigor, breadth, and (modality) of the program.**

   Educational Objectives:

   a. Students will critically analyze problems in a variety of disciplines and synthesize relevant information to support the attainment of desired outcomes.
   b. Students will identify, formulate, and solve complex construction cybersecurity problems by selecting and applying appropriate tools and techniques.
   c. Students will identify and synthesize problems in construction cybersecurity planning, tactics, techniques, procedures, cost, and decision analysis in order to develop optimum solutions.
   d. Students will conceptualize, apply and integrate effective strategies to use information effectively in the construction cybersecurity decision-making process.
   e. Students will evaluate executive decisions in the context construction cybersecurity to determine the potential impact on resources and profitability.
   f. Students will evaluate the legal, social, economic, environmental, and global ramifications of actions and decisions within construction cybersecurity.

   Learning Outcomes:

   Upon graduation:

   a. Graduates will critically analyze cybersecurity problems within the construction industry, synthesize the relevant information, and formulate solutions to attain desired outcomes.
   b. Graduates will demonstrate highly-developed traditional and technological techniques and skills in communicating ideas effectively and persuasively.

c. Graduates will evaluate the legal, social, economic, environmental, and global ramifications of their cybersecurity decisions in the construction industry.
d. Graduates will integrate advanced knowledge of cybersecurity in the application of concepts, plans, processes, project management, and team leadership skills on the job.
e. Graduates will identify, formulate, and solve complex cybersecurity problems in the construction industry by selecting and applying appropriate tools and techniques.
f. Graduates will demonstrate advanced knowledge of cybersecurity and the impact of technology within the construction industry.

3. Explain how the institution will:

a) Provide for assessment of student achievement of learning outcomes in the program

Capitol Technology University will assess student achievement of the learning outcomes per the regulations specified by the university's regional accreditation organization, the Middle States Commission on Higher Education (MSCHE), and jointly by the National Security Agency (NSA) and Department of Homeland Security (DHS) via the National Centers of Academic Excellence (CAE) in Cyber Defense (CAE-CD).

Under MSCHE, the University will use Standard V, Educational Effectiveness Assessment, of the Standards for Accreditation and Requirements of Affiliation. Standard V requires:

> Assessment of student learning and achievement demonstrates that the institution's students have accomplished educational goals with their program of study, degree level, the institution's mission, and appropriate expectations for institutions of higher education.
>
> (Source: https://www.msche.org/?Nav1=About&Nav2=FAQ&Nav3=Question07)

Per the MSCHE's accreditation requirements, Capitol Technology University will measure Standard V by using the following criteria:

> An accredited institution possesses and demonstrates the following attributes or activities:
>
> 1. clearly stated educational goals at the institution and degree/program levels, which are interrelated with one another, with relevant educational experiences, and with the institution's mission;
>
> 2. organized and systematic assessments, conducted by faculty and/or appropriate professionals, evaluating the extent of student achievement of institutional and degree/program goals. Institutions should:
>
> a. define meaningful curricular goals with defensible standards for evaluating whether students are achieving those goals;
> b. articulate how they prepare students in a manner consistent with their mission for successful careers, meaningful lives, and, where appropriate, further education. They should collect and provide data on the extent to which they are meeting these goals;
> c. support and sustain assessment of student achievement and communicate the results of this assessment to stakeholders;

3. consideration and use of assessment results for the improvement of educational effectiveness. Consistent with the institution's mission, such uses include some combination of the following:

a. assisting students in improving their learning;
b. improving pedagogy and curriculum;
c. reviewing and revising academic programs and support services;
d. planning, conducting, and supporting a range of professional development activities;
e. planning and budgeting for the provision of academic programs and services;
f. informing appropriate constituents about the institution and its programs;
g. improving key indicators of student success, such as retention, graduation, transfer, and placement rates;
h. implementing other processes and procedures designed to improve educational programs and services;

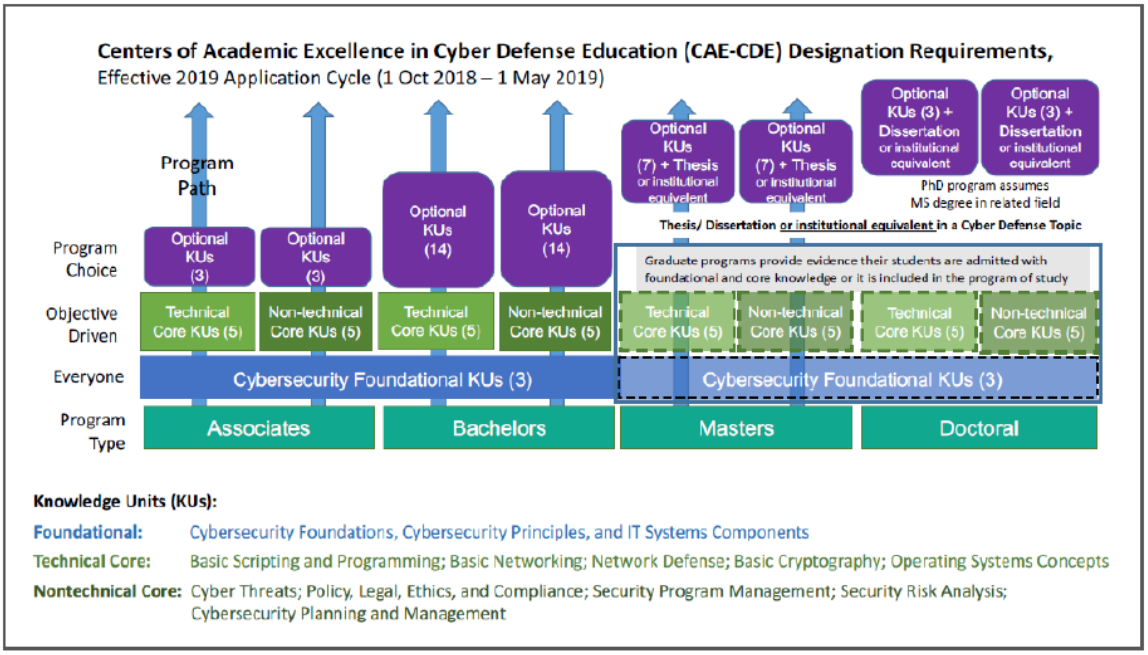
4. if applicable, adequate and appropriate institutional review and approval of assessment services designed, delivered, or assessed by third-party providers; and

5. periodic assessment of the effectiveness of assessment processes utilized by the institution for the improvement of educational effectiveness.

(Source: https://www.msche.org/publications/RevisedStandardsFINAL.pdf)

The University will also use the NSA/DHS National Centers of Academic Excellence (CAE) in Cyber Defense (CAE-CD) and its related assessment tools to assess student achievement of the learning outcomes in the program. The following tables provide a high-level view of the National Centers of Academic Excellence (CAE) in Cyber Defense (CAE-CD) program as it relates to degrees, Cybersecurity Foundations Knowledge Units, Technical Knowledge Units, Non-Technical Knowledge Units, and Optional Knowledge Units. All four Knowledge Unit areas work together and have highly detailed assessment tools.

NSA/DHS National Centers of Academic Excellence (CAE) in Cyber Defense (CAE-CD) Program's Knowledge Units Mapped to Degree Levels



(Source: NSA/DHS 2019 Knowledge Units)

NAS/DHS Cyber Defense (CAE-CD) Foundational Knowledge Units

1. Security Concepts
   - Confidentiality, Integrity, Availability
   - Access
   - Identification, Authentication, Authorization, Non-Repudiation
   - Privacy
   - Critical infrastructures
   - Security Models (Bell-La Padula, Biba, Clark Wilson, Brewer Nash, Multi-level security)
2. People and security
   - Social engineering
   - Cyber Defense Partnerships (Federal, State, Local, Industry)
3. Security Processes
   - Basic Risk Assessment/Management
   - Security Life-Cycle
4. Threats and Adversaries (threat actors, malware, natural phenomena)
   - External
   - Internal
5. Vulnerabilities
   - Vulnerability Scanning (core)
   - Vulnerability Windows (0-day to patch availability)
   - Data Vulnerabilities (in transmission, at rest, in processing)
6. Common Attacks
   - Forms of Attack
7. Appropriate Countermeasures
   - Security Mechanisms (e.g., Identification/Authentication, Audit)
   - Network Security Components (Data Loss Prevention, VPNs / Firewalls)
   - Intrusion Detection and Prevention Systems,
   - Malicious activity detection
8. Concepts of the applications of Cryptography and PKI
   - Physical and environmental security concerns
   - Access Control Models (MAC, DAC, RBAC, Lattice)
9. Exception Management
   - Incident Response
10. Legal issues
11. Ethics (Ethics associated with cybersecurity profession)

(Source: NSA/DHS 2019 Knowledge Units)

NSA/DHS Cyber Defense (CAE-CD) Technical Core KUs & Non-Technical Core KUs

Technical Core KUs	Non-Technical Core KUs
Basic Cryptography	Cyber Threats
Basic Networking	Cybersecurity Planning and Management
Basic Scripting and Programming	Policy, Legal, Ethics, and Compliance
Network Defense	Security Program Management
Operating Systems Concepts	Security Risk Analysis

(Source: NSA/DHS 2019 Knowledge Units)

NSA/DHS Cyber Defense (CAE-CD) Optional KUs

Optional KU's

Programs need to document their programs of study using knowledge units. The categories of knowledge units are foundational (used in all programs), core (either technical or nontechnical) which form the base of the program. The remainder of the knowledge units are called optional KUs, and this is a category that can be adopted by any program as needed to document their program of study. Additionally, opposing core KUs may be used as optional KUs (i.e. If technical core is chosen, then non-technical core maybe used as optional KUs and if non-technical core is chosen, then technical core maybe used as optional KUs.)

Advanced Algorithms
Advanced Cryptography
Advanced Network Technology and Protocols
Algorithms
Analog Telecommunications
Basic Cyber Operations
Cloud Computing
Cyber Crime
Cybersecurity Ethics
Data Administration
Data Structures
Database Management Systems
Databases
Device Forensics
Digital Communications
Digital Forensics
Embedded Systems
Forensic Accounting
Formal Methods
Fraud Prevention and Management
Hardware Reverse Engineering
Hardware/Firmware Security
Host Forensics
IA Architectures
IA Compliance
IA Standards
Independent/Directed Study/Research
Introduction to Theory of Computation
Intrusion Detection/Prevention Systems
Life-Cycle Security
LINUX System Administration
Low Level Programming
Media Forensics
Mobile Technologies
Network Forensics
Network Security Administration
Network Technology and Protocols
Operating Systems Hardening
Operating Systems Theory
Penetration Testing
Privacy
QA/Functional Testing
Radio Frequency Principles
Secure Programming Practices
Software Assurance
Software Reverse Engineering
Software Security Analysis
Supply Chain Security
Systems Certification and Accreditation
Systems Programming
Systems Security Engineering
Virtualization Technologies
Vulnerability Analysis
Windows System Administration
Wireless Sensor Networks

(Source: NSA/DHS 2019 Knowledge Units)

b) Document student achievement of learning outcomes in the program

The University will document student achievement of the learning outcomes in the program in the same fashion as its current programs. The University will also publicly post the results of the assessment on its website.

4. Provide a list of courses with title, semester credit hours and course descriptions, along with a description of program requirements.

Program description, as it will appear in the catalog:

The **Master of Science (M.S.) in Construction Cybersecurity** degree program is designed to meet the growing needs of today's business and government where construction cybersecurity is now a major consideration. The **M.S. in Construction Cybersecurity** provides advanced graduate-level management education where the latest construction cybersecurity concepts are reviewed and analyzed with a laser focus. Throughout the program, the latest technological developments, applications, and considerations in the construction industry are explored and applied to real-life industry challenges. Students will learn optimum methods and techniques in construction cybersecurity and how to define related resources and associated risks at an executive level in order to maintain profitability, manage work effectivity and efficiently, and ensure customer satisfaction.

The **M.S. in Construction Cybersecurity** will prepare students for cybersecurity leadership positions in the construction industry.

Description of program requirements:

Entrance requirements: To be fully accepted into the program, students must have completed an undergraduate degree with a cumulative GPA of no less than 3.0 on a 4.0 scale.

Students who have not met the 3.0 undergraduate cumulative GPA requirements, or do not meet all the program specific prerequisites, are provided an opportunity to gain full acceptance. Depending on the degree program, additional information may be requested. In this case, students are provisionally admitted and limited to three courses of enrollment. To achieve full acceptance, provisional students must maintain a 3.0 cumulative GPA in their first three graduate courses. Upon doing so, students are automatically converted to full acceptance status. If a provisional student fails to achieve a minimum 3.0 cumulative GPA after completing three courses, then he or she will be academically dismissed, and will not be permitted to enroll in any further courses.

Degree Requirements:

The following is a list of courses for the **M.S. in Construction Cybersecurity** degree. Students expecting to complete this degree must meet all prerequisites for the courses listed below.

Master of Science in Construction Cybersecurity
Courses
Total 30-36 Credits

CONSTRUCTION CYBERSECURITY
30-36 CREDITS

FOUNDATIONAL CORE: 6 CREDITS

(NOTE: *IAE-500 and CS-620 may be waived with University Academic Dean's approval based on a student's previous work experience and demonstrated mastery of the course knowledge.)

IAE-500 Introduction to Information Assurance (3 Credits) *
This course will provide the requisite computer, data communications, Internet and database skills to students embarking on careers in information assurance (IA), at the senior levels. It is designed primarily for professionals who seek concentrated professional education in one or more of the many fields associated with IA. Students who complete this course successfully will be able to master the more technical application and analysis skills demanded by the Master of Science in Information Assurance (MSIA) degree program, and the several certificate programs offered in various IA concentrations. Labs, simulations and special problems will be used throughout the course. Prerequisite: None. Course may be waived based on student's relevant work experience and demonstrated knowledge in the subject matter.

CS-620 Operating System Principles for Information Assurance (3 Credits) *
This course is an overview of the UNIX operating system. The content will include shell programming, process management, processor management, storage management, scheduling algorithms, resource protection and system programming. The course will include programming projects focused on Information Assurance problem solving utilizing the C programming language primarily. Students are expected to be familiar with virtual machines, the UNIX command line and a basic programming language. Basic knowledge of C programming and UNIX helpful. (3) Note: This course is not an approved elective for the MSCS program. Prerequisite: None. Course may be waived based on student's relevant work experience and demonstrated knowledge in the subject matter.

CONSTRUCTION CYBERSECURITY CORE: 30 CREDITS

CM-600 Cybersecurity Impacts on Construction Industry (3 Credits)
The course will focus on emerging issues related to cybersecurity in the construction industry. Students will research current issues and attacks on construction companies and their systems and what was the company's response. The course will allow students to create policies and plans to produce value for their future business, employers, and customers. Prerequisite: None

CM-602 Construction Industry Software (3 credits)
The course focuses on construction industry software that is used to support the industry. Software for project management, estimating, BIM, scheduling, documentation, communication, as related to representation, processing, and communication of construction information will be discussed. This course develops an understanding of the variety of software used as it relates to the tools necessary to be successful for a general contractor. Prerequisite: None

CRI-501 Critical Infrastructure Introduction (3 Credits)
This course will introduce participants to the key terms, policy, guidance, and preparedness efforts required to safeguard the Nation's critical infrastructure. Students will learn relevant policy and guidance, discuss the risk management framework, describe Federal critical infrastructure security and resilience and information sharing programs, and relate critical infrastructure

programs to individual actions. Primary focus will be on incorporating Critical Infrastructure protection in to construction of facilities in six of the sixteen critical infrastructure sectors: chemical facilities, commercial (e.g., retail, entertainment, lodging), communications facilities, critical manufacturing facilities, dams, and energy facilities. Students will complete hands-on Critical Infrastructure projects related to the construction of those types of facilities. Prerequisite: None.

CM-675 Computer Forensics and Incident Handling for Construction (3 Credits)
This course begins with lectures discussing the laws and rights to privacy by individuals and what organizations may or may not do. Online ethics are considered. It then moves on to understanding incident handling and how incident response teams work, managing trouble tickets, and basic analysis of events to determine if an incident has occurred. It concludes with computer forensics issues and practices, and rules of evidence. This course prepares students for the AccessData Certified Examiner (ACE) and Mobile Phone Examiner Plus (MPE+) Certifications. Cross-list: IAE-675. Prerequisite: CM-685.

CM-677 Malicious Software in Construction (3 Credits)
This course examines malicious software detection and malicious software defenses including tripwire and signature software techniques. Viruses, worms and Trojan horses, logic bombs, malicious CGI scripts will be discussed. Students will review the anatomy of well-known viruses and worms to understand how they work. Mobile code issues as they apply to web and application technologies and resulting insecurities will be discussed in detail. Students will then review the underlying methodologies used by the anti-virus vendors and freeware offerings to protect electronic assets from harm or other compromise. Cross-list: IAE-677. Co-requisite: CM-675.

CM-679 Cyber Vulnerability Mitigation in Construction (3 Credits)
This "Defense-in-Depth" course provides the student detailed understanding of the need for internal and external vulnerability assessment. This is an integral technical part of any risk management program. Cross-list: IAE-679. Co-requisites: CM-685.

CM-680 Cyber Perimeter Protection in Construction (3 Credits)
In this "defense-in-depth" course, firewalls and network IDS issues are discussed. A detailed understanding of firewall configuration and rule sets, load balancing, web farms, wireless access, web security issues and network intrusion detection is explored to prepare the student with the basic tools to coordinate the design and implementation of perimeter network defenses for a high volume, high access site. Prerequisite: none. This course is best taken in the last semester of the program. Cross-list: IAE-680. Prerequisite: None.

CM-682 Cyber Internal Protection in Construction (3 Credits)
This course explores the protections available to the practitioner through host operating systems and third party equipment and software, to protect the inner network from the attacker who has successfully circumvented the perimeter or from the disgruntled insider. Use of methodologies including host-based intrusion detection methods, audit settings and review PC Firewalls, host operating hardening for Linux and Windows 2000, and Virtual LANs will be reviewed. It is recommended that students complete CM-685 before taking this course, but this is not a requirement. Cross-list: IAE-682. Prerequisite: none.

CM-685 Principles of Cybersecurity for Construction (3 Credits)

This class explores the overarching security architectures and vectors of information assurance from a management perspective to allow the learner to formulate the basis for sound business decisions. Students gain an appreciation for systems, networks, processes, methodologies, documentation requirements, recovery processes, certification and accreditation processes as well as "best practice" implementation, training and continuous improvement. Discussions in this course give the correct acumen of personnel security, physical security, and technical operational security as these principles relate and interface with information security principles. Defense-in-depth principles also are covered for designing proper physical security programs. At the completion of the course students should be able to manage an IA function and evaluate an organization's Contingency Planning process for adequacy. Cross-list: IAE-685. Prerequisite: None

CM-700 Construction Cybersecurity Research Project (3 Credits)
Students will begin a graduate level research project in the field of Construction Cybersecurity. The research and thesis development are supervised by a faculty member. The student will research and write the thesis in this course and prepare to defend the thesis in a viva voce (i.e., oral) examination. This course is the second to last course in the program as the student applies accumulated knowledge of program's classes to this effort. Prerequisite: Completed in last term.

5. Discuss how general education requirements will be met, if applicable.

N/A. This is a graduate program.

6. **Identify any specialized accreditation or graduate certification requirements for this program and its students.**

The program will be accredited regionally by Middle States Commission on Higher Education (MSCHE) and jointly by the National Security Agency (NSA) and Department of Homeland Security (DHS) via the National Centers of Academic Excellence (CAE) in Cyber Defense (CAE-CD) program.

7. **If contracting with another institution or non-collegiate organization, provide a copy of the written contract.**

The University will not be contracting with another institution or non-collegiate organization.

8. **Provide assurance and any appropriate evidence that the proposed program will provide students with clear, complete, and timely information on the curriculum, course and degree requirements, nature of faculty/student interaction, assumptions about technology competence and skills, technical equipment requirements, learning management system, availability of academic support services and financial aid resources, and costs and payment policies.**

The **M.S. in Construction Cybersecurity** program will provide students with clear, complete, and timely information on the curriculum, course and degree requirements, nature of faculty/student interaction, assumptions about technology competence and skills, technical equipment requirements, Learning Management System, availability of academic support services and financial aid resources, and costs and payment policies.

Curriculum, course, and degree information will be available on the University website and via e-

mail as well as regular mail (by request). The expectations on faculty/student interaction are available to students during virtual open house events, literature, website, etc. In addition, this information is part of the material distributed for each course. Students receive guidance on proper behavior/interaction with professors, in the on-ground classroom, and in the online environment to facilitate a high-level learning experience. Technology competence and skills and technical equipment requirements are part of the material distributed for each course. The technical equipment requirements are also listed on our website and provided to students in the welcome package.

The University's academic support services, financial aid resources, costs and payment policies, Learning Management System, are covered in the University Open Houses, application process, Welcome Aboard process, Orientation, Student Town Halls, and individual counseling.

7. **Provide assurance and any appropriate evidence that advertising, recruiting, and admissions materials will clearly and accurately represent the proposed program and the services available.**

   The **M.S. in Construction Cybersecurity** program's advertising, recruiting, and admissions materials will clearly and accurately represent the proposed program and the services available. The material for every new degree program is derived from the new program proposal approved by the Maryland Higher Education Commission.

H. Adequacy of articulation:

1. **If applicable, discuss how the program supports articulation with programs at partner institutions.**

   This program does not have articulation partners currently. However, it is expected that articulation for the program will work as it does for the University's current degrees. The University is very active with its transfer partners throughout the state and beyond. The goal of the University is to work with partners to make transfer as seamless as possible and to maximize the number transfer credits (as allowable). There are dedicated transfer student personnel to guide this process.

I. Adequacy of faculty resources (as outlined in COMAR 13B.02.03.11):

1. **Provide a brief narrative demonstrating the quality of the program faculty. Include a summary list of faculty members with appointment type, terminal degree title and field, academic title/rank, status (full-time, part-time, adjunct) and the course(s) each faculty member will teach.**

   All faculty listed below have been engaged with the University for at least several years. Dr. Antunes, Dr. Bajracharya, Dr. Bajwa, Dr. Baker, Dr. Butler, Dr. Sims, and Prof. Hanson are fulltime faculty members. Seven of the eight faculty members hold terminal degrees. One is professionally qualified. The University has reviewed the resumes and curriculum vitae of all faculty and each one is deemed professionally qualified to teach their courses at this level. The University leadership is confident in the quality of the faculty and their abilities to provide a learning environment supportive of the University goals for student success. Additional doctorally-qualified faculty will be added as needed.

Instructors who will be engaged with the **M.S. in Construction Cybersecurity** are:

INSTRUCTOR	BACKGROUND	COURSES ALIGNED TO BE TAUGHT
Dr. Alex "Sandy" Antunes Full time	Ph.D. Computational Sciences and Informatics M.S. Astronomy B.S. Astronomy	All CS Courses
Dr. Chandra Bajracharya Full time	Ph.D. Electrical and Computer Engineering M.S. Applied Computing M.S. Electrical Power Engineering B.E. Electrical Engineering	All CS courses
Dr. Garima Bajwa Full time	Ph.D. Computer Science and Engineering M.S. Electrical and Computer Engineering B.S. Electronics and Communication Engineering	All CS courses
Dr. Richard Baker Full time	Ph.D. Information Systems M.S. Computer Science B.S. Mathematics F-4 Pilot	All CS and CM courses
Dr. William Butler Full-time	D.Sc. Cyber Security M.S. Strategic Studies B.S. Computer Science NSTISSI No. 4011 CNSSI No. 4012 NSTISSI No. 4015 CNSSI No. 4016	All CS courses, IAE courses, and CM-600 series courses
Dr. Jami Carroll Adjunct	D.Sc. Cyber Security M.S. Cyber Security M.B.A.	All IAE Courses
Prof. Rick Hanson Full time	Professionally Qualified M.S. Computer Science B.S. Electrical Engineering	All IAE, CS courses, and CM-600 series courses
Dr. Bradford Sims Full time	Ph.D. Curriculum Instruction Design M.S. Building Construction Management B.S. Building Construction Technology	CM-700

Additional doctoral-qualified faculty will be added in the near future.

ADDITIONAL JUSTIFICATION:

Capitol Technology University's instructors are leading experts in the construction and cybersecurity fields:

1. Dr. William Butler, Chair, Cyber and Information Security, Director, Critical Infrastructures and Cyber Protection Center (CICPC). Dr. Butler is currently Director, Critical Infrastructures and Cyber Protection Center (CICPC) at Capitol Technology University. Prior to this appointment in 2013 Bill worked in the networking and IT industries as a network engineer and consultant for over 20 years. Bill also served as a joint qualified communications information systems officer in the U.S. Marine Corps and retired as a Colonel with 30 years of service (active and reserve). Bill holds a Doctorate in cybersecurity earned from Capitol focusing on preserving cellphone privacy and countering illegal cell towers (IMSI catchers).

2. Dr. Sims has extensive experience in Construction Science and the construction industry. He worked for ten years for multiple construction companies before moving into academia. He founded an online construction education company. He served as the faculty founder and Department Chair for the Construction Management program at Western Carolina University. He was the Assistant Secretary General of the International Council for Research and Innovation in Building and Construction. During his career, he has also served as a professor of construction management at the University of Florida and visiting professor of building construction management at Purdue University.

3. Dr. Baker has significant senior management experience in the construction industry. Dr. Baker served for six years as a Senior Director for Information Technology at Turner Construction Company – one of the largest construction companies in the United States and a wholly owned subsidiary of HOCHTIEF AG, Germany. HOCHTIEF AG, Germany is of the five largest construction companies in the world. Dr. Baker was responsible for strategy development, risk management, major benchmarking, and data mining at Turner Construction Company. During his distinguished follow-on career in academia, he has also served as the instructor for eight construction courses at Indiana State University.

4. Prof. Rick Hanson is the President of APS GLOBAL LLC. His company works on leading projects and programs to address cybersecurity and technology challenges. He has worked with large organizations and startups that require creative thinking and innovation to meet challenges. His accomplishments include cybersecurity consulting for vulnerability assessment, cybersecurity architecture, and key management for new and upgraded DoD IoT systems and communications and control (C2) networks, and has managed and served as technical lead for $29M in contracts for DOD Technology Modernization for medical operations and research. Prof. Hanson is an expert in Technology Evaluation and Development, Cybersecurity & Information Assurance, research, and program management. He has served as Clinical Program Manager and Information Security Lead (Cyber/IA) for technology development for the U.S. Air Force and the National Institutes of Health.

2. Demonstrate how the institution will provide ongoing pedagogy training for faculty in evidenced-based best practices, including training in:

a) Pedagogy that Meets the Needs of the Students

The primary pedagogy for faculty at Capitol Technology University is the Active Learning

model. The University believes strongly in a highly-interactive, thinking, and hands-on experience for students in each class to the maximum extent possible.

> It was two Missouri State professors, historian Charles Bonwell and psychologist James Eison, who coined the term "active learning." In their 1991 book on the subject, Active Learning: Creating Excitement in the Classroom, they offered this definition of the concept: "active learning involves students in doing things and thinking about the things they are doing."
>
> The definition, though it seems circuitous, marks a definitive pedagogical shift in college teaching and learning. Rather than think about what they are watching, hearing, or reading, students are first encouraged to be "doing" something in class, and then to apply critical thought and reflection to their own classroom work and activity. Their argument was backed up by research. Even Bligh, 20 years earlier, had pointed out that the immediate rehearsal of new information and knowledge had a significant impact upon learning.
>
> This approach is as helpful in the sciences as it is in the arts or humanities: whether it's organic chemistry, creative writing, or behavioral economics, concepts are all best understood through repeated practice and open, social exploration. The central tenet of active learning is that practice matters, and that classroom time is better spent giving students opportunities to work with concepts over and over, in a variety of ways and with opportunities.
>
> The central tenet of active learning — that practice and interaction matters— can be applied across disciplines for immediate feedback, so that knowledge can take hold in their own minds.
>
> (Source: Preville, P. Active Learning: The Perfect Pedagogy for the Digital Classroom: An Essential Guide for the Modern Professor)

All faculty receive regular periodic and recurring pedagogical training during the academic year. Those training sessions occur in a hybrid format – simultaneously live online and live on-ground in the classroom. The sessions are designed to reach all faculty, both fulltime and adjunct, in order to ensure all members receive the training. Additionally, the sessions are recorded for faculty who are unable to attend the live training session due to other professional commitments and who are teaching classes.

b) The Learning Management System

The Department of Online Learning and the instructional technology division support the online program needs of faculty and students. Those University organizations and the IT Help Desk provide constant and on-going support to the faculty. The Canvas is the University's online Learning Management System. Canvas is paired with Zoom – an enterprise video conferencing system with real-time messaging and content sharing. When a new faculty member is assigned to teach an online course, the Department of Online Learning provides formal training for that instructor. New faculty are assigned an experienced faculty mentor to ensure a smooth transition to the online environment as well as to ensure compliance with the University's online teaching

pedagogy. The University believes this approach provides the highest-level learning experience for the faculty member and, in turn, students attending online classes.

c) Evidenced-based Best Practices for Distance Education, if Distance Education is Offered.

Faculty at Capitol Technology University receive training in Keller's ARCS Motivational Model and his associated strategies for distance education/online learning.

> A model used in online delivery of teaching and learning to increase learner motivation is the Keller's ARCS motivational model. This model has been considered an important element in online education because of its implications on increased learner motivation and learning outcomes. The Keller's model consists of motivating students by maintaining and eliciting attention (A), such as virtual clinical simulations; making the content and format relevant (R), by modeling enthusiasm or relating content to future use; facilitating student confidence (C), by providing "just the right challenge"; and promoting learner satisfaction (S), by providing reinforcement and praise when appropriate. Examples of the Keller's model include increasing motivation including the arousal of curiosity of students, making the connection between learning objectives and future learning goals, autonomous thinking and learning, and fostering student satisfaction. Keller's ARCS model has been researched by various educational online programs to analyze student motivation and learning outcomes. The Keller's model serves as an example and guide for instructors to motivate and increase online engagement with their students as wells as research purposes.
>
> A qualitative study by Chan Lin investigated online student learning and motivation. Discussion boards, student projects, and reflection data were collected and analyzed from a 12-week web-based course. Respondents indicated the importance of online feedback from the instructor and peer modeling of course tasks to visualize learning progress. The study revealed using Keller's ARCS strategies fosters greater student online engagement by fostering self-efficacy and a sense of accomplishment.
>
> In a mixed method study, assessing the use of Keller's ARCS on instructional design, the use of educational scaffolding fostered positive levels of student motivation. Relevancy, attention, confidence, and satisfaction were all common factors associated with student success in the course and course completion.
>
> (Source: Pinchevsky-Font T, Dunbar S. Best Practices for Online Teaching and Learning in Health Care Related Programs. The Internet Journal of Allied Health Sciences and Practice. January 2015. Volume 13 Number 1.)

All faculty receive regular periodic and recurring training on evidence-based practices for distance education/online learning during the academic year. Those training sessions occur in a hybrid format – simultaneously live online and live on-ground in the classroom. The sessions are designed to reach all faculty, both fulltime and adjunct, to ensure all members receive the training. Additionally, the sessions are recorded for those faculty who are unable to attend the live training session due to other professional commitments or who are teaching classes at the training delivery time.

J. Adequacy of Library Resources (as outlined in COMAR 13B.02.03.12):

1. **Describe the library resources available and/or the measures to be taken to ensure resources are adequate to support the proposed program. If the program is to be implemented within existing institutional resources, include a supportive statement by the President for library resources to meet the program's needs.**

   Library Services: The Puente Library offers extensive services and a wide collection for Capitol Technology University students to be academically successful. Library resources are available digitally. The library also provides a mailing service for materials borrowed through the Maryland system. The library is currently supporting the following degrees at the undergraduate level: B.S. in Astronautical Engineering, B.S. in Business Analytics and Data Sciences, B.S. in Computer Engineering, B.S. in Computer Engineering Technology, B.S. in Computer Science, B.S. in Construction Management and Critical Infrastructure, B.S. in Cyber Analytics, B.S. in Cybersecurity, B.S. in Electrical Engineering, B.S. in Electrical Engineering Technology, B.S. in Engineering Technology, B.S. in Facilities Management and Critical Infrastructure, B.S in Management of Cyber and Information Technology, B.S. in Mechatronics Engineering, B.S. in Mechatronics and Robotics Engineering Technology, B.S. in Mobile Computing, B.S. in Software Engineering, and B.S. in Technology and Business Management, and B.S in Unmanned and Autonomous Systems. The library is currently supporting the following degrees at the graduate level: M.S. in Aviation, M.S. in Aviation Cybersecurity, M.S. in Computer Science, M.S. in Critical Infrastructure, M.S. in Cyber Analytics, M.S. in Cybersecurity, M.S. in Engineering Technology, M.S. in Information Systems Management, M.S. in Internet Engineering, M.S. in Unmanned and Autonomous Systems Policy and Risk Management, M.B.A., T.M.B.A. Business Analytics and Data Science, T.M.B.A. in Cybersecurity, D.Sc. in Cybersecurity, Ph.D. in Aviation, Ph.D. in Business Analytics and Decision Sciences, Ph.D. in Critical Infrastructure, Ph.D. in Manufacturing, Ph.D. in Product Management, Ph.D. in Technology, Ph.D. in Technology/M.S. in Research Methods Combination Program, and Ph.D. in Unmanned Systems Applications. Therefore, the library is fully prepared to support a **M.S. in Construction Cybersecurity**.

   Services provided to online students include:

   - "Ask the Librarian"
   - Research Guides
   - Tutorials
   - Videos
   - Online borrowing

   The John G. and Beverley A. Puente Library provides access to management, decision science, and research methods materials through its 10,000-title book collection, e-books, and its 90 journal subscriptions. The library will continue to purchase new and additional materials in the management, decision science, and research methods area to maintain a strong and current collection in this subject area. Students can also access materials through the library's participation in Maryland's Digital eLibrary Consortium. This online electronic service provides access to numerous databases (Access Science, NetLibrary) that supply students with the materials they need. Available databases include ProQuest, EBSCO, ACM, Lexis Nexis, Taylor Francis, and Sage Publications.

The Puente Library can provide access to historical management and decision science materials through its membership in the Maryland Independent College and University Association (MICUA) and the American Society of Engineering Education (ASEE). Reciprocal loan agreements with fellow members of these organizations provide the library access to numerous research facilities that house and maintain archives of management and decision science documents. The proximity of the University of Maryland, College Park and other local area research and academic libraries provide the Puente Library with quick access to these materials as well.

The library currently supports the needs students at the undergraduate, masters and doctoral levels.

K. Adequacy of Physical Facilities, Infrastructure and Instructional Equipment (as outlined in COMAR 13B.02.03.13):

1. **Provide an assurance that the physical facilities, infrastructure and instruction equipment are adequate to initiate the program, particularly as related to spaces for classrooms, staff and faculty offices, and laboratories for studies in the technologies and sciences. If the program is to be implemented within existing institutional resources, include a supportive statement by the President regarding adequate equipment and facilities to meet the program's needs.**

   No new facilities are required for the program. The online class platform is web based and requires no additional equipment for the institution. The current Learning Management System, Canvas and Zoom, meets the needs of the degree program. The Business and Technology lab, Computer Science Lab, Cyber Lab, Robotics Lab, and Unmanned Systems Lab together meet the potential research needs of the students. The labs provide both local and virtual support.

2. **Provide assurance and any appropriate evidence that the institution will ensure students enrolled in and faculty teaching in distance education will have adequate access to:**

   a) An institutional electronic mailing system

   Capitol Technology University provides an institutional electronic mailing system to all students and faculty. The capability is provided to all students and faculty in all the institution's modalities of course delivery. Capitol Technology University students and faculty are required to use the institution's email addresses (e.g., xxxxxxxx@captechu.edu) in all University matters and communications. The University uses the email capabilities in Microsoft Office 365 and Microsoft Outlook.

   b) A learning management system that provides the necessary technological support for distance education

   Capitol Technology University provides a robust Learning Management Systems (LMS) through the use of the Canvas LMS by Instructure (www.canvaslms.com). The University pairs Canvas with Zoom (zoom.us) to provide a platform for every student and faculty member to meet face-to-face in a synchronous "live" mode of communication. The use of Canvas is required for every course offered at the University; as a result, every course has a classroom on Canvas and Zoom.

All syllabi, grades, and assignments must be entered in to Canvas on a timely basis throughout the semester.

Canvas provides the world's most robust LMS. It is a 21st Century LMS; Canvas is a native cloud, Amazon Web Service hosted system. The system is adaptable, reliable, and customizable. Canvas is easy to use for students and faculty. The system is fully mobile and has proven to be timesaving when compared to other systems. The following list provides the features of the system:

Time and Effort Savings

- CANVAS DATA
  Canvas Data parses and aggregates more than 280 million rows of Canvas usage data generated daily.
- CANVAS COMMONS
  Canvas Commons makes sharing a whole lot easier.
- SPEEDGRADER ANNOTATIONS
  Preview student submissions and provide feedback all in one frame.
- GRAPHIC ANALYTICS REPORTING ENGINE
  Canvas Analytics help you turn rich learner data into meaningful insights to improve teaching and learning.
- INTEGRATED MEDIA RECORDER
  Record audio and video messages within Canvas.
- OUTCOMES
  Connect each learning outcome to a specific goal, so results are demonstrated in clearly measurable ways.
- MOBILE ANNOTATION
  Open, annotate, and submit assignments directly within the Canvas mobile app.
- AUTOMATED TASKS
  Course management is fast and easy with automated tasks.
- NOTIFICATION PREFERENCES
  Receive course updates when and where you want - by email, text message, even Twitter or LinkedIn.
- EASE OF USE
  A familiar, intuitive interface means most users already have the skills they need to navigate, learn, and use Canvas.
- IOS AND ANDROID
  Engage students in learning anytime, anywhere from any computer or mobile device with a Web-standard browser.
- USER-CUSTOMIZABLE NAVIGATION
  Canvas intelligently adds course navigation links as teachers create courses.

- RSS SUPPORT
  Pull feeds from external sites into courses and push out secure feeds for all course activities.

- DOWNLOAD AND UPLOAD FILES
  Work in Canvas or work offline—it's up to you.

- SPEEDGRADER
  Grade assignments in half the time.

Student Engagement

- ROBUST COURSE NOTIFICATIONS
  Receive course updates when and where you want—by email, text message, and even Facebook.

- PROFILE
  Introduce yourself to classmates with a Canvas profile.

- AUDIO AND VIDEO MESSAGES
  Give better feedback and help students feel more connected with audio and video messages.

- MULTIMEDIA INTEGRATIONS
  Insert audio, video, text, images, and more at every learning contact point.

- EMPOWER GROUPS WITH COLLABORATIVE WORKSPACES
  By using the right technologies in the right ways, Canvas makes working together easier than ever.

- MOBILE
  Engage students in learning anytime, anywhere from iOS or Android, or any mobile device with a Web-standard browser.

- TURN STUDENTS INTO CREATORS
  Students can create and share audio, video, and more within assignments, discussions, and collaborative workspaces.

- WEB CONFERENCING
  Engage in synchronous online communication.

- OPEN API
  With its open API, Canvas easily integrates with your IT ecosystem.

- BROWSER SUPPORT
  Connect to Canvas from any Web-standard browser.

- LTI INTEGRATIONS
  Use the tools you want with LTI integrations.

- MODERN WEB STANDARDS
  Canvas is built using the same Web technologies that power sites like Google, Facebook, and Twitter.

Lossless Learning

- CANVAS POLLS
  Gauge comprehension and incorporate formative assessment without the need for "clicker" devices.
- MAGICMARKER
  Track in real-time how students are performing and demonstrating their learning.
- QUIZ STATS
  Analyze and improve individual assessments and quiz questions.
- LEARNING MASTERY FOR STUDENTS
  Empower students to take control of their learning.

(Source: https://www.canvaslms.com/higher-education/features)

Capitol Technology University has been using Canvas for over four years. Canvas has proven to be a completely reliable LMS system that provides the necessary technological support for distance education/online learning.

L. Adequacy of financial resources with documentation (as outlined in COMAR 13B.02.03.14):

1. **Table 1: Resources. Finance data for the first five years of the program implementation.**

TABLE 1: RESOURCES

Resource Categories	Year 1	Year 2	Year3	Year 4	Year 5
1. Reallocation Funds	$0	$0	$0	$0	$0
2. Tuition/Fee Revenue (c + g)	$211,356	$421,578	$619,146	$813,960	$1,006,632
a. Number of F/T Students	0	0	0	0	0
b. Annual tuition/Fee rate	$0	$0	$0	$0	$0
c. Total F/T Revenue (a x b)	$0	$0	$0	$0	$0
d. Number of P/T Students	19	37	53	68	82
e. Credit Hour Rate	$618	$633	$649	$665	$682
f. Annual Credit Hour	18	18	18	18	18
g. Total P/T Revenue (d x e x f)	$211,356	$421,578	$619,146	$813,960	$1,006,632
3. Grants, Contracts and Other External Sources	0	0	0	0	0
4. Other Sources	0	0	0	0	0
TOTAL (Add 1 – 4)	$211,356	$421,578	$619,146	$813,960	$1,006,632

A. **Provide a narrative rationale for each of the resource categories. If resources have been or will be reallocated to support the proposed program, briefly discuss those funds.**

1. **Reallocated Funds**

   The University will not need to reallocate funds for the program.

2. **Tuition and Fee Revenue**

   Tuition is calculated to include an annual 2.5% tuition increase. A 20% attrition rate has been calculated.

3. Grants and Contracts

There are currently no grants or contracts.

4. Other Sources

There are currently no other sources of funds.

5. Total Year

No additional explanation or comments needed.

2. Table 2: Program Expenditures. Finance data for the first five years of program implementation.

TABLE 2: EXPENDITURES

Expenditure Category	Year 1	Year 2	Year 3	Year 4	Year 5
1. Faculty (b + c below)	$144,000	$184,500	$226,937	$310,147	$397,374
a. #FTE	2	2.5	3	4	5
b. Total Salary	$120,000	$153,750	$189,114	$258,456	$331,145
c. Total Benefits (20% of salaries)	$24,000	$30,750	$37,823	$51,691	$66,229
2. Admin Staff (b + c below)	$4,942	$5,090	$5,243	$5,374	$6,464
a. #FTE	.07	.07	.07	.07	.07
b. Total Salary	$4,084	$4,207	$4,333	$4,441	$5,508
c. Total Benefits	$858	$883	$910	$933	$956
3. Support Staff (b + c below)	$57,475	$87,638	$119,772	$153,460	$188,755
a. #FTE	1.00	1.5	2	2.5	3
b. Total Salary	$47,500	$73,032	$99,810	$127,883	$157,296
c. Total Benefits	$9,975	$14,606	$19,962	$25,577	$31,459
4. Technical Support and Equipment	$1,140	$2,405	$3,710	$5,100	$6,560
5. Library	$0	$0	$0	$0	$0
6. New or Renovated Space	$0	$0	$0	$0	$0
7.Other Expenses	$3,610	$10,730	$20,670	$33,320	$48,380
TOTAL (ADD 1-7)	$211,167	$290,363	$376,332	$507,401	$647,533

1. Provide a narrative rationale for each expenditure category. If expenditures have been or will be reallocated to support the proposed program, briefly discuss those funds.

a. Faculty

Table 2 reflects the faculty hours in total, but this does not imply that these are new hire requirements.

b. Administrative Staff

Capitol Technology University will continue with current the administrative staff through the proposed time period.

c. Support Staff

Capitol Technology University will add additional support staff to facilitate the program.

d. Equipment

Software for courses is available free to students or is freeware. Additional licenses for the LMS will be purchased by the University at the rate of $60 per student in Year 1. The rate is estimated to increase by $5 per year.

e. Library

Money has been allocated for additional materials to be added to the on campus and virtual libraries to ensure the literature remains current and relevant. However, it has been determined that the current material serves the needs of this degree due to the extensive online database.

f. New or Renovated Space

No new or renovated space is required.

g. Other Expenses

Funds have been allocated for office materials, travel, professional development, course development, marketing, and additional scholarships.

M. Adequacy of Provisions for Evaluation of Program (as outlined in COMAR 13B.02.03.15):

1. Discuss procedures for evaluating courses, faculty and student learning outcomes.

The assessment process at the University consists of a series of events throughout the Academic Year. The results of each event are gathered by the University Assessment Team and stored in Canvas for analysis and use in annual reports, assessments, etc. The University Assessment Team analyzes the results, develops any necessary action plans, and monitors implementation of the action plans.

Academic Year Assessment Events:

Fall Semester:

- At the August Faculty Retreat, the faculty reviews any outstanding student learning challenges that have not been adequately addressed. The issues are brought to the Academic Deans for review and development of implementation plans.
- Faculty submit performance plans consistent with the mission and goals of the University and department. The documents are reviewed and approved by the Academic Deans.

- Department Chairs and Academic Deans review the Graduating Student Survey data.
- Department Chairs and Academic Deans review student internship evaluations.
- Department Chairs and Academic Deans review grade distribution reports from the spring and summer semesters.
- Department Chairs and Academic Deans review student course evaluations from the Summer Semester.
- Departments conduct Industrial Advisory Board meetings to review academic curriculum recommendations. The Advisory Board meets to begin curriculum review or address special issues that may arise related to curriculum. Based on an analysis and evaluation of the results, the Academic Deans, faculty and the advisory boards will develop the most effective strategy to move the changes forward.

    - NOTE: A complete curriculum review for degrees occurs every 2 years. In most cases, the changes only require that the Academic Deans inform the University President and provide a report that includes a justification and the impact of the changes as well as a strategic plan. Significant changes normally require the approval of the Executive Council.

- The Academic Deans attend the Student Town Hall and review student feedback with Department Chairs.
- Department Chairs conduct interviews with potential employers at our Career Fair.
- Post-residency, the Academic Deans meet with the faculty to review the student learning progress and discuss needed changes.

Spring Semester:

- Faculty Performance Plans are reviewed with faculty to identify issues of divergence and to adjust the plan as needed.
- Department Chairs and Academic Deans review grade distribution reports from the Fall Semester.
- Department Chairs and Academic Deans review the Graduating Student Survey data.
- Department Chairs and Academic Deans review student course evaluations from the Fall Semester and the Spring Semester (in May before the Summer Semester begins).
- Department Chairs and Academic Deans meet to review the content of the graduating student, alumni, and course surveys to ensure the surveys continue to meet the university's assessment needs.
- At Annual Faculty Summit in May, the faculty review and discuss student learning challenges from the past academic year and provide recommendations to the Academic Deans for review and development of implementation plans.
- Department Chairs conduct interviews with potential employers at our Career Fair.
- Departments conduct Industrial Advisory Board meetings to review academic curriculum recommendations.

In addition to these summative assessments, the Academic Deans meet with the Department Chairs on a weekly basis to review current student progress. This formative assessment allows for immediate minor changes, which increase faculty effectiveness and, ultimately, student outcomes.

The Faculty Senate meets monthly during August through April. The Faculty Senate addresses issues that impact student outcomes as those issues emerge. The leadership of the Faculty Senate then provides a report on the matter to the Academic Deans. The report may include a

recommendation or a request to move forward with a committee to further examine the issue. In most cases, the changes only require the Academic Deans to inform the University President and provide a report that includes a justification and the impact of changes as well as a strategic plan. Significant changes normally require the approval of the Executive Council.

2. **Explain how the institution will evaluate the proposed program's educational effectiveness, including assessments of student learning outcomes, student retention, student and faculty satisfaction, and cost-effectiveness.**

Student Learning Outcomes:

Student learning outcomes for the proposed **M.S. in Construction Cybersecurity** will be measured using the instruments identified in Section G and Section M as well as the assigned rubrics and assessment measures (e.g., competency exams/projects, case study exams) dictated by the accreditation requirements of the University's regional accreditor [i.e., Middle States Commission in Higher Education (MSCHE)] and our degree specific accrediting organizations (i.e., IACBE, ABET, NSA, DHS). This program is designed to meet the requirements of MSCHE. The University will also use NSA/DHS National Centers of Academic Excellence (CAE) and its related assessment tools to assess student achievement of the learning outcomes in the program. The University is in good standing with all its accrediting bodies.

Student Retention:

The University maintains a comprehensive student retention program under the Vice President for Student Engagement. The program assesses student retention at all levels, including the individual course, major, and degree. During the semester and term, the University's Drop-Out Detective capability, within its Learning Management System (Canvas), provides an early alert at the course level to potential issues related to retention. Within the Office of Student Life, Academic Advisors monitor Drop-Out Detective and contact students who appear to have issues affecting their academic performance. The Academic Advisors work with each student to create a plan to remove any barriers to success. The Academic Advisors also work with the course instructors as needed to gain additional insight that may be helpful to correcting the situation.

Each student also meets with their Academic Advisor each semester to evaluate their progress toward degree completion. An updated plan of action is developed for each student for their next semester's registration and each succeeding semester through degree completion.

The Vice President for Student Engagement also meets on a regular basis with the Academic Deans to review the student retention within each degree program and address any issues that appear to be impediments to degree completion.

Student and Faculty Satisfaction:

Evaluations and assessment of Student and Faculty satisfaction occur every semester. Faculty members are evaluated every semester by students enrolled in their courses. Students are required to complete a course evaluation online within a specified time frame at the end of the semester for every enrolled course or they are locked out of Canvas (the University's Learning Management System) until they complete each survey. Every faculty member is also required to review each of their courses for the semester.

The Department Chairs and Academic Deans review the student evaluations for every course offered at the university. The Department Chairs and Academic Deans also review faculty satisfaction every semester. If changes are needed at the course level, the changes are developed and implemented by the faculty responsible for the courses upon approval of the Academic Deans. If changes are needed at the faculty level, the Department Chairs will make the changes. At the end of this cycle, an evaluation is repeated and the results are analyzed with the appropriate stakeholders regarding the effectiveness of the changes. This is an ongoing process

Cost Effectiveness:

Based on the year-long inputs, evaluations, and reviews described in Section M.1 from faculty, students, industry representatives, and Department Chairs, the University Academic Deans prepare the proposed academic budget for each program for the upcoming year. Budget increases are tied to intended student learning improvements and key strategic initiatives.

Each academic program is also monitored by the Interim Vice President for Finance and Administration throughout every semester and term for its cost effectiveness. Additionally, the revenue and costs of every University program are reviewed annually by the Executive Council and Board of Trustees prior to approving the next year's budget.

N. Consistency with the State's Minority Student Achievement goals (as outlined in COMAR 13B.02.03.05 and in the State Plan for Post-Secondary Education):

1. **Discuss how the proposed program addresses minority student access & success, and the institution's cultural diversity goals and initiatives.**

   Capitol Technology University is a majority/minority school. Our programs attract a diverse set of students who are multiethnic and multicultural. The University actively recruits minority populations for all undergraduate and graduate level degrees. Special attention is also provided to recruit females into the STEM and multidisciplinary programs at all degree levels – undergraduate, master's, and doctoral. The same attention will be given to the **M.S. in Construction Cybersecurity.**

O. Relationship to Low Productivity Programs Identified by the Commission:

1. **If the proposed program is directly related to an identified low productivity program, discuss how the fiscal resources (including faculty, administration, library resources and general operating expenses) may be redistributed to this program.**

   This program is not associated with a low productivity program identified by the commission.

P. Adequacy of Distance Education Programs (as outlined in COMAR 13B.02.03.22)

1. **Provide affirmation and any appropriate evidence that the institution is eligible to provide Distance Education.**

   Capitol Technology University is fully eligible to provide distance education. The University has a long history of providing high-quality distance education. The University is accredited regionally by the Middle States Commission in Higher Education (MSCHE) and through four

specialized accrediting organizations: International Accreditation Council of Business Education (IACBE), Accreditation Board for Engineering and Technology (ABET), NSA, and DHS. All five accrediting organizations have reviewed the University's distance education program as part of their accreditation process. Capitol Technology University is fully accredited by MSCHE, IACBE, ABET, NSA, and DHS. The University is in good standing with all its accrediting bodies.

2. **Provide assurance and any appropriate evidence that the institution complies with the C-RAC guidelines, particularly as it relates to the proposed program.**

   Capitol Technology University has a long history of providing high quality distance education/online learning that complies with the Council of Regional Accrediting Commissions (C-RAC) Interregional Guidelines for the Evaluation of Distance Education. The University will also continue to comply with the C-RAC guidelines with the proposed **M.S. in Construction Cybersecurity** program.

   a. **Council of Regional Accrediting Commissions (C-RAC) Interregional Guidelines for the Evaluation of Distance Education.**

      1. **Online learning is appropriate to the institution's mission and purposes.**

         Online learning is consistent with the institution's mission, purpose and history. Please refer to Section A of this proposal.

      2. **The institution's plans for developing, sustaining, and, if appropriate, expanding online learning offerings are integrated into its regular planning and evaluation processes.**

         All programs at the University – online, hybrid, and on-ground – are subject to the same regular planning, assessment, and evaluation processes. Please see Section M of this proposal for the detailed process.

      6. **Online learning is incorporated into the institution's systems of governance and academic oversight.**

         All programs at the University – online, hybrid, and on-ground – are subject to the same systems of governance and academic oversight. Please refer to Section G and Section M of this proposal.

      4. **Curricula for the institution's online learning offerings are coherent, cohesive, and comparable in academic rigor to programs offered in traditional instructional formats.**

         Online programs/courses meet the same accreditation standards, goals, objectives, and outcomes as traditional instruction at the University. The online course development process incorporated the Quality Matters research-based set of standards for quality online course design to ensure academic rigor of the online course is comparable to the traditionally offered course. The University Academic Dean, chairs, and faculty review curriculum annually. Courses are reviewed at the end of each term of course delivery. This process applies to online and traditional courses. In addition, advisory boards are

engaged in the monitoring of course quality to ensure quality standards are met regardless of the delivery platform.

5. **The institution evaluates the effectiveness of its online learning offerings, including the extent to which the online learning goals are achieved, and uses the results of its evaluations to enhance the attainment of the goals.**

   Online programs/courses meet the same accreditation standards, goal, objectives, and outcomes as traditional classroom delivery. Learning platforms are chosen to ensure high standards of the technical elements of the course. The University Academic Dean monitors any course conversion from in-class to online to ensure the online course is academically equivalent to traditionally offered course and that the technology is appropriate to support the expected rigor and breadth of the programs courses.

6. **Faculty responsible for delivering the online learning curricula and evaluating the students' success in achieving the online learning goals are appropriately qualified and effectively supported.**

   The Department of Cybersecurity, where this degree will be sponsored, is staffed by qualified teaching chair, and other appropriately credentialed faculty.

   The evaluation of programs and courses are done using the same process as all other programs at the University (please see Section M of this document). All Capitol Technology University faculty teach in the traditional classroom environment and online. (Please see qualifications in Section I of this document.)

7. **The institution provides effective student and academic services to support students enrolled in online learning offerings.**

   Students can receive assistance in using online learning technology via several avenues. Student aides are available to meet with students and provide tutoring support in both subject matter and use of the technology. Tutors are available in live real-time sessions using Zoom or other agreed upon tools. Pre-recorded online tutorials are also available.

   In addition to faculty support, on ground and online tutoring services are available to students in a one-on-one environment.

   Laboratories (on ground and virtual) are available for use by all students and are staffed by faculty and tutoring staff who provide academic support.

   Library services and resources are appropriate and adequate. Please refer to Section J of this document and the attached letter from the university president. The library adequately supports the students learning needs.

8. **The institution provides sufficient resources to support and, if appropriate, expand its online learning offerings.**

The University has made the financial commitment to the program (please refer to Section L). The University has a proven record of accomplishment in supporting degree completion.

9. The institution assures the integrity of its online offerings.

Current faculty serve on internal advisory boards that examine possible for program changes, including course and program development. All faculty are selected on domain expertise and program-related teaching experience.

When new faculty or outside consults are necessary for the design of courses offered, our Human Resource Department initiates a rigorous search and screening process to identify appropriate faculty to design and teach online courses. Again, all faculty are selected on domain expertise and program-related teaching experience

The University online platforms offer several avenues to support instructors engaged in online learning. The Director of our Online Learning Division is highly skilled and trained in faculty development. Several seminars and online tutorials are available to the faculty every year. Mentors are assigned to new faculty. Best practice sharing is facilitated through the Academic Deans, Department Chairs, and formal meetings.

The assessment for online learning classes/students is the same as for all academic programs at the University. Faculty provide required data on student achievement. The Learning Management System provides data on student achievement. Proof of these assessments is available during the class and post class to the Academic Deans and Department Chairs. On an annual basis, the information is reported to the University's accreditation authorities such as MSCHE and NSA/DHS.