Office Use Only: PP#

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

Payment Submitted: (●) Yes ( ) No Payment Type: ( ) R*STARS # 99982 (●) Check # 99982 Payment Amount: 850.00 Date Submitted: 4/1/2026

Department Proposing Program	Engineering
Degree Level and Degree Type	Bachelor of Science (B.S.)
Title of Proposed Program	Bachelor of Science in Cybersecurity Engineering
Total Number of Credits	120
Suggested Codes	HEGIS: 901.00 CIP: 14.0901
Program Modality	( ) On-campus ( ) Distance Education (fully online) (●) Both
Program Resources	(●) Using Existing Resources ( ) Requiring New Resources
Projected Implementation Date (must be 60 days from proposal submisison as per COMAR 13B.02.03.03)	(●) Fall ( ) Spring ( ) Summer Year: 2026
Provide Link to Most Recent Academic Catalog	URL: http://catalog.captechu.edu
Preferred Contact for this Proposal	Name: Dr. Mohamed Ghazy Title: Dean of Academics Phone: (340) 965-2473 Email: mshehata@captechu.edu
President/Chief Executive	Type Name: Dr. Bradford Sims Signature: [signature] Date: 4-1-26
	Date of Approval/Endorsement by Governing Board: APRIL 1, 2026

Revised 1/2021

CAPITOL
Technology University

April 1, 2026

Dr. Elena Quiroz-Livanis
Deputy Secretary of Maryland Higher Education
Maryland Higher Education Commission
217 E. Redwood Street, Suite 2100
Baltimore, MD 21202

Dear Dr. Quiroz-Livanis,

Capitol Technology University is requesting approval to offer a Bachelor of Science (B.S.) in Cybersecurity Engineering. This new degree program will be delivered by experienced faculty and supported by the University's existing instructional and laboratory infrastructure. It is designed to meet the growing workforce demand for engineers with expertise in secure systems design, network security, embedded systems protection, cyber-physical systems security, and critical infrastructure protection.

The B.S. in Cybersecurity Engineering aligns with Capitol Technology University's mission to provide a hands-on, career-focused education in science, technology, engineering, and mathematics. The program prepares students for immediate entry into professional roles in sectors such as cybersecurity engineering, defense systems, secure software development, network infrastructure protection, and critical infrastructure security. Students will gain practical experience through project-based learning, laboratory courses, and a senior design capstone sequence, ensuring readiness to contribute to Maryland's evolving cybersecurity and technology workforce.

Cybersecurity engineering is one of the fastest-growing and most strategically important engineering fields, and this program will help expand access to high-quality STEM education for students throughout the region. It is also structured to support transfer pathways, workforce development initiatives, and potential ABET Engineering Accreditation Commission (EAC) accreditation.

We respectfully submit the full proposal for the Bachelor of Science in Cybersecurity Engineering for your review and approval. Enclosed is the required documentation, including the letter confirming the adequacy of library resources to support this program.

Respectfully,

Bradford L. Sims, PhD

President

CAPITOL
Technology University

April 1, 2026

Dr. Elena Quiroz-Livanis
Deputy Secretary of Maryland Higher Education
Maryland Higher Education Commission
217 E. Redwood Street, Suite 2100
Baltimore, MD 21202

Dear Dr. Quiroz-Livanis
,

This letter is in response to the need for confirmation of the adequacy of the library of Capitol Technology University to support the proposed **Bachelor of Science in Cybersecurity Engineering**. As President of the University, I confirm that the library resources, including support staff, are more than adequate to support the **B.S. in Cybersecurity Engineering**. Additionally, the University remains dedicated and committed to the continuous improvement of its library resources by providing sufficient budget to ensure the success of our students.

Respectfully,

Bradford L. Sims, PhD
President

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 2026
Projected Implementation Date

Bachelor of Science
Award to be Offered

Bachelor of Science in Cybersecurity Engineering
Title of Proposed Program

0901
Suggested HEGIS Code

14.0901
Suggested CIP Code

Engineering
Department of Proposed Program

Dr. Mohamed Ghazy
Name of Department Head

Dr. Mohamed Ghazy
Dean of Academic

mshehata@captechu.edu
Contact E-Mail Address

(240) 965-2473
Contact Phone Number

4-1-26
Signature and Date

____ President/Chief Executive Approval

APRIL 1, 2026
Date

Date Endorsed/Approved by Governing Board

Bachelor of Science (B.S.) in Cybersecurity Engineering

Capitol Technology University
Laurel, Maryland

A. Centrality to Mission and Planning Priorities

1. Program description and alignment with institutional mission

The Bachelor of Science in Cybersecurity Engineering is a 120-credit undergraduate program designed to prepare students for professional careers in the design, protection, and management of secure computing systems, communication networks, and cyber-physical infrastructure. The program focuses on the engineering principles required to design resilient and secure digital systems that support modern technological environments including enterprise networks, industrial control systems, communication systems, embedded devices, and critical infrastructure platforms.

The curriculum provides a strong foundation in engineering fundamentals, computer science, and cybersecurity principles, followed by advanced study in computer architecture, digital systems, communication systems, network security, secure software engineering, machine learning applications in cybersecurity, and protection of cyber-physical infrastructure. Students learn to analyze vulnerabilities in hardware, software, and network environments and to design secure systems that address evolving cyber threats affecting government, defense, financial, and critical infrastructure sectors. Through project-based coursework and laboratory experiences, students gain hands-on experience using modern engineering and cybersecurity tools to analyze, test, and secure complex systems. The program culminates in a two-course senior design sequence in which students work in multidisciplinary teams to develop applied solutions addressing real-world cybersecurity engineering challenges.

In addition to the technical engineering core, the program includes coursework in mathematics and science (30 credits), general education in humanities, ethics, and business (18 credits), and computer science and programming (18 credits). This balanced curriculum ensures that graduates develop strong analytical, communication, and professional skills while maintaining a focus on engineering design, secure system development, and lifelong learning.

The program aligns with the mission of Capitol Technology University to educate individuals for professional opportunities in engineering, computer and information sciences, and business by providing relevant, practice-oriented learning experiences that lead to success in an evolving global community. The Bachelor of Science in Cybersecurity Engineering fulfills this mission by equipping graduates with the engineering expertise, technical knowledge, and professional readiness required to design and protect modern computing systems and digital infrastructure in an increasingly interconnected and threat-prone environment. The program also strengthens Capitol's leadership in STEM education by expanding its portfolio of engineering programs into the rapidly growing and strategically critical field of cybersecurity engineering.

The program supports the university's Strategic Vision 2025 by advancing the goals of technological innovation, digital security, and workforce development. It emphasizes applied, hands-on learning and

aligns with regional and national priorities related to cybersecurity resilience, digital infrastructure protection, and the secure operation of advanced computing systems.

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

The proposed Bachelor of Science in Cybersecurity Engineering directly supports Capitol Technology University's strategic goals of expanding STEM program offerings, fostering innovation, and strengthening alignment with industry and government workforce needs. The program was developed in response to increasing demand for engineers with specialized expertise in securing computing systems, networks, and cyber-physical infrastructure. It leverages Capitol's existing strengths in cybersecurity, computer science, electrical engineering, and systems engineering to deliver a focused and sustainable academic pathway without requiring significant new capital investment.

The program contributes to Goal I: Expand Educational Offerings and Increase Program Completion by introducing a specialized engineering degree that builds upon existing foundations in computer engineering, networking, and cybersecurity while addressing a clearly defined and growing workforce need. Its curriculum responds to student and employer demand for expertise in secure system design, network security, and protection of cyber-physical systems. The structure allows for future elective development in areas such as advanced cyber defense, embedded system security, artificial intelligence in cybersecurity, and critical infrastructure protection, providing flexibility and long-term curricular growth.

The program supports Goal II: Increase Enrollment and Institutional Awareness by attracting both traditional students and transfer students seeking careers in cybersecurity engineering, defense-related technology development, critical infrastructure protection, and secure computing systems design. The program's applied, career-oriented focus and alignment with national and regional cybersecurity priorities enhance Capitol's visibility as a provider of specialized, mission-driven engineering education.

The program advances Goal III: Improve Utilization of University Resources and Institutional Effectiveness by relying on existing faculty expertise, laboratories, and facilities already supporting related programs in cybersecurity, computer science, and engineering. The integration of shared foundational courses promotes instructional efficiency, interdisciplinary collaboration, and cost-effective program delivery.

Finally, the program contributes to Goal IV: Strengthen Industry and Community Partnerships by fostering connections with organizations involved in cybersecurity operations, secure software development, defense technology, financial technology systems, and critical infrastructure protection. These partnerships will support internships, senior design projects, applied research, and workforce engagement opportunities for students and faculty.

Evidence that this program is an institutional priority includes the following:

a. The program was developed under the direction of the Office of Academic Affairs and the Department of Engineering as part of a coordinated effort to expand Capitol's offerings in cybersecurity engineering and secure systems design.

b. The program concept was endorsed during academic planning retreats and Undergraduate Academic Council discussions as part of the university's long-term strategy to strengthen its engineering portfolio and address emerging cybersecurity workforce needs.

c. The curriculum was designed by faculty with expertise in cybersecurity, computer engineering, networking, and secure systems development, ensuring alignment with industry practices and engineering education standards.

d. The program leverages shared instructional resources and laboratories used for existing engineering and cybersecurity programs, demonstrating institutional efficiency and sustainability.

e. The development of this degree supports Capitol's strategic enrollment growth objectives by attracting transfer students, military-affiliated learners, and nontraditional students interested in cybersecurity engineering and secure systems design.

f. The program aligns with recent institutional initiatives to strengthen engagement with external partners, professional organizations, and employers operating in cybersecurity, defense technology, and critical infrastructure sectors.

3. Narrative of how the proposed program will be adequately funded for at least the first five years of implementation

The Bachelor of Science in Cybersecurity Engineering will be funded through existing university resources, tuition revenue, and strategic allocation of instructional capacity within the School of Engineering. The university's five-year financial projections confirm the program's sustainability, with conservative initial enrollment estimates followed by steady growth supported through targeted recruitment and established transfer pathways.

Most courses required for the program already exist within the Electrical Engineering, Computer Science, and Cybersecurity curricula, minimizing the need for new course development or significant capital expenditures. Existing laboratories supporting networking, digital systems, secure computing environments, and embedded systems are sufficient to meet program requirements. Instructional equipment such as networking hardware, FPGA platforms, microcontroller systems, and cybersecurity analysis tools are already available and maintained through the university's ongoing laboratory enhancement and renewal plans.

Faculty staffing will primarily draw from existing full-time and adjunct instructors with expertise in cybersecurity, computer engineering, networking, and systems engineering. As enrollment increases, additional adjunct faculty may be engaged to support specialized upper-level coursework related to cybersecurity engineering and secure system design. These instructional needs have been anticipated in academic planning and will be implemented as enrollment growth warrants.

The program is expected to generate sufficient tuition revenue to support instructional and administrative costs by leveraging shared resources and maintaining efficient faculty-to-student ratios. The university will also pursue external funding opportunities through partnerships with industry, government agencies, and organizations supporting workforce development in cybersecurity and digital infrastructure protection.

4. Description of the institution's commitment to program support and continuity

Capitol Technology University is fully committed to the long-term success and sustainability of the Bachelor of Science in Cybersecurity Engineering. The program has been incorporated into the

university's academic planning, budgeting, and resource allocation processes, ensuring continued administrative, financial, and technical support.

a) Ongoing administrative, financial, and technical support

The program will be administered by the School of Engineering under the supervision of the Department of Engineering, with support from the Office of Academic Affairs. Financial and technical support will be integrated into the university's operating budget and technology planning processes. The program will utilize existing laboratories, computing resources, and secure instructional environments, with upgrades scheduled as part of Capitol's regular equipment renewal cycle. Faculty will receive professional development support to maintain currency in cybersecurity engineering, secure systems design, and emerging digital technologies.

b) Continuation of the program to allow students to complete their degrees

Capitol Technology University is committed to maintaining the program for a sufficient duration to ensure that all enrolled students are able to complete their degree requirements. The university will ensure appropriate course sequencing, academic advising, and instructional staffing continuity for each student cohort. In the event of future program modification or restructuring, a formal teach-out plan will be implemented in accordance with institutional policy and accrediting body requirements to ensure minimal disruption to student progress.

The proposed Bachelor of Science in Cybersecurity Engineering reflects Capitol Technology University's mission-driven approach to providing career-relevant, industry-aligned engineering education. The program builds on existing institutional strengths, addresses state and national workforce needs related to cybersecurity and digital infrastructure protection, and advances the university's long-term goals of innovation, resilience, and academic excellence in engineering education.

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

a) The need for the advancement and evolution of knowledge

The Bachelor of Science in Cybersecurity Engineering addresses a growing and urgent need for advanced engineering knowledge related to the design, protection, and resilience of modern computing systems, communication networks, and cyber-physical infrastructure. Across Maryland and the nation, government agencies, defense organizations, financial institutions, and critical infrastructure sectors—including energy, transportation, healthcare, and communications—are increasingly dependent on interconnected digital systems that must operate securely in a highly networked and threat-prone environment.

This program advances engineering knowledge by integrating foundational principles of computer engineering, electrical engineering, and computer science with specialized study in secure system design, computer architecture, network security, secure software development, machine learning applications in cybersecurity, and protection of cyber-physical systems. Students gain the ability to analyze vulnerabilities across hardware, software, and network layers and to design resilient computing systems

capable of withstanding sophisticated cyber threats. The curriculum emphasizes engineering challenges unique to modern computing environments, including distributed system security, secure communication protocols, system integration, and the protection of large-scale digital infrastructure.

Graduates of the program will be prepared to contribute to innovation in areas such as secure system architecture, resilient network design, intelligent threat detection, and cyber-physical infrastructure protection. These capabilities address a critical gap that is not fully met by traditional computer science, electrical engineering, or cybersecurity programs that focus primarily on software development or cybersecurity operations rather than engineering the secure systems themselves.

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

The Cybersecurity Engineering program expands access to high-demand engineering education for a diverse population of learners, including community college transfer students, adult learners, military-affiliated students, and individuals from populations historically underrepresented in STEM fields. The program's interdisciplinary structure leverages existing courses and laboratory resources, enabling efficient delivery while maintaining affordability and academic rigor.

Capitol Technology University's emphasis on small class sizes, personalized advising, and hands-on learning supports an inclusive educational environment that promotes student persistence and success. The program is designed to accommodate flexible entry pathways through articulation agreements and prior learning opportunities, allowing students with backgrounds in computer science, information technology, engineering technology, or cybersecurity to transition into a bachelor's-level engineering degree. By focusing on the protection of computing systems, communication networks, and digital infrastructure that underpin modern society, the program appeals to students motivated by service, national security, and the protection of public and economic systems.

These features align with Maryland's goals of expanding equitable access to high-quality STEM education and strengthening the state's technology workforce. The program provides students from diverse backgrounds with opportunities to enter high-demand careers in cybersecurity engineering, secure systems design, and infrastructure protection.

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

Although Capitol Technology University is not a historically black institution, it maintains a strong commitment to collaboration with Maryland's historically black institutions (HBIs) and other minority-serving institutions. The Cybersecurity Engineering program provides opportunities for articulation, transfer pathways, and collaborative initiatives that expand access to specialized engineering education related to secure computing systems and digital infrastructure protection.

Capitol will pursue partnerships that support joint academic initiatives, faculty collaboration, and workforce development programs focused on cybersecurity engineering and secure system design. These partnerships may include articulation agreements, joint research activities, and cooperative workforce development initiatives addressing cybersecurity workforce shortages.

Such collaborations contribute to statewide efforts to increase diversity in cybersecurity and engineering fields. By serving as a complementary provider of specialized cybersecurity engineering education, the program supports Maryland's broader efforts to strengthen HBI capacity and increase participation by underrepresented populations in high-impact technical disciplines.

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

The Maryland State Plan for Postsecondary Education identifies three overarching goals: Student Access, Student Success, and Innovation. The proposed Bachelor of Science in Cybersecurity Engineering aligns directly with each of these goals by expanding access to specialized engineering education, promoting student achievement through applied learning, and supporting innovation in cybersecurity and digital infrastructure protection.

Goal 1: Student Access

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

Capitol Technology University is committed to expanding access to high-demand engineering disciplines that address emerging workforce needs. The Cybersecurity Engineering program was developed to serve students who may be underserved by traditional engineering or cybersecurity pathways, including transfer students, adult learners, and military-affiliated individuals. The curriculum supports seamless transition from community colleges offering programs in computer science, information technology, cybersecurity, and engineering technology. Through articulation agreements, financial aid initiatives, and targeted recruitment, the program reduces barriers to entry while expanding educational access for diverse student populations. These efforts directly support the State Plan's priorities related to affordability, equity, and workforce participation.

Goal 2: Student Success

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

The proposed program emphasizes experiential learning through laboratory instruction, programming projects, and engineering design activities that support engagement, retention, and academic achievement. Students' progress from foundational coursework in mathematics, programming, networking, and digital systems to advanced topics in cybersecurity engineering, secure software development, machine learning applications in cybersecurity, and protection of critical infrastructure systems. The two-course senior design sequence allows students to apply engineering principles to real-world cybersecurity challenges involving secure computing systems and digital infrastructure. Comprehensive academic support services, including faculty mentoring, advising, and tutoring, further reinforce student success and timely degree completion. These practices align with the State Plan's focus on educational quality, completion outcomes, and career readiness.

Goal 3: Innovation

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

The Cybersecurity Engineering program promotes innovation by integrating engineering education with emerging challenges in cybersecurity and digital infrastructure protection. Its focus on engineering secure computing systems represents a forward-looking response to evolving industry and government needs.

The program leverages existing laboratory infrastructure while incorporating modern cybersecurity analysis tools, simulation platforms, and system design technologies to deliver high-quality and cost-effective instruction. Students are trained to apply innovative engineering solutions to detect, prevent, and mitigate cyber threats affecting modern computing systems and networks.

In summary, the Bachelor of Science in Cybersecurity Engineering is consistent with the Maryland State Plan for Postsecondary Education by expanding access to specialized STEM education, promoting student success through applied and experiential learning, and fostering innovation in response to the State's cybersecurity workforce needs. The program prepares graduates to support the secure and resilient operation of computing systems and digital infrastructure that are essential to Maryland's economic vitality, public safety, and technological leadership.

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 for graduates of the proposed program

Graduates of the Bachelor of Science in Cybersecurity Engineering will be prepared for professional careers across Maryland's cybersecurity, technology, defense, and critical infrastructure sectors. The program addresses workforce needs in industries that rely on the secure operation of computing systems, communication networks, and cyber-physical infrastructure, including federal and state government agencies, defense contracting, financial services, healthcare systems, telecommunications, transportation systems, and technology companies.

Graduates will be qualified for entry-level engineering positions such as cybersecurity engineer, network security engineer, secure systems engineer, security software engineer, cyber-physical systems security engineer, and critical infrastructure security analyst. Additional employment opportunities include roles in secure system architecture, vulnerability analysis, infrastructure protection, and cybersecurity operations engineering. Employers include federal agencies, defense contractors, technology firms, cybersecurity consulting organizations, financial institutions, and infrastructure operators responsible for maintaining secure digital environments.

Typical entry-level employment for graduates will be at the assistant or junior engineer level, with opportunities for advancement to systems design, cybersecurity architecture, and project leadership roles as experience is gained or graduate study is completed. The program's emphasis on hands-on laboratories, programming assignments, system-level engineering design, and cybersecurity analysis ensures that graduates are prepared to contribute effectively within multidisciplinary teams responsible for protecting complex computing systems and digital infrastructure.

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

National and state labor market data demonstrate sustained and growing demand for cybersecurity and information security professionals. According to the U.S. Bureau of Labor Statistics (BLS, 2024),

employment of information security analysts is projected to grow by approximately 32 percent from 2023 to 2033, which is significantly faster than the average for all occupations. The BLS projects more than 16,000 openings annually in cybersecurity-related occupations due to both industry growth and workforce replacement needs. The median annual wage for information security analysts in 2024 was approximately $120,360, reflecting strong national demand for cybersecurity expertise.

In addition to information security roles, demand continues to grow for professionals with engineering expertise in secure systems, network defense, and cyber-physical infrastructure protection. The increasing integration of cloud computing, distributed networks, embedded systems, and automated infrastructure has created a need for engineers who can design secure architectures rather than simply manage security tools.

In Maryland, labor market projections reflect these national trends. The Maryland Department of Labor projects strong growth in computer and mathematical occupations, including cybersecurity-related roles, between 2022 and 2032. The state's proximity to federal agencies and defense organizations, including the National Security Agency, U.S. Cyber Command, and numerous Department of Defense contractors, creates a particularly strong regional demand for cybersecurity professionals with advanced technical expertise.

Maryland's cybersecurity workforce is concentrated in the Baltimore–Washington corridor, one of the largest cybersecurity employment hubs in the United States. Employers across the region—including federal agencies, defense contractors, technology firms, and financial institutions—report ongoing demand for professionals capable of securing networks, computing systems, and digital infrastructure. Job postings throughout the region consistently reference the need for cybersecurity engineers, network security specialists, and secure systems architects—roles that align directly with the competencies developed through the proposed program.

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 five years

Labor market analyses from federal, state, and industry sources confirm the growing need for professionals with expertise in cybersecurity engineering and secure system design. The Maryland Department of Labor's occupational projections identify sustained demand for cybersecurity professionals supporting government agencies, defense contractors, financial services institutions, and technology firms operating within the state.

National workforce reports addressing cybersecurity workforce shortages consistently identify significant gaps between the demand for cybersecurity professionals and the available supply of qualified graduates. Industry analysts note that many organizations face difficulty recruiting professionals who possess both cybersecurity knowledge and strong engineering or computing backgrounds necessary to design secure systems and networks.

Market analytics platforms such as Lightcast (2024) report tens of thousands of annual job postings nationwide for cybersecurity-related occupations, with a significant share located in the Mid-Atlantic region. Within Maryland, major employers posting cybersecurity positions include federal agencies, defense contractors, financial institutions, and technology companies. These postings frequently list skills

in network security, secure programming, digital system security, vulnerability analysis, and infrastructure protection—core components of the proposed curriculum.

Collectively, these data sources indicate a sustained and quantifiable demand for cybersecurity engineers and secure systems specialists over the next five years, validating the need for the proposed program.

4. Provide data showing the current and projected supply of prospective graduates

The current supply of graduates in Maryland with specialized preparation in cybersecurity engineering is limited. While several institutions offer programs in cybersecurity, computer science, or information technology, many of these programs emphasize cybersecurity operations, policy, or information assurance rather than engineering the secure systems themselves.

According to data from the Integrated Postsecondary Education Data System (IPEDS, 2022), Maryland institutions award several hundred bachelor's degrees annually in computer science, cybersecurity, and related fields. However, only a small portion of these programs integrate engineering coursework such as digital systems, computer architecture, communication systems, and systems engineering with cybersecurity education. As a result, there is a limited pipeline of graduates specifically trained in cybersecurity engineering and secure system design.

Based on institutional enrollment projections, the proposed program is expected to enroll approximately 15 to 20 students during its initial year of implementation, with enrollment increasing to approximately 60 to 70 students by the fifth year of operation. The program anticipates graduating approximately 10 to 15 students annually by year five, assuming standard retention and completion rates.

These graduates will contribute directly to Maryland's cybersecurity workforce, supporting organizations responsible for securing computing systems, communication networks, and critical digital infrastructure. By providing a specialized engineering-oriented curriculum focused on cybersecurity engineering, the Bachelor of Science in Cybersecurity Engineering will help address a documented workforce gap and establish a sustainable pipeline of professionals prepared to protect Maryland's digital and technological systems.

D. Reasonableness of Program Duplication

1. Identify Similar Programs in the State and/or Same Geographical Area

A comprehensive review of Maryland institutions was conducted using the Maryland Higher Education Commission (MHEC) Academic Program Inventory, CIP code searches, title-based searches, and institutional program listings. The review examined programs related to computer engineering, cybersecurity, and engineering disciplines with computing or systems focus.

a. Computer Engineering Programs (CIP 14.0901 / related classification)

The following institutions offer bachelor's degrees in Computer Engineering:

• Johns Hopkins University – Computer Engineering (B.S.)
• University of Maryland, Baltimore County – Computer Engineering (B.S.)
• University of Maryland, College Park – Computer Engineering (B.S.)

These programs provide strong foundations in digital systems, computer architecture, embedded systems, and hardware-software integration. While they include elements of system design and computing, cybersecurity is typically addressed as a supporting topic rather than a central engineering focus.

Distinction:
The proposed Cybersecurity Engineering program differs by placing cybersecurity at the core of the engineering design process. It integrates secure system architecture, hardware-level security, communication security, and cyber-physical system protection throughout the curriculum. Unlike traditional computer engineering programs, which emphasize performance and functionality, the proposed program emphasizes secure design, threat mitigation, and resilience of computing systems and infrastructure.

b. Cybersecurity and Information Assurance Programs (Title-Based Search)

The following institutions offer cybersecurity-related bachelor's programs:

• Coppin State University – Cybersecurity Engineering (B.S.)
• Frostburg State University – Cybersecurity and Information Assurance (B.S.)
• Morgan State University – Cybersecurity Intelligence Management (B.S.)
• Mount St. Mary's University – Cybersecurity (B.S.)
• SANS Technology Institute – Applied Cybersecurity (B.S.)
• Stevenson University – Cybersecurity & Digital Forensics (B.S.)
• University of Baltimore – Applied Information Technology (Cybersecurity concentration) (B.S.)
• University of Maryland Global Campus – Cybersecurity Technology; Cybersecurity Management and Policy (B.S.)

These programs focus primarily on cybersecurity operations, information assurance, digital forensics, cyber intelligence, and IT systems security. They prepare students for roles in network defense, security analysis, incident response, and cybersecurity management.

Distinction:
The proposed Cybersecurity Engineering program differs significantly in its engineering orientation. While Coppin State University offers a Cybersecurity Engineering program, its focus is primarily on applied cybersecurity and computing systems. In contrast, the proposed program integrates:

• Computer engineering and digital system design
• Secure hardware and embedded systems
• Secure communication and RF systems
• Industrial control systems and cyber-physical security
• Machine learning applications in cybersecurity
• Critical infrastructure protection

This approach emphasizes the **engineering design and development of secure systems**, rather than primarily the operation, monitoring, or management of cybersecurity environments.

c. Engineering Programs with Computing or Systems Focus

The following programs were identified with an engineering and computing focus:

• Bowie State University – Cyber Operations Engineering; Software Engineering (B.S.)
• Johns Hopkins University – Systems Engineering (B.S.)
• Morgan State University – Interdisciplinary Engineering (Information Systems) (B.S.)
• University of Maryland, Baltimore County – Engineering (Computer Engineering track) (B.S.)
• University of Maryland, College Park – Cyber-Physical Systems Engineering (B.S.)
• University of Maryland – Technology & Engineering Education / Engineering Technology (B.S.)

These programs provide interdisciplinary engineering education combining systems design, computing, and applied engineering principles. Some include elements of cybersecurity or cyber-physical systems, but cybersecurity is not consistently the central organizing theme of the curriculum.

Distinction:
The proposed Cybersecurity Engineering program is specifically structured around the **integration of cybersecurity with engineering design across computing systems and infrastructure**. It uniquely combines:

• Secure digital and embedded system design
• Network and communication security engineering
• Cyber-physical and industrial system protection
• Infrastructure resilience and systems-level security

This integrated focus distinguishes it from broader engineering programs, which typically emphasize general systems design or software development without a comprehensive cybersecurity engineering framework.

d. Summary of Duplication Analysis

The review confirms that while Maryland institutions offer programs in computer engineering, cybersecurity, and related engineering disciplines:

• No program provides a fully integrated **Cybersecurity Engineering curriculum centered on secure system design across hardware, software, networks, and infrastructure**
• Existing cybersecurity programs emphasize **operations, policy, and information assurance**, rather than engineering design
• Existing computer engineering programs emphasize **system performance and architecture**, with limited focus on security integration
• Interdisciplinary engineering programs do not provide a **dedicated cybersecurity engineering framework**

Although Coppin State University offers a program titled Cybersecurity Engineering, the proposed program at Capitol Technology University differs in its **depth of engineering integration, focus on cyber-physical and infrastructure systems, and emphasis on secure system design across multiple engineering domains**.

Accordingly, the proposed program **complements rather than duplicates** existing offerings and fills a distinct and unmet need within Maryland's higher education landscape.

2. Justification for the Proposed Program

a. Workforce Demand
Maryland's economy depends heavily on cybersecurity, defense, and technology sectors that require professionals capable of designing secure computing systems and infrastructure. The proposed program addresses the growing need for engineers who can integrate cybersecurity into system design at all levels.

b. Academic Need
The program bridges a gap between traditional computer engineering and cybersecurity programs by integrating secure system design, communication systems, embedded systems, and infrastructure protection into a unified engineering curriculum.

c. Accessibility and Flexibility
The program supports traditional students, transfer pathways, and non-traditional learners, leveraging existing institutional resources and providing a cost-effective pathway to a specialized engineering degree.

d. Institutional Alignment
The program aligns with Capitol Technology University's mission to deliver career-focused, applied engineering education in high-demand technical fields.

e. Strategic Differentiation
The proposed program is distinctive in its integration of:
• Computer engineering
• Cybersecurity
• Communication systems
• Cyber-physical systems
• Critical infrastructure protection

It therefore strengthens Maryland's capacity to educate engineers prepared to address modern cybersecurity challenges without duplicating existing academic programs.

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 proposed Bachelor of Science in Cybersecurity Engineering is designed to complement, rather than compete with, high-demand engineering, computing, and cybersecurity programs offered by Maryland's Historically Black Institutions (HBIs).

Maryland HBIs offering related programs include:
• Morgan State University – Bachelor of Science in Electrical Engineering and Bachelor of Science in Computer Engineering
• University of Maryland Eastern Shore – Bachelor of Science in Engineering

• Bowie State University – Bachelor of Science in Cyber Operations Engineering and related computing programs
• **Coppin State University – Bachelor of Science in Cybersecurity Engineering**

These programs provide broad preparation in electrical engineering, computer engineering, general engineering, and cybersecurity. They play an important role in Maryland's efforts to expand participation of underrepresented populations in STEM disciplines and are recognized as high-demand programs within the state.

The proposed Cybersecurity Engineering program is similar in title to Coppin State University's Cybersecurity Engineering program; however, it differs in scope, structure, and curricular emphasis. While Coppin State University's program focuses on cybersecurity technologies, applied computing, and workforce preparation in information security and cyber operations, the proposed program at Capitol Technology University emphasizes an engineering-based approach that integrates computer engineering, digital systems, communication systems, and cybersecurity within a unified curriculum.

While HBI engineering and cybersecurity programs provide strong foundational preparation in circuits, computing systems, cybersecurity operations, and information security, they do not typically offer a structured undergraduate curriculum specifically focused on the engineering design and protection of secure computing systems and digital infrastructure.

The Cybersecurity Engineering program emphasizes specialized areas including:
• Secure system architecture and digital system design
• Secure communication systems and network security engineering
• Machine learning applications in cybersecurity
• Industrial control systems security
• Secure RF communications and cyber-physical systems protection
• Critical infrastructure protection and resilience engineering

The program integrates computer engineering principles, cybersecurity technologies, and systems engineering approaches to address cybersecurity challenges affecting modern computing systems and infrastructure environments.

The proposed program is structured to serve traditional undergraduate students, community college transfers, military-affiliated learners, and working professionals seeking specialized engineering preparation in cybersecurity engineering and secure system design. Its applied engineering focus positions it as a complementary academic pathway rather than a substitute for existing HBI programs.

Rather than diverting students from HBIs, the proposed program has the potential to support and strengthen high-demand HBI programs in several ways:

1. By creating potential articulation or transfer pathways for students completing foundational coursework in engineering, computer science, or cybersecurity at HBI institutions who wish to pursue specialized preparation in cybersecurity engineering and secure systems design.
2. By enabling collaborative academic initiatives such as joint senior design projects, shared laboratory experiences, or applied research focused on cybersecurity engineering, infrastructure protection, and secure computing systems.

3. By expanding Maryland's overall capacity to educate engineers in cybersecurity and infrastructure protection fields, thereby supporting statewide workforce development goals without duplicating existing HBI offerings.

The introduction of the Cybersecurity Engineering program is not expected to negatively impact enrollment at Maryland HBIs. Instead, it broadens educational access and strengthens Maryland's STEM education ecosystem by addressing a specialized workforce need not currently met by existing HBI degree programs.

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 proposed Bachelor of Science in Cybersecurity Engineering is not expected to negatively affect the uniqueness, missions, or institutional identities of Maryland's Historically Black Institutions (HBIs). Rather, the program complements statewide efforts to expand access to high-quality, workforce-aligned engineering and cybersecurity education in fields critical to digital infrastructure protection, national security, and technological resilience.

Maryland's HBIs include:
• Morgan State University
• Bowie State University
• Coppin State University
• University of Maryland Eastern Shore

Among these institutions, relevant academic programs include:
• Electrical Engineering and Computer Engineering at Morgan State University
• Engineering at the University of Maryland Eastern Shore
• Cyber Operations Engineering and computing programs at Bowie State University
• **Cybersecurity Engineering at Coppin State University**

These programs play an important role in advancing diversity within engineering, cybersecurity, and computing professions and are central to Maryland's efforts to increase participation of underrepresented populations in STEM disciplines.

The proposed Cybersecurity Engineering program is similar in title to Coppin State University's Cybersecurity Engineering program; however, it differs in academic structure, emphasis, and integration of engineering and systems-level design. While Coppin State University's program focuses on cybersecurity technologies, applied computing, and workforce preparation in information security and cyber operations, the proposed program at Capitol Technology University emphasizes an engineering-oriented approach that integrates computer engineering, digital system design, communication systems, and cybersecurity within a unified framework.

The Cybersecurity Engineering curriculum emphasizes specialized areas including:
• Secure computing system architecture and digital system design
• Secure communication systems and network security engineering
• Machine learning applications in cybersecurity

• Industrial control systems security
• Secure RF communications and cyber-physical systems protection
• Critical infrastructure protection and resilience engineering

The program integrates computer engineering, cybersecurity technologies, and systems engineering to prepare graduates for roles requiring both engineering design and cybersecurity expertise. This engineering-focused approach distinguishes the program from existing cybersecurity and computing programs offered at HBIs, which primarily emphasize cybersecurity operations, information assurance, and applied computing.

The introduction of this program does not alter or diminish the institutional identities of Maryland's HBIs, whose missions emphasize leadership development, community engagement, and access to high-impact educational opportunities. Instead, the proposed degree strengthens Maryland's overall STEM education ecosystem by expanding specialized pathways aligned with emerging workforce demands.

Furthermore, the program creates potential opportunities for collaboration with HBIs through:

1. Articulation pathways for students completing foundational coursework in engineering, computer science, or cybersecurity at HBI institutions who may seek additional specialization in cybersecurity engineering and secure systems design.
2. Joint academic initiatives, including collaborative senior design projects or shared applied research activities focused on cybersecurity engineering, infrastructure protection, and secure computing systems.
3. Workforce development partnerships that benefit students across institutions and support Maryland's cybersecurity, defense, and technology sectors.

By reinforcing shared statewide goals of expanding minority participation in high-demand engineering and cybersecurity fields, the Bachelor of Science in Cybersecurity Engineering enhances—rather than diminishes—the distinct missions and identities of Maryland's HBIs. The program aligns with Maryland's commitment to equity, access, academic excellence, and workforce preparedness while addressing a specialized and evolving area of engineering education.

G. Adequacy of Curriculum Design, Program Modality, and Related Learning Outcomes

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

The Bachelor of Science in Cybersecurity Engineering was developed through an interdisciplinary planning process involving the School of Engineering, the Office of Academic Affairs, and input from external stakeholders in cybersecurity, secure systems engineering, networking, and critical infrastructure protection. The program was designed in response to documented workforce demand for engineers capable of designing, analyzing, and securing computing systems, networks, embedded systems, and cyber-physical infrastructures.

The program builds upon Capitol Technology University's established strengths in electrical engineering, computer engineering, cybersecurity, networking, and applied computing. It integrates foundational coursework in programming, digital systems, computer architecture, and communication systems with

newly developed specialized coursework in network security, secure software engineering, machine learning for cybersecurity, secure communications, and critical infrastructure protection. This approach ensures both curricular efficiency and academic depth while aligning with Engineering Accreditation Commission (EAC) of ABET standards for undergraduate engineering programs.

The program will be overseen by full-time faculty within the School of Engineering who possess expertise in cybersecurity, computer engineering, networking, secure software development, communication systems, and systems engineering. These faculty members hold doctoral degrees in engineering, cybersecurity, or closely related fields and bring a combination of academic scholarship, applied research, and industry experience. Instruction in selected upper-level or specialized courses may be supported by qualified adjunct faculty with professional backgrounds in cybersecurity engineering, network security, secure systems design, and critical infrastructure protection.

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

The program is delivered primarily in a traditional face-to-face modality, with a strong emphasis on laboratory instruction, hands-on experimentation, and project-based learning. Selected courses may be offered in hybrid or online formats to provide flexibility for transfer students, adult learners, or working professionals, while maintaining equivalent academic rigor and learning outcomes.

The curriculum integrates theoretical foundations, applied engineering practice, and systems-level problem-solving to ensure students develop both technical depth and interdisciplinary breadth in cybersecurity engineering, including secure system design, network security, and protection of cyber-physical and computing systems.

Educational Objectives

Graduates of the Cybersecurity Engineering program will:

1. Enter the workforce as competent and ethical engineers in cybersecurity engineering, secure systems design, network security, and protection of computing and cyber-physical systems.
2. Design, analyze, and implement secure and reliable solutions for computing systems, embedded systems, and networked infrastructures while addressing real-world constraints related to security, safety, performance, and resilience.
3. Collaborate effectively in multidisciplinary teams and communicate technical information clearly to both technical and non-technical audiences.
4. Engage in continuous professional development, certification, or graduate study to remain current in evolving cybersecurity technologies, secure system design practices, and emerging threats.

Learning Outcomes

Upon graduation, students will be able to:

1. Identify, formulate, and solve complex engineering problems by applying principles of engineering, science, and mathematics.
2. Apply engineering design to produce solutions that meet specified needs with consideration of cybersecurity requirements, public health, safety, and welfare, as well as global, cultural, social, environmental, and economic factors.

3. Communicate effectively with a range of audiences.
4. Recognize ethical and professional responsibilities in engineering situations and make informed judgments that consider the impact of engineering solutions in cybersecurity, global, economic, environmental, and societal contexts.
5. Function effectively on a team whose members together provide leadership, create a collaborative environment, establish goals, plan tasks, and meet objectives.
6. Develop and conduct appropriate experimentation, analyze and interpret data, and use engineering judgment to draw conclusions, including evaluation of secure systems and networks.
7. Acquire and apply new knowledge as needed, using appropriate learning strategies.

These learning outcomes are fully aligned with ABET Engineering Accreditation Commission (EAC) Student Outcomes 1–7 and support career readiness and lifelong learning in cybersecurity engineering and secure systems design

3. Explain how the institution will:

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

Assessment of student learning will be conducted using both direct and indirect measures. Direct assessment methods include examinations, laboratory reports, design assignments, system integration projects, and evaluations of senior design performance. Indirect assessment methods include student surveys, course evaluations, alumni feedback, and employer input.

Each course includes clearly defined course learning outcomes that are mapped to program-level learning outcomes and ABET criteria. Faculty use standardized rubrics to evaluate student performance, particularly in high-impact courses such as control systems, industrial automation, embedded systems, secure system design, and the two-course senior design sequence. Assessment results are reviewed annually to identify strengths, areas for improvement, and opportunities for curricular refinement.

The program chair prepares annual assessment summaries, which are reviewed by the School of Engineering and the Office of Academic Affairs as part of the university's continuous improvement process. Input from industry partners and the program advisory board is incorporated into curriculum review and enhancement.

b) Document student achievement of learning outcomes in the program

Capitol Technology University maintains a structured learning outcomes assessment system to document and track student achievement at both the course and program levels. Faculty collect and archive key assessment artifacts, including examinations, laboratory documentation, design reports, project deliverables, and capstone materials, on an annual basis.

These records are used to analyze trends in learning outcome attainment, support data-driven curricular decisions, and provide evidence for internal review and external accreditation processes. The documentation process ensures that graduates meet program educational objectives and demonstrate competencies consistent with ABET standards and industry expectations.

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

The Bachelor of Science in Cybersecurity Engineering program is a 120-credit undergraduate program designed to prepare students to design, analyze, and secure computing systems, networks, embedded systems, and cyber-physical infrastructures. The curriculum emphasizes a systems-oriented engineering approach and integrates foundational coursework in mathematics, programming, digital systems, computer architecture, and communication systems with advanced coursework in cybersecurity engineering, including network security, secure software engineering, machine learning applications in cybersecurity, secure communications, industrial control systems security, and critical infrastructure protection.

Program requirements are distributed across general education, mathematics and science, computer science core, engineering core, cybersecurity engineering core, and a two-course senior design capstone sequence. This structure ensures that graduates possess a strong engineering foundation, applied technical expertise, and the professional skills necessary to succeed in cybersecurity engineering and secure systems design roles.

Program Requirements Distribution

Category	**Description**	**Credits**
General Education	Courses in communication, humanities, ethics, and business that develop written communication, ethical reasoning, and professional management skills.	18
Mathematics and Science	Foundational coursework in mathematics and physics supporting engineering analysis, including calculus, linear algebra, differential equations, statistics, and physics.	30
Computer Science Core	Courses in programming, networking, data structures, and operating systems that provide computing foundations required for cybersecurity engineering.	18
Engineering Core	Fundamental engineering coursework covering circuits, digital electronics, computer architecture, signals and systems, communication systems, control systems, and systems engineering.	24
Cybersecurity Engineering Core	Specialized courses addressing cybersecurity engineering topics including information assurance, secure software engineering, network security, machine learning for cybersecurity, industrial control systems security, secure communications, and critical infrastructure protection.	24
Senior Design Capstone	Two-course senior design sequence involving team-based engineering projects addressing real-world cybersecurity engineering problems.	6
Total Program Credits		**120**

Bachelor of Science (B.S.) in Cybersecurity Engineering

Total Credits: 120

Course Number and Title	Credits	Prerequisites
1. General Education (18 Credits)		
EN 101 – English Communication I	3	Placement or admission requirement
EN 102 – English Communication II	3	EN 101
SS 351 – Ethics	3	EN 102
HU 331 – Arts and Ideas	3	EN 102
BUS 174 – Introduction to Business and Management	3	None
BUS 301 – Project Management	3	BUS 174
2. Mathematics and Science (30 Credits)		
MA 114 – Algebra and Trigonometry	4	MA 112 or placement
MA 261 – Calculus I	4	MA 114
MA 262 – Calculus II	4	MA 261
MA 330 – Linear Algebra	3	MA 262
MA 340 – Differential Equations	3	MA 262
MA 124 – Discrete Mathematics	3	MA 112, MA 114 or placement test score
MA 345 – Probability and Statistics for Engineers	3	MA 262
PH 201 – General Physics I	3	MA 114
PH 202 – General Physics II	3	PH 201
3. Computer Science Core (18 Credits)		
CS 120 – Introduction to Programming using Python	3	None
CS 150 – Programming in C	3	MA 111 or MA 112 and CS 120 or placement test
NT 150 – Computer Networking	3	None
CS 200 – Programming in C++	3	CS 130 or CS 150
CS 230 – Data Structures	3	CS 225 or CS 200, Co-requisite: MA 124
CT 152 – Introduction to UNIX	3	CS 120
4. Engineering Core (24 Credits)		
EL 100 – Introduction to DC/AC Circuits	3	MA 112
EL 204 – Digital Electronics	3	None
EE 304 – Digital Design	3	EL 204
CE 310 – Computer Architecture	3	EL 204
EE 406 – Signals and Systems	3	MA 262
EE 453 – Control I	3	MA 340
EE 340 – Systems Engineering	3	BUS 301
EL 261 – Introduction to Communication Circuits and Systems	3	EL 200, Co-requisite: MA 261
5. Cybersecurity Engineering Core (24 Credits)		
IAE 201 – Introduction to Information Assurance Concepts	3	MA 110 or MA 112 or MA 114 or MA 261
CSE 304 – Cyber Security in Logic Design and Digital Systems	3	EE 304

Course Number and Title	Credits	Prerequisites
CSE 341 – Machine Learning Applied to Cyber Security Engineering	3	IAE 201, CS 120, MA 330
CSE 411 – Secure Software Engineering	3	CS 120
CSE 310 – Network Security	3	NT 150, EL 204
CSE 421 – Industrial Control Systems Security	3	NT 150, EL 204
CSE 425 – Secure RF Communications	3	CS 150, NT 150, MA 124
CSE 430 – Critical Infrastructure Protection	3	EE 340
6. Senior Design Capstone (6 Credits)		
SDE 457 – Senior Design I	3	Senior Standing
SDE 458 – Senior Design II	3	SDE 457
Total Credits	**120**	

Courses Descriptions

1. General Education (18 Credits)

EN-101 – English Communications I (3 credits): This introductory college-level course focuses on effective oral and written communication skills and the development of analytical abilities through various reading and writing assignments. Students must demonstrate competence in writing mechanics, including grammar, sentence structure, logical content development, and research documentation through 4 essays/research papers. Rhetorical modes may include description, comparison/contrast, narrative, and process analysis. Students are expected to develop effective oral communication skills through speeches. Group projects will develop effective team skills such as decision-making, time management, and cooperation. Prerequisite(s): Acceptance based on placement test scores.

EN-102 – English Communications II (3 credits): This sequel to EN-101 involves more sophisticated reading, writing, speaking, and research assignments. Students must demonstrate competence in writing mechanics, as well as advanced research skills, the ability to handle complex information, and effective team skills. Students write research papers: an information paper, a cause-and-effect paper, an argument paper, and a final research paper. Course includes group work. Presentations are required. Prerequisite(s): EN 101

SS 351 – Ethics (3 credits): This course is designed to help students improve their ability to make ethical decisions. This is done by providing a framework that enables the student to identify, analyze, and resolve ethical issues that arise when making decisions. Case analysis is a primary tool of this course. Prerequisite(s): EN 102

HU 331 - Arts and Ideas (3 credits): This course enables students to study and appreciate various forms of art, including painting, sculpture, architecture, music, drama, film, and literature through in- class and on-site experiences. The arts are also surveyed from an historical perspective, focusing primarily on eras in Western civilization. This enables students to sense the parallel development of the arts, of philosophy, and of sociopolitical systems and to recognize various ways of viewing reality. Prerequisite(s): EN 102

BUS 174 - Introduction to Business and Management (3 credits): This course presents a survey of the general business and management environment. Topics include an introduction to the various forms of business, organizational structure, and their legal implications. Modern management and supervision concepts, history and development of theory and practice, the roles of managers, and the relationship between manager and employee are examined. This is a seminar course with emphasis on class discussion and collaborative learning

BUS 301 - Project Management (3 credits): This course is an introduction to project management. It covers the origins, philosophy, methodology, and involves actual applications and use of tools such as MS Project. The System Development Cycle is used as a framework to discuss project management in a variety of situations. Illustrative cases are used and project leadership and team building are covered as integral aspects of good project management. Prerequisite(s): BUS 101 or BUS 174

2. Mathematics and Science (30 Credits)

MA 114 - Algebra and Trigonometry (4 credits): Designed for students needing mathematical skills and concepts for MA-261. Topics in this course are as follows. Algebra: basic operations on real and complex numbers, fractions, exponents and radicals. Determinates: Solution of linear, fractional, quadratic and system equations. Trigonometry: definition and identities, angular measurements, solving triangles, vectors, graphs and logarithms. Prerequisite(s): MA 112 or placement test score.

MA 124 – Discrete Mathematics

MA 261 - Calculus I (4 credits): This course covers lines, circles, ellipses; functions and limits, differentiation, power rule, higher-order derivatives, product, quotient and chain rules, implicit differentiation, and applications. Regarding integration, it addresses definite integrals; indeterminate forms; exponential, logarithmic, trigonometric and hyperbolic functions; differentiation and integration, and graphing. Prerequisite(s): MA 114

MA 262 - Calculus II (4 credits): This course centers on methods of integration, including completing the square, substitution, partial fractions, integration by parts, trigonometric integrals, power series, and parametric equations. It also addresses partial derivatives, directional derivatives, and an introduction to multiple integrals. Prerequisite(s): MA 261

MA 330 - Linear Algebra (3 credits): This course introduces the study of linear systems of equations, vector spaces, and linear transformations. Students will solve systems of linear equations as a basic tool in many mathematical procedures used in science and engineering. Topics include solving linear equations, performing matrix algebra, calculating determinants, finding eigenvalues and eigenvectors and developing an understanding of a matrix as a linear transformation relative to a basis of a vector space. Prerequisite(s): MA 262.

MA 340 - Ordinary Differential Equations (3 credits): This course addresses methods for solving first order equations with applications to mechanics and rate problems. It also covers solutions of second order equations by undetermined coefficients and variations of parameters. Applications to circuits are also included as well as an introduction to systems of equations and operational and numerical methods. Prerequisite(s): MA 262

MA 345 – Probability & Statistics for Engineers (3 credits): This course focuses on sets and methods of counting, as well as probability density functions, expected values, and correlations. Forms of distribution addressed included binomial, Poisson, exponential, and normal. Additional topics covered include the central limit theorem, statistical estimation, an introduction to stochastic processes, and applications to noise and reliability. **Prerequisite(s):** MA 262

PH 201 - General Physics I (3 credits): This is a non-calculus-based physics course intended for credit in engineering technology courses. PH-261 is to be used for electrical, computer, and software engineering courses. PH-201 addresses mechanics, focusing on units, conversion factors, vector diagrams, translational equilibrium, friction, torque and rotational equilibrium, uniformly accelerated motion, projectiles, Newton's Law, work energy and power, kinetic and potential energy, conservation of energy, and impulse and momentum. It also addresses heat, focusing on temperature scales, thermal properties of matter, heat and temperature change, heat and change of phase, physics of heat transfer, and applications. Students completing this course may not enroll in PH-261 for additional credit. **Prerequisite(s):** MA 114.

PH 202 - General Physics II (3 credits): Non-calculus-based physics intended for credit in engineering technology courses. Use PH-262 for electrical, computer and software engineering courses. Light and sound: wave motion, nature of light, reflection and mirrors, refraction, prisms, dispersion lenses; simple harmonic motion; sound transmission, resonance, interference. Doppler Effect. Electricity and magnetism: Static electricity, electric fields, magnetic fields, electric potential, capacitance; electricity in motion; magnetic induction; electromagnetic relations. Alternating currents. **Prerequisite(s):** PH 201.

3. Computer Science Core (18 Credits)

CS 120 - Introduction to Programming Using Python (3 credits): The course will cover basic concepts and elements of computer programming using Python. Topics include variables, constants, operators, expressions, statements, branching, loops, and functions. Additionally, Python specific data structures, built-in functions, library modules and working with external files will be applied in developing working code.

CS 150 - Programming in C (3 credits): This introductory course in programming will enable students to understand how computers translate basic human instructions into machine executable applications. The language of choice for this course is C. The C syntax that will be covered includes functions; variables and memory allocations including pointer notation; conditional statements and looping. Students will also learn binary to hexadecimal and decimal conversions along with basic computer architecture. Memory management, data input output and file manipulations will be among some other topics discussed and applied during this course. Formerly titled Introduction to Programming Using C. Prerequisite(s): MA 111 or MA 112 and CS 120 or placement test.

NT 150 - Computer Networking (3 credits): This course is a continuation of NT-100 with major emphasis on local network equipment, network software and addressing schemes. Students build, configure, test and troubleshoot a network in the laboratory. Routers and switches are included. This material can be used as a basis for studying for CISCO's ICND1.

CS 200 - Programming in C++ (3 credits):
Students learn how to program in C++ using an object-oriented approach. Design of classes and objects, inheritance and polymorphism, use of pointers and data structured based projects are also covered in this course. **Prerequisite(s):** CS 130 or CS 150

CS 230 - Data Structures (3 credits): Advance pointers and dynamic memory usage. Concepts of object-oriented design and programming. Includes classes, friend functions, templates, operator overloading, polymorphism, inheritance, exception handling, containers, iterators and the standard template library. Applications involve the use of simple data structures such as stacks, queues, linked lists and binary trees. Recursion, searching and sorting algorithms. The above concepts are implemented through a series of hands-on programming projects, all of which are completed as part of the homework requirements. **Prerequisite(s):** CS 225 or CS 200. **Corequisite(s):** MA 124

CT 152 - Introduction to UNIX (3 credits): Unix file and operating system. Understanding multi-user and multitasking concepts. Editors, X-windows, Awk, email, Internet commands, shell commands and shell scripts. Projects, which provide practical experience, are completed as part of the homework requirements. **Corequisite(s):** CS 120.

4. Engineering Core (24 Credits)

EL 100 – Introduction to DC/AC Circuits (3 credits): Basic electrical concepts and laboratory techniques. Current, voltage, resistance and power. Ohm's law, series and parallel resistive circuits. Kirchhoff's voltage and current laws. Loading effects on meters and supplies. Capacitors and Inductors. Charging and discharging. RC and RL time constants. Introduction to AC. Sinusoidal waveforms, phasors and use of the J operator. Reactance and admittance. Average values and RMS. Laboratory emphasis is on the proper use of standard meters,

testing equipment and circuit breadboarding. MATLAB Part I: Introduction to MATLAB, variables, MATLAB functions, data types, writing a MATLAB program, using basic plotting functions. Corequisite(s): MA 112.

EL-204 – Digital Electronics (3 credits): Number systems, including binary, octal and hexadecimal bases. Binary arithmetic. Boolean algebra, Karnaugh map simplification. Design of combinational circuits. Decoders, multiplexers, flip-flops and other multi-vibrator circuits. Logic families including TTL, CMOS, ECL and others. Memory, shift registers and counters. Prerequisite(s): None

EE 304 - Digital Design I (3 credits): Minimization of Boolean functions using Kamaugh Maps and Quine-McCluskey Tabulation. Multilevel circuits: FPGA's. Combinational logic design with MSI LSI. Chip count reduction. Sequential circuit analysis and design. State tables and state diagrams. Asynchronous circuit design. Introduction to FPGA design software. Students design, simulate and build circuits. **Prerequisite(s):** EL 204.

CE 310 - Computer Architecture (3 credits): Study of the internal organization and operation of digital computers. Topics include instruction set architecture, CPU organization, arithmetic logic units, control units, data paths, and microprogramming. Memory organization and hierarchy including cache memory, virtual memory, and secondary storage are examined. Input/output systems, buses, and interrupt structures are discussed. Performance evaluation techniques, pipelining, and parallel processing concepts are introduced. Students analyze the interaction between hardware and software and explore architectural features that influence system performance and security. **Prerequisite(s):** EL 204.

EE 406 - Signals and Systems (3 credits): Mathematical models, systems, signal classifications, I/O differential and difference equations, block diagram realizations, discrete-time systems. Convolutions: discrete-time and continuous-time. The Z-transform in linear discrete-time systems, transfer functions. Trigonometric Fourier series, polar and rectangular forms, odd/even functions, response of a linear system to periodic input. Fourier transform, symmetry properties, transform theorems, linear filtering, modulation theorem. Laplace and Fourier transforms and their properties. Offered during fall semester only. Offered during fall semester only. **Prerequisite(s):** MA 262 and MA 340.

EE 453 - Control I (3 credits): This course provides a comprehensive introduction to feedback control systems, focusing on the analysis and design of dynamic systems. Key topics include mathematical modeling of physical systems, transfer functions, system response for first- and second-order systems, and stability analysis using Routh-Hurwitz criterion. Students will study steady-state error, system performance metrics, and compensator design methods such as lead and lag compensators. Frequency-domain analysis is emphasized with Bode plots, gain and phase margins, and crossover frequencies. Practical applications are integrated through laboratory exercises and industry-standard computer-aided design tools (e.g., MATLAB/Simulink), equipping students with skills to design and analyze control systems for mechatronics and robotics applications. This course emphasizes both theoretical foundations and hands-on implementation to bridge the gap between theory and practice. **Prerequisite(s):** MA 340.

EE 340 – Systems Engineering (3 credits): This course introduces the principles and practices of systems engineering, focusing on the design, management, and improvement of complex engineering systems. Students will learn systems lifecycle planning, project management, quality control, and risk analysis, with an emphasis on integrating safety and compliance with engineering standards. Topics include system modeling, production systems planning, and human factors, preparing students to tackle multifaceted projects. Designed for engineering students across disciplines, the course equips participants with the technical and managerial skills needed to develop safe, efficient, and sustainable systems in diverse engineering fields

EL 261 - Introduction to Communication Circuits and Systems (3 credits): Fundamental concepts in communications. Amplitude and frequency modulation. Waveform and waveform analysis. Spectral content of signal. Circuits used to generate signal. Signal recovery circuits. Introduction to digital modulation and digital waveforms. Students build and test circuits. MATLAB Part IV: using Communications System Toolbox for analysis, design, simulation and verification of communication systems. Offered during spring semester only. Offered during spring semester only. **Prerequisite(s):** EL 200. **Corequisite(s):** MA 261.

5. Cybersecurity Engineering Core (24 Credits)

IAE 201 - Introduction to Information Assurance Concepts (3 credits): This course covers topics related to administration of network security. Topics include a survey of encryption and authentication algorithms; threats to security; operating system security; IP security; user authentication schemes; web security; email security protocols; intrusion detections; viruses; firewalls; Virtual Private Networks; network management and security policies and procedures. Laboratory projects are assigned as part of the homework requirements. Classes are a mixture of lecture, current event discussions, and laboratory exercises. NOTE: Students enrolled in this course incur an additional lab fee of $100. **Prerequisite(s):** MA 110 or MA 112 or MA 114 or MA 261.

CSE 304 - Cyber Security in Logic Design and Digital Systems (3 credits): This course examines security vulnerabilities and protection mechanisms in digital logic and hardware systems. Topics include hardware threats, malicious circuit modification, hardware Trojans, side-channel attacks, fault injection attacks, and secure hardware design principles. Students study security implications in combinational and sequential circuits, FPGA-based systems, and embedded processors. Methods for secure logic design, trusted hardware verification, and countermeasures against hardware-level attacks are explored. Practical exercises include analysis of digital systems for vulnerabilities and implementation of secure digital logic designs using simulation and hardware development tools. **Prerequisite(s):** EE 304.

CSE 341 - Machine Learning Applied to Cyber Security Engineering (3 credits): This course introduces the application of machine learning techniques to cybersecurity engineering problems. Topics include supervised and unsupervised learning, classification algorithms, anomaly detection, clustering, feature engineering, and model evaluation. Students explore the use of machine learning in intrusion detection, malware classification, network traffic analysis, threat intelligence, and behavioral analytics. Practical projects involve implementing machine learning algorithms using modern tools to analyze cybersecurity datasets and detect malicious activity. Ethical considerations, adversarial machine learning, and security challenges in AI-based systems are also discussed. **Prerequisite(s):** IAE 201, CS 120, MA 330.

CSE 411 - Secure Software Engineering (3 credits): This course focuses on principles and practices for designing and developing secure software systems. Topics include secure coding practices, software vulnerabilities, threat modeling, authentication and authorization mechanisms, secure software architecture, and defensive programming techniques. Students examine common software attacks such as buffer overflows, injection attacks, and cross-site scripting, and study methods to mitigate these vulnerabilities. The course also covers secure software development lifecycle (SSDLC), code review, static and dynamic analysis tools, and security testing techniques. Programming assignments and projects emphasize the development of secure applications and the identification and remediation of software vulnerabilities. **Prerequisite(s):** CS 120.

CSE 310 - Network Security (3 credits): This course examines the principles and technologies used to secure computer networks and data communications. Topics include network threats and vulnerabilities, cryptographic protocols, secure communication techniques, authentication systems, firewalls, intrusion detection and prevention systems, virtual private networks, and network monitoring. Students analyze security architectures for wired and wireless networks and explore defensive strategies against common attacks such as denial-of-service, spoofing, and network intrusion. Laboratory exercises provide practical experience in configuring security tools, analyzing network traffic, and implementing secure network infrastructures. **Prerequisite(s):** NT 150, EL 204.

CSE 421 - Industrial Control Systems Security (3 credits): This course examines cybersecurity challenges associated with industrial control systems used in critical infrastructure sectors. Topics include supervisory control and data acquisition (SCADA) systems, programmable logic controllers (PLCs), distributed control systems, industrial communication protocols, and operational technology networks. Students study vulnerabilities and cyber threats affecting industrial automation environments and analyze real-world cyber incidents targeting infrastructure systems. Methods for securing industrial networks, protecting control devices, and implementing defense-in-depth strategies are explored. Practical exercises include analysis of industrial control architectures and implementation of security measures for operational technology systems. **Prerequisite(s):** NT 150, EL 204.

CSE 425 - Secure RF Communications (3 credits): This course explores security concepts in wireless and radio frequency communication systems. Topics include wireless communication fundamentals, RF signal propagation, wireless protocols, and vulnerabilities in wireless networks. Students study threats such as signal interception, jamming, spoofing, replay attacks, and unauthorized access to wireless systems. Methods for securing wireless communications, including encryption, authentication, spread spectrum techniques, and secure wireless protocols, are examined. Laboratory activities involve analysis of wireless signals, RF spectrum monitoring, and implementation of techniques to secure wireless communication systems. **Prerequisite(s):** CS 150, NT 150, MA 124.

CSE 430 - Critical Infrastructure Protection (3 credits): This course examines strategies for protecting national and industrial critical infrastructure systems from cyber and physical threats. Topics include risk assessment, threat modeling, infrastructure resilience, and security of energy, transportation, communication, and industrial control systems. Students analyze the interdependencies between cyber and physical infrastructure and study frameworks for infrastructure protection and incident response. Emphasis is placed on cybersecurity strategies for large-scale systems, policy considerations, and resilience planning. Case studies and applied projects examine real-world infrastructure security challenges and mitigation strategies. **Prerequisite(s):** EE 340.

6. Senior Design Capstone (6 Credits)

SDE 457 - Senior Design I (3 credits):
Students/teams select a project, develop an understanding of the project scope that includes research and documentation of related work, prepare a feasibility study, develop project requirements (constraints) and engineering, software, and/or security specifications, propose solutions and multiple designs, analyze proposed designs, select a final proposed design, and prepare and present a preliminary design review (PDR). Students are expected to apply proper systems engineering and project management to their work. Additional components may be required in some projects. Students/teams submit a final report at the end of the semester.
Prerequisite(s): Senior standing.

SDE 458 - Senior Design II (3 credits):
Students/teams build and test their selected designs (completed in SDE 457). Each student team delivers a tested prototype and defends its project in front of a panel of experts. Students/teams submit a final report that includes description of the design, realization, and test processes as well as test results, discussion, and conclusion. Failure to deliver a completed design and a working prototype that meets engineering, software, and/or security specifications by the end of the semester may result in failing the course.
Prerequisite(s): SDE 457

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

The Bachelor of Science in Cybersecurity Engineering meets all general education requirements as specified by the Maryland Higher Education Commission and COMAR 13B.02.03. The curriculum includes coursework in written communication (EN 101, EN 102), ethics (SS 351), arts and humanities (HU 331), and introductory business and management studies (BUS 174 and BUS 301), which together broaden students' understanding of professional practice, communication, and ethical responsibility in technical environments.

Quantitative reasoning and scientific literacy are addressed through a comprehensive mathematics and science sequence that includes algebra and trigonometry, calculus, linear algebra, differential equations, probability and statistics, and physics. These courses provide the analytical foundation necessary for engineering analysis and secure system design in computing systems, communication networks, and cyber-physical infrastructure.

Collectively, the general education component ensures that graduates are not only technically proficient in cybersecurity engineering concepts but also well prepared to address ethical, societal, and professional responsibilities associated with designing and protecting modern computing systems and digital infrastructure.

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

Capitol Technology University intends to pursue accreditation for the Cybersecurity Engineering program through the Engineering Accreditation Commission (EAC) of ABET. The curriculum is structured to satisfy EAC-ABET criteria, including:

– A minimum of one year of college-level mathematics and basic sciences, including calculus, differential equations, statistics, and physics
– At least one and one-half years of engineering topics encompassing engineering science and engineering design
– A culminating senior design experience that integrates cybersecurity engineering, system design, and infrastructure protection considerations

The program will be eligible for ABET review following graduation of the first cohort. Upon accreditation, graduates will meet the educational requirements for licensure as Professional Engineers (PE), subject to state-specific licensure regulations.

In addition, selected coursework aligns with industry-recognized certifications in cybersecurity and information security, providing students with preparation relevant to professional credentialing pathways in areas such as network security, information assurance, and secure systems engineering.

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

The proposed program does not involve contractual agreements with other institutions or non-collegiate organizations. All instruction, laboratories, advising, and administrative support will be provided internally by Capitol Technology University faculty and staff.

8. Provide assurance and any appropriate evidence that the proposed program will provide students with clear, complete, and timely information.

Students enrolled in the Cybersecurity Engineering program will receive clear, complete, and timely information regarding curriculum requirements, course sequencing, faculty interaction, technology expectations, support services, and financial obligations. This information is disseminated through the university catalog, program webpages, the Canvas learning management system, and student orientation materials.

Key elements include:

– Published program curricula, degree requirements, and course descriptions
– Assigned academic advisors to guide course selection and progression
– Detailed course syllabi outlining learning objectives, assessment methods, and expectations
– Information on required hardware, software, laboratory tools, and technical competencies
– Access to Canvas LMS training and technical support services
– Academic support resources, including tutoring, library services, and career development support
– Clear information regarding tuition, fees, billing procedures, and financial aid availability

These mechanisms ensure transparency and support student success throughout the program.

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

All advertising, recruiting, and admissions materials for the Cybersecurity Engineering program will be developed and reviewed by the Office of Marketing and Communications in coordination with the Office of Admissions and the School of Engineering. Program materials will accurately reflect the approved curriculum, program objectives, admission requirements, and available student support services.

These efforts will include:

– Maintaining current and accurate program information on the university website
– Producing print and digital materials for recruitment events and outreach activities
– Training admissions counselors and faculty representatives to communicate consistent program information
– Ensuring all public-facing materials align with approved academic documentation and accreditation status

Through these practices, Capitol Technology University ensures that prospective students receive accurate, transparent information to make informed enrollment decisions.

H. Adequacy of Articulation

1. If applicable, discuss how the program supports articulation with programs at partner institutions. Provide all relevant articulation agreements.

At the time of submission, Capitol Technology University does not maintain articulation agreements specifically designated for the proposed Bachelor of Science in Cybersecurity Engineering. However, the University maintains established transfer pathways with a number of regionally accredited two-year institutions whose programs in computer science, cybersecurity, information technology, and engineering technology align with the foundational coursework required for this degree.

The Cybersecurity Engineering program has been designed to accommodate transfer students from associate degree programs in computer science, cybersecurity, information technology, and related technical disciplines. The lower-division portion of the curriculum includes coursework in mathematics, programming, networking, digital electronics, and introductory cybersecurity concepts that are commonly offered at community colleges. This structure enables students entering with an associate degree or

transferable credits to transition efficiently into upper-division coursework and complete the bachelor's degree in approximately two additional years of full-time study.

Capitol Technology University maintains transfer relationships with several institutions, including Cecil College, Community College of Rhode Island (CCRI), Columbia Southern University, and Notre Dame of Maryland University. While existing agreements currently support transfer into related programs such as cybersecurity, computer science, and engineering technology, the university intends to incorporate the Cybersecurity Engineering program into these agreements as appropriate.

In addition, the university engages in STEM outreach and pre-college preparation through partnerships with high schools participating in Project Lead The Way (PLTW) and through service on regional PLTW Engineering Program Advisory Committees. These activities encourage students to pursue postsecondary education in engineering and cybersecurity-related fields.

As the program develops and enrollment grows, Capitol Technology University will pursue formal articulation agreements with Maryland community colleges and other institutions offering relevant associate-level programs. These agreements will support student mobility and strengthen transfer pathways into the Cybersecurity Engineering program.

I. Adequacy of Faculty Resources

1. Provide a brief narrative demonstrating the quality of program faculty.

The Bachelor of Science in Cybersecurity Engineering will be delivered by a qualified and interdisciplinary team of full-time and adjunct faculty drawn from Capitol Technology University's School of Engineering and related academic units. Program faculty possess advanced academic credentials and professional experience in cybersecurity, computer engineering, electrical engineering, networking, secure software development, and systems engineering.

Faculty supporting the Cybersecurity Engineering program hold terminal degrees in engineering, computer science, cybersecurity, and closely related technical disciplines. In addition to their academic qualifications, many faculty members bring professional industry experience in areas such as network security, digital system design, secure software engineering, communication systems, and critical infrastructure protection. This combination of academic expertise and practical experience ensures that instruction reflects current industry practices and evolving cybersecurity technologies.

The program leverages existing full-time faculty who currently teach core courses in engineering, computer science, networking, and cybersecurity across related programs at the university. These faculty members support foundational courses in programming, digital electronics, computer architecture, signals and systems, communication systems, and cybersecurity engineering. This approach ensures instructional continuity while making efficient use of institutional resources.

Adjunct faculty with specialized experience in cybersecurity operations, secure communications, industrial control systems security, and infrastructure protection may supplement instruction in advanced or specialized courses as enrollment grows. This combination of full-time and adjunct faculty allows the program to maintain both academic rigor and flexibility in addressing emerging cybersecurity topics.

Capitol Technology University has demonstrated a sustained commitment to faculty development and capacity building through ongoing hiring in engineering, cybersecurity, and computing disciplines. Faculty assigned to the Cybersecurity Engineering program are actively engaged in curriculum development, laboratory enhancement, student mentoring, and senior design supervision. These activities support the academic quality of the program and contribute to the preparation of graduates capable of addressing complex cybersecurity engineering challenges.

Full-Time Faculty

Dr. Jeff Chi, Ph.D. in Project Management. Dr. Chi supports instruction in systems engineering and project management, with industry experience in project integration, planning, and sustainability.

Dr. Nisma M. Omar, Ph.D. in Analytical Chemistry. Dr. Omar teaches foundational science courses and supports general education related to scientific literacy and technical communication.

Dr. Gregory P. Behrmann, Ph.D. in Mechanical Engineering (The Catholic University of America). Dr. Behrmann teaches robotics, engineering mechanics, and systems engineering, with applied research interests in intelligent systems and human–robot collaboration.

Dr. Andrew Mehri, Ph.D. in Computer Science. Dr. Mehri provides instruction in digital logic, computer systems, and technical computing, and supports integration between software and electronics curricula.

Dr. Tahani Baabdullah, Ph.D. in Computer Science, **Full-Time Faculty** specializing in artificial intelligence and machine learning, with research and industry experience in deep learning, cybersecurity, and blockchain-integrated AI systems.

Prof. Amelia Wear, M.S. in Software Engineering; B.S. in Mechanical Engineering, **Full-Time Faculty and Lead Systems Engineer (industry background)**. Prof. Wear brings expertise in systems integration, controls, and agile development to instruction in applied systems design and mechatronics.

Dr. Mohamed Ghazy, Ph.D. in Engineering (Purdue University), Dean of Academics and Chair of Engineering. Dr. Shehata provides academic leadership for the program and teaches courses in engineering design, control systems, systems engineering, and autonomous systems applications.

Prof. Jeff Volosin, B.S. in Space Science (Florida Institute of Technology), **Full-Time Faculty and Chair of Astronautical and Space Engineering**. Mr. Volosin brings over 38 years of industry and NASA experience in spacecraft systems, mission operations, and autonomous systems development, supporting instruction in systems integration and AI applications in aerospace systems.

Dr. Kellep Charles, Ph.D. in Cybersecurity (Capitol Technology University), M.S. in Telecommunication Management (University of Maryland University College), B.S. in Computer Science (North Carolina Agricultural and Technical State University). Dr. Charles teaches courses in artificial intelligence, cybersecurity, and autonomous systems

Mr. Joseph Harvey, M.A. in Information Technology Management (Webster University), B.S. in Computer Science (Bowie State University). Mr. Harvey teaches artificial intelligence, software systems, and applied computing courses and is currently a Ph.D. candidate in Artificial Intelligence at Capitol Technology University.

Professors of Practice *(Part-Time)*

Dr. Ron Martin is a Professor of Practice with extensive expertise in critical infrastructure protection, industrial control systems security, and identity, credential, and access management (ICAM). His professional experience

includes senior leadership roles with the U.S. Army and federal agencies, as well as active participation in national and international standards organizations. His applied government and industry experience supports instruction in technology operations, systems integration, and cybersecurity.

Adjunct Faculty (Part-Time)

Prof. Megan Miskovish (M.S., Education) supports general education by teaching writing and communication skills essential to technical professionals

Summary of Faculty Resources for the B.S. in

Cybersecurity Engineering

Faculty Name	Type of Appointment	Taught Courses
Prof. Megan Miskovish	Part-Time	EN 101, EN 102, SS 351, HU 331
Dr. Jeff Chi	Full Time Faculty	BUS 174, BUS 301
Dr. Nisma M. Omar	Full Time Faculty	MA 114, MA 261, MA 345, PH 201
Dr. Gregory P. Behrmann	Full Time Faculty	MA 262, MA 330, MA 340, PH 202
Dr. Andrew Mehri	Full Time Faculty	MA 124, NT 150, CE 310, EL 261
Dr. Tahani Baabdullah	Full Time Faculty	CS 120, CS 150, CS 200, CS 230, CT 152
Prof. Amelia Wear	Full Time Faculty	EL 100, EL 204, EE 304
Dr. Mohamed Ghazy	Full Time Faculty	EE 406, EE 453
Prof. Jeff Volosin	Full Time Faculty	EE 340
Dr. Kellep Charles	Full Time Faculty	IAE 201, CSE 304, CSE 341, SDE 457
Dr. Joseph Harvey	Full Time Faculty	CSE 411, CSE 310, CSE 425
Dr. Ron Martin	Part-Time	CSE 421, CSE 430, SDE 458

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

Capitol Technology University is committed to continuous faculty development through its Center for Innovation in Teaching and Learning (CITL). The CITL provides structured professional development opportunities that support instructional quality, promote evidence-based teaching practices, and enhance student learning outcomes across engineering, cybersecurity, and technology programs.

a) Pedagogy that meets the needs of the students

Faculty teaching in the Cybersecurity Engineering program receive training in student-centered and inclusive pedagogical approaches designed to meet the needs of Capitol Technology University's diverse student population. Professional development offerings emphasize active learning strategies, project-based instruction, problem-based learning, and team-based design experiences that align with engineering and cybersecurity education best practices. Special attention is given to supporting adult learners, military-affiliated students, transfer students, and underrepresented populations in STEM. Faculty are encouraged to integrate applied examples, laboratory exercises, and industry-relevant cybersecurity scenarios that reinforce student engagement and persistence.

b) The learning management system

Capitol Technology University utilizes Canvas as its learning management system. All faculty members receive Canvas training during onboarding and have access to ongoing support through tutorials, workshops, and individualized consultations. Training covers effective use of Canvas tools, including course organization, assignment and rubric design, gradebook management, peer review features, and learning analytics. These resources enable faculty to deliver consistent, accessible, and well-structured course materials and to monitor student progress throughout the academic term.

c) Evidence-based best practices for distance education, if distance education is offered

The Cybersecurity Engineering program is currently offered in a traditional, face-to-face instructional format. As such, distance education pedagogy is not applicable at this time. Should the program expand to include online or hybrid delivery in the future, faculty will receive appropriate training in evidence-based distance education practices in accordance with institutional policies and accreditation standards.

J. Adequacy of Library Resources

1. Library Resources and Access

Capitol Technology University's Puente Library provides robust academic and professional support for students and faculty enrolled in the Bachelor of Science in Cybersecurity Engineering program. The library maintains a comprehensive collection of digital and physical resources that are reviewed and updated regularly to ensure alignment with the program's curriculum, student learning outcomes, and evolving industry standards in cybersecurity, computing systems, and secure engineering.

The Puente Library offers full-text access to a wide range of engineering, computing, and cybersecurity-focused databases and peer-reviewed journals. Key digital resources supporting the Cybersecurity Engineering program include:

– IEEE Xplore, providing extensive coverage of electrical engineering, digital systems, communication systems, computer architecture, and cybersecurity research
– ACM Digital Library, supporting coursework and research in computer science, data structures, secure software development, and computing systems
– ScienceDirect and SpringerLink, offering access to journals and eBooks related to cybersecurity, secure systems engineering, networking, machine learning, and cyber-physical systems
– ProQuest and JSTOR, supporting interdisciplinary research in ethics, policy, management, and societal dimensions of cybersecurity and digital infrastructure

The library also provides access to standards and technical documentation relevant to cybersecurity engineering and secure computing systems, including IEEE standards and other industry references that support coursework in network security, digital system security, secure communications, and critical infrastructure protection.

2. Instructional Support and Research Assistance

The Puente Library supports student learning and faculty scholarship through individualized research assistance, information literacy instruction, and guidance on the effective use of scholarly and technical

resources. Librarians work directly with students and faculty to support research projects, programming assignments, laboratory activities, and senior design projects.

Additional services include access to citation management tools such as RefWorks and EndNote, as well as interlibrary loan services for materials not immediately available in the library's holdings. These services are offered both in person and online, ensuring equitable access for all students regardless of instructional modality.

3. Program-Specific Resource Development

To support the launch and ongoing delivery of the Cybersecurity Engineering program, Capitol Technology University will continue to invest in targeted library resource development. Planned measures include:

– Targeted acquisitions, coordinated between library staff and Cybersecurity Engineering faculty, to obtain textbooks, handbooks, standards, and industry publications focused on cybersecurity engineering, network security, secure system design, and infrastructure protection
– Annual resource review, ensuring library holdings remain current with advances in cybersecurity technologies, emerging cyber threats, and industry best practices
– Faculty collaboration, encouraging faculty to recommend resources associated with new or revised courses, laboratory activities, and senior design projects

These efforts ensure that library resources remain aligned with program needs and accreditation expectations.

4. Digital and Remote Access

All major library resources are accessible through the Puente Library portal and integrated with the university's Canvas learning management system. This provides students with continuous access to scholarly literature, technical standards, and research tools in support of coursework, laboratory assignments, and capstone design projects. The availability of digital resources ensures that students can effectively engage in research and applied learning activities regardless of location.

K. Adequacy of Physical Facilities, Infrastructure, and Instructional Equipment

1. Classroom, Office, and Laboratory Space

Capitol Technology University affirms that it possesses sufficient physical facilities, infrastructure, and instructional equipment to support the effective launch and sustained delivery of the proposed Bachelor of Science in Cybersecurity Engineering program.

Instructional delivery will be supported by modern classroom spaces equipped with multimedia projection systems, smart boards, wireless connectivity, and integrated audio-visual technology. These classrooms are designed to support traditional lectures, collaborative learning, hands-on demonstrations, and technology-enhanced instruction aligned with engineering and cybersecurity education.

Faculty and staff offices are available and appropriately furnished to support academic advising, faculty–student interaction, curriculum development, and instructional planning. Office space allocation is reviewed on a regular basis and expanded as needed to accommodate enrollment growth and additional faculty assignments.

Laboratory instruction for the Cybersecurity Engineering program will utilize existing laboratories that currently support engineering, cybersecurity, networking, and computing programs. These facilities are well suited to deliver the hands-on, project-based components of the curriculum. Key laboratory resources include:

– Electrical Circuits and Electronics Laboratory, supporting foundational engineering courses such as EL 100 and EL 200 with breadboards, multimeters, oscilloscopes, power supplies, and signal generators

– Digital Systems and Computer Architecture Laboratory, equipped with digital logic trainers, FPGA platforms, microcontroller systems, and simulation tools to support courses in digital electronics, digital design, and computer architecture

– Networking and Cybersecurity Laboratory, supporting courses in computer networking, network security, and information assurance through networked computing environments, routers, switches, virtualization platforms, and secure configuration tools

– Communication Systems and Signal Processing Laboratory, supporting coursework in signals and systems and communication circuits using signal generators, oscilloscopes, and simulation environments

– Engineering Simulation and Software Resources, including MATLAB and Simulink, Multisim, Logisim, Quartus FPGA design tools, and cybersecurity analysis platforms to support modeling, analysis, and system design across the curriculum

All laboratories comply with applicable safety standards and include appropriate safety equipment, emergency shut-off mechanisms, and instructional safeguards. These facilities provide sufficient capacity to support the Cybersecurity Engineering program's applied learning objectives without requiring significant capital investment at program launch.

2. Support for Distance Education Students and Faculty

Although the Cybersecurity Engineering program is primarily delivered in a face-to-face format, Capitol Technology University maintains robust digital infrastructure to support instructional technology needs and potential hybrid or online components.

a) Institutional Email System

All students, faculty, and staff are issued official university email accounts through Microsoft Office 365. This system supports secure, reliable communication related to coursework, advising, instructional coordination, and university communications.

b) Learning Management System

Capitol Technology University utilizes Canvas as its primary Learning Management System (LMS). Canvas supports course content delivery, assignment submission, assessment, communication, and collaboration. Core LMS features include:

– Centralized access to course materials and resources
– Online discussions, messaging, and group collaboration tools
– Assignment submission, grading, and rubric-based assessment
– Embedded multimedia content and recorded lectures
– Integration with instructional tools such as Turnitin and Zoom

Faculty receive onboarding and ongoing training in the effective use of Canvas, supported by instructional design and technical staff. Students are introduced to the LMS during orientation and have access to continuous technical support resources.

Together, Capitol Technology University's physical facilities, laboratory infrastructure, and instructional technologies provide a strong and scalable foundation for delivering the Cybersecurity Engineering program and supporting student learning outcomes.

L. Adequacy of Financial Resources with Documentation

1. Program Resources

The proposed Bachelor of Science in Cybersecurity Engineering will be implemented using existing institutional resources, including instructional infrastructure, laboratories, software platforms, and administrative support. No internal reallocation of funds is required at program launch, and no existing academic programs will be reduced, modified, or eliminated to support the introduction of this degree.

The program leverages existing faculty expertise in engineering, cybersecurity, computer science, networking, and systems engineering, as well as established laboratory facilities supporting electronics, digital systems, networking, and information assurance. As a result, startup costs are minimal and the program is financially sustainable within current institutional capacity.

Table 1: Program Resources

Resource Category	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**
1. Reallocated Funds	$0	$0	$0	$0	$0
2. Tuition and Fee Revenue (c + g below)	$350,060	$707,940	$1,065,072	$1,449,072	$1,851,644
a. Number of Full-Time Students	8	16	24	32	40
b. Annual Tuition/Fee Rate	$27,808	$28,503	$29,216	$29,946	$30,695
c. Total Full-Time Revenue (a × b)	$222,464	$465,048	$701,184	$958,272	$1,227,800
d. Number of Part-Time Students	7	13	19	25	31
e. Credit Hour Rate	$1,519	$1,557	$1,596	$1,636	$1,677
f. Annual Credit Hours	12	12	12	12	12
g. Total Part-Time Revenue (d × e × f)	$127,596	$242,892	$363,888	$490,800	$623,844
3. Grants, Contracts, and Other Sources	$0	$0	$0	$0	$0
4. Other Sources	$0	$0	$0	$0	$0
TOTAL (1–4)	**$350,060**	**$707,940**	**$1,065,072**	**$1,449,072**	**$1,851,644**

Narrative Rationale for Table 1

– **Reallocated Funds:** No funds are diverted from existing programs. The Cybersecurity Engineering program is supported by current faculty, laboratories, and institutional infrastructure.

– **Tuition and Fee Revenue:** Enrollment projections are conservative and reflect gradual growth from 8 full-time and 7 part-time students in Year 1 to 40 full-time and 31 part-time students by Year 5. Annual tuition increases are estimated at approximately 2.5 percent.

– **Grants and External Sources:** While no external funding is included in the initial projections, the university anticipates future opportunities related to cybersecurity workforce development, digital infrastructure protection, and industry-sponsored initiatives.

– **Other Sources:** No additional funding sources are assumed at this time.

2. Program Expenditures

Projected expenditures support instructional delivery, laboratory and technical support, faculty development, and administrative functions. Costs are scaled to align with projected enrollment growth and increasing instructional demand over the five-year period.

Table 2: Program Expenditures

Expenditure Category	Year 1	Year 2	Year 3	Year 4	Year 5
1. Faculty (b + c below)	$113,468	$155,071	$238,421	$325,843	$417,486
a. FTE Faculty	1.5	2.0	3.0	4.0	5.0
b. Total Faculty Salaries	$94,557	$129,226	$198,684	$271,536	$347,905
c. Faculty Benefits (20%)	$18,911	$25,845	$39,737	$54,307	$69,581
2. Administrative Staff (b + c below)	$5,942	$6,091	$6,244	$6,400	$6,559
a. FTE Admin Staff	0.08	0.08	0.08	0.08	0.08
b. Admin Salaries	$4,952	$5,076	$5,203	$5,333	$5,466
c. Admin Benefits	$990	$1,015	$1,041	$1,067	$1,093
3. Support Staff (b + c below)	$59,885	$92,076	$125,837	$161,230	$198,313
a. FTE Support Staff	1.0	1.5	2.0	2.5	3.0
b. Support Salaries	$49,905	$76,730	$104,864	$134,358	$165,261
c. Support Benefits (20%)	$9,980	$15,346	$20,973	$26,872	$33,052
4. Technical Support and Equipment	$840	$1,425	$2,320	$3,145	$4,140
5. Library	$0	$0	$0	$0	$0
6. New or Renovated Space	$0	$0	$0	$0	$0
7. Other Expenses	$5,850	$14,210	$25,370	$39,330	$56,090
TOTAL (1–7)	**$185,985**	**$268,873**	**$398,192**	**$535,948**	**$682,588**

Narrative Rationale for Table 2

– **Faculty:** Faculty costs include salaries and benefits for full-time and adjunct instructors delivering engineering, cybersecurity, networking, and computing courses. Faculty FTE increases from 1.5 in Year 1 to 5.0 in Year 5 as enrollment and course offerings expand.

– **Administrative Staff:** A fractional administrative position supports scheduling, reporting, assessment coordination, and advising logistics.

– **Support Staff:** Support personnel include laboratory coordinators and technical staff who maintain instructional equipment, cybersecurity software environments, and networked laboratory resources. Staffing increases proportionally with enrollment growth.

– **Technical Support and Equipment:** Funds support ongoing maintenance of laboratory equipment, cybersecurity tools, networking hardware, and software licenses used in instructional laboratories.

– **Library:** Existing digital and physical library resources are sufficient to support the program.

– **New or Renovated Space:** No new construction or renovation is required.

– **Other Expenses:** Includes faculty development, accreditation preparation, recruitment and marketing activities, and continuous program improvement efforts.

M. Adequacy of Provisions for Evaluation of Program

1. Procedures for Evaluating Courses, Faculty, and Student Learning Outcomes

Capitol Technology University employs a comprehensive and systematic approach to evaluating academic programs, faculty effectiveness, and student learning outcomes. These procedures are aligned with institutional assessment policies, Middle States Commission on Higher Education standards, and national accreditation expectations.

Courses are evaluated each semester through standardized student course evaluations. These evaluations assess instructional effectiveness, course organization, clarity of presentation, student engagement, assessment methods, and the extent to which stated course learning outcomes are achieved. Results are reviewed by program leadership, department chairs, and the Vice President for Academic Affairs as part of the continuous improvement process.

Faculty performance is evaluated using multiple sources of evidence, including:

– Peer observations of teaching
– Student course evaluations
– Annual performance reviews conducted by department leadership and the Vice President for Academic Affairs

Student Learning Outcomes (SLOs) for the Cybersecurity Engineering program are assessed at both the course and program levels. Faculty teaching designated assessment courses collect and analyze outcome-specific data using examinations, programming assignments, laboratory exercises, design projects, case studies, and technical presentations. Outcomes are mapped to the program's learning objectives and aligned with ABET Engineering Accreditation Commission (EAC) Student Outcomes. Assessment rubrics are applied consistently across courses to ensure rigor, transparency, and comparability of results. Aggregated results are reviewed annually by program faculty to inform curricular and instructional improvements.

2. Evaluation of Program Educational Effectiveness

The educational effectiveness of the Bachelor of Science in Cybersecurity Engineering will be evaluated through multiple integrated measures designed to assess student achievement, instructional quality, and long-term program sustainability. These measures include:

• **Assessment of Student Learning Outcomes:**
A structured assessment plan evaluates student performance across technical, analytical, and professional competencies throughout the curriculum. Key assessment artifacts include laboratory reports, programming assignments, cybersecurity exercises, network security projects, and the senior capstone design sequence. These assessments provide evidence of achievement across ABET-aligned outcomes such as problem solving, secure system design, teamwork, ethics, communication, experimentation, and lifelong learning. Results are reviewed annually by program faculty to guide continuous improvement.

• **Student Retention and Graduation Rates:**
Retention, progression, and graduation data are monitored by the Office of Institutional Research and shared with program leadership. These metrics are used to identify potential barriers to student success and inform advising strategies, curriculum sequencing, and academic support interventions.

• **Student and Faculty Satisfaction:**
Annual satisfaction surveys are administered to students and faculty to evaluate instructional quality, advising effectiveness, laboratory resources, academic support services, and overall program operations. Additional qualitative feedback is gathered through student focus groups and regular faculty discussions. Results are used to support strategic planning and targeted improvements.

• **Cost-Effectiveness and Resource Utilization:**
The University's Business and Finance Division, in collaboration with Academic Affairs, conducts annual reviews of the program's financial performance. These reviews examine enrollment trends, instructional costs, staffing levels, laboratory utilization, and resource allocation to ensure fiscal sustainability while maintaining academic quality.

• **Accreditation and External Advisory Input:**
The Cybersecurity Engineering program intends to pursue accreditation through the Engineering Accreditation Commission (EAC) of ABET. In support of this process, the program will maintain an active industry advisory board composed of professionals from cybersecurity, information security, network engineering, and critical infrastructure sectors. The advisory board will review curriculum relevance, emerging industry needs, and graduate preparedness, providing recommendations for ongoing program enhancement.

N. Consistency with the State's Minority Student Achievement Goals

1. Access and Success for Minority Students

The proposed Bachelor of Science in Cybersecurity Engineering is fully aligned with the Maryland State Plan for Postsecondary Education, particularly its goals related to student access, success, and equity. The program supports the objectives of COMAR 13B.02.03.05 by expanding educational opportunities for underrepresented minority students in high-demand engineering and cybersecurity fields.

Capitol Technology University maintains a strong institutional commitment to diversity, equity, and inclusion, with a mission focused on providing access to career-relevant STEM education for students from a wide range of backgrounds. The Cybersecurity Engineering program advances this commitment by reducing traditional barriers to entry, strengthening transfer pathways, and embedding academic and co-curricular support structures that promote retention, persistence, and degree completion among minority and underserved student populations.

Key strategies supporting minority student access and success include:

• **Transfer Pathways and Community College Partnerships:**
The Cybersecurity Engineering program is designed to support transfer students from Maryland community colleges, many of which serve high proportions of minority, first-generation, and non-traditional students. Clearly defined transfer pathways, flexible credit transfer policies, and individualized advising enable students to transition efficiently into the upper-division engineering curriculum and complete the degree in a timely manner.

• **Inclusive Curriculum and Pedagogy:**
The curriculum emphasizes applied, hands-on learning through laboratory exercises, programming projects, and engineering design experiences related to secure computing systems, network security, and infrastructure protection. These instructional approaches support engagement and persistence among students from historically underserved groups. Faculty development initiatives promote inclusive teaching practices, culturally responsive pedagogy, and Universal Design for Learning (UDL) to address diverse learning styles and academic preparation levels.

• **Advising and Retention Support:**
Students in the Cybersecurity Engineering program benefit from structured academic advising, early alert systems, tutoring, and academic coaching services. These supports are designed to identify challenges early and provide timely intervention, particularly for students who may face socioeconomic, academic, or transitional barriers to success.

• **Financial Aid and Scholarships:**
Capitol Technology University provides access to federal and state financial aid programs, institutional need-based assistance, and scholarships that support students from underrepresented and economically disadvantaged backgrounds. These financial resources help reduce barriers to enrollment and persistence in engineering and cybersecurity programs.

• **Campus Diversity and Engagement Initiatives:**
The University fosters an inclusive campus climate through student organizations, multicultural programming, mentoring initiatives, and support services that promote belonging and student engagement. These efforts are integrated into institutional planning and assessment processes to ensure continuous improvement in equity and inclusion outcomes.

The Cybersecurity Engineering program directly advances Goal 1 (Access) and Goal 2 (Student Success) of Maryland's State Plan for Postsecondary Education. By expanding access to high-demand engineering pathways and supporting minority student achievement in cybersecurity and digital infrastructure protection fields, the program contributes to the state's efforts to close equity gaps, strengthen workforce diversity, and increase degree attainment among underrepresented populations.

O. Relationship to Low Productivity Programs Identified by the Commission

1. Reallocation of Resources from Low Productivity Programs

The proposed Bachelor of Science in Cybersecurity Engineering is not a direct continuation, merger, or redesign of any program currently identified by the Maryland Higher Education Commission (MHEC) as low productivity. However, the program was developed in response to internal institutional analyses that identified opportunities to strengthen academic efficiency and align program offerings more closely with evolving workforce demands in cybersecurity, secure systems engineering, and digital infrastructure protection.

Capitol Technology University has adopted a strategic approach to improving academic productivity and resource utilization by leveraging existing instructional, fiscal, and administrative resources across engineering, computing, and cybersecurity disciplines. This approach allows the University to expand academic offerings in high-demand fields while maintaining efficient use of institutional resources.

Specifically, the Cybersecurity Engineering program will:

• **Leverage Faculty Expertise from Related Programs:**
Faculty with expertise in electrical engineering, computer engineering, cybersecurity, networking, and systems engineering—currently teaching in related programs—will contribute to courses within the Cybersecurity Engineering curriculum. This interdisciplinary teaching model ensures effective faculty utilization while supporting instruction in areas aligned with current workforce needs.

• **Utilize Existing Laboratory Facilities and Equipment:**
The program will utilize existing laboratories supporting electronics, digital systems, networking, cybersecurity, and computing. These facilities are already equipped with instructional tools and software used in related programs, allowing the University to deliver hands-on learning experiences without requiring significant new capital investment.

• **Optimize Classroom and Administrative Resources:**
No new classroom, laboratory, or office space is required to support the Cybersecurity Engineering program. Existing instructional and administrative resources are sufficient to support program delivery and projected enrollment growth.

• **Strengthen Program-Level Productivity and Sustainability:**
The interdisciplinary structure of the Cybersecurity Engineering program—integrating computer engineering, cybersecurity technologies, network security, and critical infrastructure protection—is expected to attract a broad range of students interested in careers in cybersecurity engineering and secure system design. This structure is anticipated to support sustainable enrollment growth and strong alignment with industry workforce needs.

Although the Cybersecurity Engineering program does not formally replace a specific low-productivity program identified by MHEC, it reflects Capitol Technology University's ongoing commitment to responsible academic planning, effective resource utilization, and alignment of program offerings with labor market demand and state workforce priorities.

P. Adequacy of Distance Education Programs

1. Institutional Eligibility to Offer Distance Education

Capitol Technology University affirms that it is fully authorized by the Maryland Higher Education Commission (MHEC) to offer distance education programs. The University has an established history of delivering high-quality online and hybrid instruction across multiple academic disciplines, including engineering, cybersecurity, information assurance, applied computing, and business.

Capitol Technology University is an active participant in the National Council for State Authorization Reciprocity Agreements (NC-SARA), which permits the institution to offer distance education to students residing in other participating SARA member states. This authorization ensures that the University's distance education offerings comply with applicable state and national regulatory requirements.

2. Compliance with C-RAC Guidelines

Capitol Technology University ensures full compliance with the Council of Regional Accrediting Commissions (C-RAC) Interregional Guidelines for the Evaluation of Distance Education. In accordance with these guidelines, the University affirms the following:

• **Academic Quality and Rigor:**
Courses offered in online or hybrid formats maintain the same learning outcomes, academic rigor, assessment methods, and grading standards as their face-to-face counterparts. All courses undergo internal review to ensure alignment with program objectives and institutional quality standards.

• **Faculty–Student Interaction:**
Regular and substantive interaction between faculty and students is maintained through a combination of synchronous sessions, asynchronous discussion activities, timely feedback on assignments, and virtual office hours. These practices are aligned with federal and accreditor expectations for effective distance education.

• **Student Identity Verification:**
The University employs secure authentication protocols through its learning management system to verify student identity and maintain the integrity of academic work and assessments.

• **Access to Student Services:**
Students enrolled in online or hybrid courses have full and equitable access to academic advising, tutoring, library resources, writing support, career services, and information technology assistance. These services are delivered through secure online platforms and supported by trained professional staff.

• **Technology Infrastructure:**
Capitol Technology University utilizes Canvas as its primary learning management system. Canvas supports content delivery, communication, collaboration, and assessment across instructional modalities. Technical support is available to both students and faculty through a centralized helpdesk and instructional technology team.

• **Faculty Training and Support:**
Faculty teaching in online or hybrid modalities are required to complete training in Canvas, digital

instructional tools, and evidence-based online teaching practices. Ongoing professional development is provided through the University's Center for Innovation in Teaching and Learning.

While the Bachelor of Science in Cybersecurity Engineering is primarily designed for on-campus delivery due to its laboratory-intensive and engineering design focus, select general education, business, and computing courses may be offered in hybrid or online formats. All distance-delivered courses will adhere strictly to institutional policies and C-RAC standards, ensuring instructional quality, consistency, and student support across all delivery modes.