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 # 99631 (●) Check # 99631
Payment Amount: 850.00
Date Submitted: 2/15/2026

Department Proposing Program	Cybersecurity	
Degree Level and Degree Type	Bachelor of Science (B.S.)	
Title of Proposed Program	Bachelor of Science in Aerospace Cybersecurity	
Total Number of Credits	120	
Suggested Codes	HEGIS: 701.00	CIP: 14.0101
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: 2-15-26
	Date of Approval/Endorsement by Governing Board: FEB. 15, 2026	

Revised 1/2021

CAPITOL
Technology University

February 15, 2026

Dr. Sanjay Rai
Secretary of Maryland Higher Education
Maryland Higher Education Commission
217 E. Redwood Street, Suite 2100
Baltimore, MD 21202

Dear Dr. Rai,

Capitol Technology University is requesting approval to offer a Bachelor of Science (B.S.) in Aerospace Cybersecurity. This degree program will be delivered by qualified university faculty and supported through an interdisciplinary curriculum that integrates cybersecurity principles with aviation systems, aerospace operations, and critical-infrastructure protection to meet the growing workforce demand for professionals capable of securing aviation and aerospace digital environments.

Capitol Technology University's mission is to provide a practical, hands-on education in engineering, technology, and applied sciences—preparing students for professional success and lifelong learning. The proposed B.S. in Aerospace Cybersecurity aligns with this mission by equipping students with strong foundations in cybersecurity operations, network defense, digital forensics, aviation systems, cyber-physical infrastructure protection, and regulatory compliance frameworks. Graduates will be prepared to contribute immediately to Maryland's aviation sector, aerospace industry, defense-related organizations, and government agencies responsible for securing transportation and national infrastructure systems.

Demand for professionals who understand both cybersecurity and aviation/aerospace systems continues to grow as airports, airlines, aerospace contractors, and federal agencies increase reliance on interconnected digital platforms and operational technologies. The program is designed to serve students pursuing careers in aviation cybersecurity operations, aircraft network security, airport operational technology protection, unmanned systems security, aerospace system monitoring, and related cyber-physical security roles.

To support this academic initiative, we respectfully submit the full proposal for the Bachelor of Science in Aerospace Cybersecurity for your review and approval. Enclosed is the required documentation, including confirmation of the adequacy of library resources to support this new degree program.

Respectfully,

Bradford L. Sims, PhD

President

CAPITOL
Technology University

February 15, 2026

Dr. Sanjay Rai
Secretary of Maryland Higher Education
Maryland Higher Education Commission
217 E. Redwood Street, Suite 2100
Baltimore, MD 21202

Dear Dr. Rai,

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 Aerospace Cybersecurity**.

As President of the University, I confirm that the Puente Library's resources, including professional staff support, digital databases, regulatory materials, and technical research holdings, are more than adequate to support the B.S. in Aerospace Cybersecurity. The library maintains extensive access to cybersecurity, aviation, aerospace systems, engineering, regulatory, and critical-infrastructure publications necessary to support the program's curriculum, applied coursework, and senior design sequence.

The University remains dedicated and committed to the continuous improvement of its library resources. Sufficient budget allocations are provided to ensure that scholarly databases, federal regulatory materials (including FAA, DHS, and NIST resources), technical standards, and emerging aerospace cybersecurity references remain current and accessible to students and faculty.

Capitol Technology University affirms its ongoing commitment to providing the academic resources necessary to ensure student success and program quality in Aerospace Cybersecurity

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 Aerospace Cybersecurity
Title of Proposed Program

0701
Suggested HEGIS Code

11.1003
Suggested CIP Code

Engineering
Department of Proposed Program

Dr. Mohamed Shehata
Name of Department Head

Dr. Mohamed Ghazy
Dean of Academic

mshehata@captechu.edu
Contact E-Mail Address

(240) 965-2473
Contact Phone Number

2-15-26
Signature and Date

President/Chief Executive Approval

FEBRUARY 15, 2026
Date

Date Endorsed/Approved by Governing Board

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

Capitol Technology University
Laurel, Maryland

A. Centrality to Mission and Planning Priorities

1. Program Description and Alignment with Institutional Mission

The Bachelor of Science (B.S.) in Aerospace Cybersecurity prepares students for entry-level and early-career roles focused on protecting the digital and cyber-physical systems that support modern aviation and aerospace operations. As airlines, airports, aerospace manufacturers, and space-based systems increasingly rely on interconnected networks, automation platforms, satellite communications, and digital flight systems, the aerospace sector has become a significant target for cyber threats. These threats range from data breaches affecting passenger information to sophisticated attacks capable of disrupting flight operations, navigation systems, and critical infrastructure.

The B.S. in Aerospace Cybersecurity integrates foundational cybersecurity principles with applied knowledge of aviation and aerospace systems. Students develop competencies in network security, cyber defense, risk management, regulatory compliance, and cyber-physical systems protection while gaining an understanding of aircraft systems, airport infrastructure, aerospace communications, and space-based assets. Graduates will be prepared to identify vulnerabilities, support security operations, assist with incident response, and contribute to protecting aircraft networks, communication systems, air traffic control environments, satellite systems, and ground-based aerospace infrastructure.

The program aligns directly with Capitol Technology University's mission to provide career-focused education in engineering, computer science, aviation, and cybersecurity disciplines. It reflects the University's emphasis on applied learning, industry alignment, and workforce preparation in high-demand technical fields. By combining cybersecurity with aerospace and aviation systems knowledge, the program expands Capitol Technology University's portfolio of infrastructure-focused and security-oriented academic offerings and strengthens its leadership in critical technology education.

With strong projected job growth across the cybersecurity field and increasing demand for professionals who understand both digital security and aerospace operations, the B.S. in Aerospace Cybersecurity provides a clear pathway into a high-impact, high-opportunity career sector supporting national transportation safety, defense, and space operations.

2. Explanation of How the Proposed Program Supports the Institution's Strategic Goals and Evidence That It Is an Institutional Priority

Capitol Technology University operates under four institutional strategic goals. The B.S. in Aerospace Cybersecurity directly supports each goal as follows:

a. Expand Educational Offerings and Increase Program Completion

The B.S. in Aerospace Cybersecurity expands the University's academic portfolio by introducing a specialized interdisciplinary degree that integrates aerospace systems, aviation operations, and cybersecurity. The program complements existing offerings in aviation, astronautical engineering, cybersecurity, and computer science while creating a distinct, workforce-aligned pathway focused on aerospace system protection.

By aligning coursework with employer expectations in aviation security, aerospace infrastructure protection, and cyber-physical systems defense, the program promotes student engagement, persistence, and timely degree completion. The structured curriculum sequence ensures that students build progressively from foundational cybersecurity knowledge to advanced aerospace security applications.

b. Increase Enrollment and Institutional Awareness

Demand for professionals capable of securing aerospace systems continues to grow among airport authorities, aerospace contractors, defense organizations, commercial airlines, and federal agencies. The B.S. in Aerospace Cybersecurity is positioned to attract students interested in aviation security, satellite and space systems protection, cyber-physical infrastructure defense, and transportation cybersecurity.

Through targeted recruitment efforts, partnerships with aerospace and cybersecurity employers, and engagement with industry advisory boards, the program will strengthen enrollment pipelines and enhance Capitol Technology University's visibility as a leader in aviation and aerospace cybersecurity education.

c. Improve Utilization of University Resources and Institutional Effectiveness While Expanding Revenue

The program leverages existing strengths in cybersecurity, astronautical engineering, aviation, and computer science. Many foundational courses already exist within the University's current academic offerings, allowing efficient use of faculty expertise, laboratory facilities, and instructional infrastructure. Because the curriculum builds upon established coursework, initial startup costs remain moderate while long-term enrollment growth supports tuition revenue and institutional sustainability.

The program's applied and project-based structure—including internships, laboratory experiences, simulations, and a senior capstone—enhances student learning outcomes and institutional effectiveness while maintaining fiscal responsibility.

d. Increase the Number and Scope of Partnerships

The B.S. in Aerospace Cybersecurity will expand Capitol Technology University's partnerships with airport authorities, aerospace manufacturers, cybersecurity firms, engineering contractors, and government agencies such as the Federal Aviation Administration (FAA), the Department of Homeland Security (DHS), and the Department of Defense (DoD).

These partnerships will support internships, cooperative education experiences, capstone collaborations, guest lectures, and workforce pipelines. Continuous engagement with industry stakeholders will ensure curriculum relevance, regulatory alignment, and responsiveness to evolving security threats affecting aviation and aerospace systems.

Evidence of Institutional Priority

The B.S. in Aerospace Cybersecurity has been identified as an institutional priority for the following reasons:

a. Airport authorities, aerospace organizations, cybersecurity firms, and advisory board partners have identified a growing need for professionals who can support aerospace security program implementation, operational oversight, and regulatory compliance related to aviation and space systems.

b. The program directly addresses workforce demands in security, technology, and management roles within airport development organizations, aerospace engineering firms, defense contractors, and government agencies responsible for protecting transportation and space-based infrastructure.

c. Capitol Technology University has committed faculty expertise, curriculum development resources, and administrative support to ensure successful launch and long-term sustainability of the program.

d. The degree strengthens the University's mission of delivering applied, industry-driven education while expanding its portfolio of aviation, cybersecurity, and infrastructure-aligned programs.

3. Narrative of How the Proposed Program Will Be Adequately Funded for at Least the First Five Years

The B.S. in Aerospace Cybersecurity will be adequately funded during the first five years through institutional investment, tuition revenue, industry collaboration, and external funding opportunities. Capitol Technology University has developed a financial framework that supports program sustainability while maintaining academic rigor, appropriate faculty staffing, and sufficient instructional resources.

a. Institutional Support for Program Development and Launch

The University will allocate internal resources to support curriculum development, faculty assignment, academic oversight, and administrative coordination during the program's initial implementation phase. This institutional investment ensures that the program launches with appropriate academic infrastructure and instructional quality.

b. Industry Collaboration and Experiential Learning Support

Capitol Technology University will collaborate with airport authorities, aerospace organizations, cybersecurity firms, and transportation-sector partners to support internships, cooperative education, and industry-sponsored projects. These collaborations enhance experiential learning while strengthening employer engagement and workforce alignment.

c. Tuition Revenue and Long-Term Financial Sustainability

Projected enrollment growth is expected to generate sufficient tuition revenue for the program to become financially self-sustaining within three to five years. The interdisciplinary nature of the program—combining aviation, aerospace systems, and cybersecurity—positions it to attract students from multiple interest areas, contributing to stable enrollment and long-term viability.

d. External Funding and Workforce Development Opportunities

The University will pursue federal, state, and industry-aligned funding sources, including cybersecurity education grants, workforce development initiatives, and infrastructure protection funding programs. These resources may support laboratory enhancement, instructional technology, faculty development, and student scholarships.

e. Engagement with Professional and Industry Organizations

The University will continue developing relationships with aerospace, aviation, cybersecurity, and critical infrastructure associations. These partnerships support long-term program development, student success initiatives, industry engagement, and potential philanthropic contributions.

4. Institutional Commitment

a. Ongoing Administrative, Financial, and Technical Support

Capitol Technology University maintains robust information technology infrastructure and academic support services to sustain the B.S. in Aerospace Cybersecurity. Students and faculty will have access to industry-relevant technologies including simulation platforms, cyber-range environments, secure networking laboratories, and mission-operations tools used to analyze and protect cyber-physical aerospace systems.

The University's IT infrastructure provides reliable access to the learning management system, virtualized laboratory environments, cloud-based cybersecurity platforms, digital libraries, and specialized software used in aviation systems modeling, satellite communications analysis, and cyber defense operations.

Faculty assigned to the program will receive support for professional development to remain current with evolving cybersecurity threats, FAA and DHS guidance, aerospace regulatory standards, and best practices in protecting aviation and space systems. Professional development may include participation in federal cybersecurity initiatives, aviation security workshops, aerospace cybersecurity conferences, and collaboration with industry advisory partners.

These resources ensure that the program maintains academic rigor, technological relevance, and alignment with workforce expectations.

b. Program Continuation and Teach-Out Commitment

Capitol Technology University is fully committed to sustaining the B.S. in Aerospace Cybersecurity for a period sufficient to allow enrolled students to complete their degrees in a timely manner. The institution maintains policies to ensure program continuity, including faculty coverage planning, structured course scheduling, and dedicated academic advising.

In the event of unforeseen circumstances, the University will implement formal teach-out and transition procedures consistent with institutional policy and accreditation standards to ensure student completion. Ongoing assessment of enrollment, student performance, and workforce demand will guide continuous improvement and long-term program viability.

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

The proposed Bachelor of Science (B.S.) in Aerospace Cybersecurity at Capitol Technology University is designed to address the growing statewide and regional demand for professionals capable of protecting the digital and cyber-physical systems that support Maryland's aviation, aerospace, and critical transportation infrastructure. As airports, aerospace manufacturers, airlines, and government agencies increasingly rely on interconnected networks, satellite systems, automated operations platforms, and digital communication technologies, the need for cybersecurity professionals with aviation system expertise continues to expand.

Maryland's aviation ecosystem—including Baltimore/Washington International (BWI) Thurgood Marshall Airport, regional airports, aerospace contractors, defense organizations, and federal agencies—requires a workforce prepared to safeguard aircraft communication networks, airport operational technologies, unmanned and autonomous systems, and other cyber-physical systems essential to aviation safety and continuity of operations. The concentration of federal agencies and defense contractors within the state further intensifies the need for professionals trained in aerospace-specific cybersecurity practices.

The B.S. in Aerospace Cybersecurity addresses this need by integrating foundational cybersecurity education with applied knowledge of aviation systems, airport operations, aerospace platforms, regulatory compliance, and critical infrastructure protection. Students gain exposure to aircraft network security, airport cyber-risk management, aviation communication protocols, digital forensics, incident response, and emerging threats to aerospace technologies. Graduates will be prepared for entry-level and early-career roles in aviation cybersecurity operations, airport and airline security support, aerospace system monitoring, cyber-incident response, and compliance functions within both government and industry.

By producing professionals capable of protecting Maryland's aviation and aerospace infrastructure, the program supports transportation resilience, economic development, national security interests, and long-term workforce priorities within the state.

a) The Need for Advancement and Evolution of Knowledge

The aerospace and aviation cybersecurity landscape is evolving rapidly due to increased system interconnectivity, expansion of unmanned and autonomous systems, modernization of air traffic management technologies, heightened regulatory expectations from agencies such as the Federal Aviation Administration (FAA) and the Department of Homeland Security (DHS), and the growing sophistication of cyber threats targeting critical aviation infrastructure.

In response to these developments, the proposed B.S. in Aerospace Cybersecurity incorporates a forward-looking curriculum emphasizing modern cybersecurity practices within an aviation and critical infrastructure context. Coursework integrates cybersecurity fundamentals, aviation system operations, aircraft and airport network security, cyber-physical system protection, regulatory compliance, risk management, digital forensics, and organizational leadership. Students engage with emerging topics such as secure communication protocols, autonomous system security, threat intelligence, and applied cyber-incident response scenarios through laboratory exercises and industry-informed projects.

This curricular design aligns with Maryland State Plan Goal 3: Innovation—"Foster innovation in all aspects of Maryland higher education to improve access and student success"—and supports Priority 8, which promotes the development of new ideas, pedagogies, and technologies to improve educational delivery and outcomes.

b) Societal Needs, Including Expanding Educational Opportunities and Choices for Minorities and Educationally Disadvantaged Students

The B.S. in Aerospace Cybersecurity expands access to high-growth aviation and cybersecurity career pathways for underrepresented populations, including minority, first-generation, female, adult, and veteran students. Unlike pilot training or engineering-intensive aerospace programs, this degree offers an accessible entry point into the aviation cybersecurity workforce for students with diverse academic backgrounds who are interested in technology, infrastructure protection, and aviation operations.

Capitol Technology University advances equitable access through targeted recruitment initiatives, scholarship programs, articulation agreements with community colleges, and comprehensive academic support services designed to promote student success. These efforts align with Maryland State Plan Goal 1: Student Access—"Ensure equitable access to affordable and high-quality postsecondary education for all Maryland residents."

By offering a cybersecurity-focused aerospace degree, the program broadens participation in the aviation and cybersecurity sectors and contributes to diversifying Maryland's workforce in aviation security and critical infrastructure protection.

c) Capacity and Institutional Differentiation

Although Capitol Technology University is not designated as a Historically Black Institution (HBI), approximately 51 percent of its student population identifies as minority, including approximately 34 percent identifying as Black or African American. The University is committed to expanding access and promoting collaboration with HBIs and minority-serving institutions through articulation agreements, shared academic initiatives, and student support services.

The proposed B.S. in Aerospace Cybersecurity is designed to complement, rather than duplicate, existing cybersecurity and aviation programs within Maryland. By integrating aerospace systems knowledge with cybersecurity education, the program provides a distinctive interdisciplinary pathway that strengthens Maryland's higher education capacity in aviation and aerospace infrastructure protection.

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 B.S. in Aerospace Cybersecurity aligns directly with each of these goals.

Goal 1: Student Access
"Ensure equitable access to affordable and quality postsecondary education for all Maryland residents."

Capitol Technology University is committed to providing equitable access to career-focused education in aerospace cybersecurity and critical infrastructure protection. The B.S. in Aerospace Cybersecurity expands access to stable and well-compensated career pathways within aviation security, aerospace operations, and cyber-physical system protection by offering an applied, industry-aligned curriculum that does not require prior specialized aerospace training.

The University's student demographics reflect its commitment to inclusion:

a. Approximately 51 percent of students identify as minorities, including 34 percent Black or African American students.
b. Approximately 22 percent of students are military veterans who benefit from applied and security-oriented curricula aligned with federal and defense-related careers.
c. The University actively encourages female participation in cybersecurity and aviation-related programs to address gender disparities in technical fields.

To further expand access, Capitol Technology University provides:

a. Transfer agreements with Maryland community colleges.
b. Financial aid and scholarship opportunities that reduce economic barriers.
c. Flexible learning options supporting working adults and nontraditional students.

These initiatives align with State Plan priorities promoting affordability, financial literacy, and equitable access.

Goal 2: Student Success
"Promote and implement practices and policies that will ensure student success."

The B.S. in Aerospace Cybersecurity is structured to promote student retention, timely degree completion, and strong employment outcomes. The University supports student success through:

a. Comprehensive academic advising, tutoring services, and career placement support.
b. Industry-informed curriculum aligned with employer expectations in aviation and cybersecurity sectors.
c. Experiential learning opportunities, including internships, laboratory simulations, and industry-partnered capstone projects.

Cybersecurity and aviation security roles continue to demonstrate strong employment demand and competitive compensation levels, supporting positive return on investment for graduates. Additional institutional strategies supporting student success include tuition predictability programs, veteran support services, and Early Alert academic intervention systems.

Goal 3: Innovation
"Foster innovation in all aspects of Maryland higher education to improve access and student success."

Capitol Technology University maintains a strong institutional focus on applied STEM innovation. The B.S. in Aerospace Cybersecurity advances this commitment by delivering an interdisciplinary program that integrates cybersecurity education with aviation systems, aerospace operations, and regulatory compliance frameworks.

Key program innovations include:

a. Integration of aerospace-specific security systems, aviation communication protocols, and relevant FAA regulatory frameworks.
b. Applied learning through case studies, simulations, cyber-range activities, and industry-informed projects.
c. Capstone experiences addressing real-world aerospace cybersecurity and infrastructure protection challenges.

Through partnerships with airport authorities, aerospace organizations, cybersecurity firms, and government agencies, the program remains responsive to Maryland's evolving aviation and aerospace economy, including continued growth at major transportation hubs such as BWI Thurgood Marshall Airport and regional aviation facilities.

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 (B.S.) in Aerospace Cybersecurity program will be prepared for employment across aviation, aerospace, cybersecurity, defense, and critical-infrastructure protection sectors that require expertise in securing digital aviation systems, protecting cyber-physical assets, and supporting compliance with federal cybersecurity frameworks. Demand for aviation-aligned cybersecurity professionals is driven by rapid digitalization of airport operations, increased reliance on interconnected aircraft systems and unmanned platforms, expanded FAA and DHS cybersecurity guidance, and the growing frequency and sophistication of cyber threats targeting transportation infrastructure.

As airports, airlines, aerospace contractors, and government agencies expand their cyber-defense capabilities, the need for graduates who understand both aviation operations and cybersecurity fundamentals continues to rise.

Potential industries and employment sectors include:

a. Airport Authorities and Aviation Security Divisions
Roles in airport cybersecurity operations, cyber-risk assessment, security monitoring, digital forensics support, and protection of airport operational technologies (OT), communication networks, and access-control systems.

b. Aerospace and Aviation Technology Companies
Positions in aircraft network security, avionics cybersecurity support, secure software testing, unmanned aircraft system (UAS) security, satellite communication protection, and cyber-physical systems defense for commercial and defense platforms.

c. Cybersecurity Firms Supporting Aviation and Critical Infrastructure
Employment in penetration testing, threat intelligence, vulnerability assessment, compliance auditing, and incident response services for aviation clients and aerospace supply-chain partners.

d. Federal and Government Agencies
Opportunities with the Federal Aviation Administration (FAA), Department of Homeland Security (DHS), Transportation Security Administration (TSA), Department of Defense (DoD), National Transportation Safety Board (NTSB), and related agencies supporting aviation system protection and cybersecurity compliance.

e. Airlines and Aviation Service Providers
Positions within airline cybersecurity operations centers (SOCs), identity and access management teams, aircraft data-link security, OT security monitoring, and aviation incident response functions.

f. Private Aerospace Contractors and Defense Organizations
Employment in secure system development, classified system protection, cyber-operations support, and compliance with federal cybersecurity standards including NIST frameworks and CMMC requirements.

Employment Statistics and Salary Expectations in Maryland

According to the U.S. Bureau of Labor Statistics (BLS), cybersecurity-related occupations demonstrate strong wage potential and long-term growth:

• Information Security Analysts (SOC 15-1212) report a national median annual wage of approximately $112,000, with higher regional averages in the Washington–Baltimore metropolitan area.
• Computer and Information Systems Managers report median wages exceeding $170,000 nationally, reflecting leadership opportunities within cybersecurity and IT security operations.
• Network and Computer Systems Administrators and Systems Analysts commonly earn between $80,000 and $130,000 depending on experience and sector.

The Baltimore–Washington corridor—home to BWI Thurgood Marshall Airport, major aerospace contractors, defense installations, and federal cybersecurity agencies—remains

one of the nation's strongest cybersecurity employment hubs, offering competitive salaries and sustained demand.

Expected Level of Entry

Graduates of the B.S. in Aerospace Cybersecurity program are expected to enter the workforce in entry-level to early-career roles such as:

• Cybersecurity Analyst
• Security Operations Center (SOC) Analyst
• Aviation Cybersecurity Technician
• Network Security Specialist
• Cyber-Risk and Compliance Assistant
• Airport or Aircraft Systems Security Support Technician
• Cyber-Physical Systems Technician
• UAS Cybersecurity Support Specialist

With professional experience, industry certifications (e.g., Security+, CISSP Associate, CEH), internships, and capstone project experience, graduates may advance within three to five years into roles such as Cybersecurity Engineer, Aviation Security Analyst, Cyber-Incident Responder, or Cybersecurity Project Lead.

2. Present Data and Analysis Projecting Market Demand and the Availability of Openings in a Job Market to Be Served by the New Program

The B.S. in Aerospace Cybersecurity addresses documented national and statewide demand for cybersecurity professionals capable of protecting aviation systems, airport technologies, aerospace platforms, and critical transportation infrastructure.

National Projections

The U.S. Bureau of Labor Statistics projects 32 percent employment growth for Information Security Analysts from 2022 to 2032, significantly faster than the national average for all occupations. This growth reflects increased cyber threats, expanded digital infrastructure, and heightened regulatory compliance requirements across industries, including aviation and aerospace.

Nationally, this growth translates into tens of thousands of annual cybersecurity job openings, including roles aligned with network security, cyber-risk management, incident response, and cyber-physical systems protection.

Maryland State Projections

The Maryland Department of Labor identifies cybersecurity and information technology occupations as priority growth areas, particularly within the Baltimore–Washington region. This area includes:

• BWI Thurgood Marshall Airport
• Federal cybersecurity agencies
• Aerospace and defense contractors
• Cybersecurity operations centers

State projections indicate consistent annual openings in cybersecurity analyst, network security, compliance, and infrastructure protection roles. Maryland's designation as a national cybersecurity hub strengthens employment prospects for graduates.

Industry Demand and Workforce Initiatives

Maryland workforce development strategies identify cybersecurity, aviation, and critical-infrastructure protection as high-priority sectors requiring skilled talent. As aviation infrastructure becomes increasingly digitized, employers require cybersecurity professionals who understand aviation systems, operational technologies, and regulatory environments.

Employer Hiring Trends

Employers report sustained hiring demand due to:

• Increasing cyber-risk exposure in aviation environments
• Expansion of digital airport and aircraft systems
• Federal compliance requirements
• Workforce retirement trends
• Ongoing cybersecurity workforce shortages

These factors collectively indicate sustained demand for graduates trained in aerospace-aligned cybersecurity.

3. Discuss and Provide Evidence of Market Surveys That Clearly Provide Quantifiable and Reliable Data on Educational and Training Needs and the Anticipated Number of Vacancies Expected Over the Next Five Years

Multiple national and state labor-market sources confirm sustained demand for cybersecurity professionals in sectors aligned with aviation and aerospace.

a. U.S. Bureau of Labor Statistics

The BLS projects 32 percent growth in Information Security Analyst positions through 2032. This equates to substantial annual job openings nationwide due to both growth and workforce replacement needs.

b. National Workforce Indicators

National labor-market analyses consistently identify cybersecurity operations, digital forensics, compliance, and risk management as fields experiencing workforce shortages. Aviation and aerospace employers increasingly require cybersecurity personnel capable of securing aircraft networks, airport operational systems, and unmanned platforms.

c. Maryland Department of Labor

Maryland occupational projections indicate steady annual openings in cybersecurity-related roles across public and private sectors. The Baltimore–Washington region's concentration of aviation and federal infrastructure reinforces demand.

d. Current Maryland Job Market Indicators

Recent job postings within Maryland consistently list openings for:

- Cybersecurity Analysts
- SOC Technicians
- Compliance Specialists
- Network Security Professionals
- Critical-Infrastructure Security Analysts

Aviation-aligned employers frequently seek candidates with cybersecurity experience in transportation, aerospace, or federal environments.

e. Educational and Training Needs

Employer feedback and workforce studies indicate the need for graduates who combine cybersecurity competencies with domain-specific knowledge in aviation operations and critical-infrastructure environments. The B.S. in Aerospace Cybersecurity addresses this training gap by integrating cybersecurity fundamentals with aviation systems, regulatory frameworks, and applied laboratory experiences.

4. Provide Data Showing the Current and Projected Supply of Prospective Graduates

Maryland offers multiple general cybersecurity and information technology programs; however, there are limited bachelor's-level programs dedicated specifically to aerospace or aviation cybersecurity. Most existing programs provide broad cybersecurity preparation without specialized coursework addressing aircraft networks, airport operational technologies, aerospace platforms, or aviation regulatory environments.

As a result, aviation and aerospace employers often recruit general cybersecurity graduates and provide additional sector-specific training internally. This indicates a supply gap in graduates who possess integrated aerospace cybersecurity expertise at the undergraduate level.

Over the next five years, Maryland is projected to experience continued demand for cybersecurity analysts, compliance specialists, network security professionals, and cyber-physical systems technicians. Without specialized aerospace-aligned cybersecurity education pathways, the supply of sector-ready graduates is expected to remain below employer demand.

The proposed B.S. in Aerospace Cybersecurity contributes to addressing this gap by producing graduates prepared to secure aviation technologies, airport systems, aircraft communication networks, and aerospace digital platforms. By strengthening the state's specialized cybersecurity workforce pipeline, the program supports long-term economic development and transportation resilience within Maryland's aviation and aerospace sectors.

D. Reasonableness of Program Duplication

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

No Maryland institution currently offers a bachelor's degree specifically titled Aerospace Cybersecurity or a program that formally integrates cybersecurity education with aviation systems, aircraft network protection, airport operational technologies, and aerospace cyber-physical infrastructure protection. However, several Maryland institutions offer programs under related CIP classifications, including Cybersecurity (11.1003), Computer Science (11.0701), Electrical Engineering (14.1001), Computer Engineering (14.0901), Aerospace Engineering (14.0201), and Aviation Management. The following discussion identifies similar programs and explains how the proposed B.S. in Aerospace Cybersecurity differs in scope and focus.

a. Cybersecurity Programs (CIP 11.1003 and Related)

University of Maryland, College Park offers a Bachelor of Science in Cybersecurity and related computing degrees. The program emphasizes cryptography, secure software development, networks, and cyber defense but does not include coursework specific to aviation systems, aircraft networks, airport operational technologies, or aerospace infrastructure protection.

University of Maryland Global Campus (UMGC) offers a Bachelor of Science in Cybersecurity Management and Policy and related cybersecurity degrees. These programs focus on policy, governance, digital forensics, and information assurance but do not integrate aviation systems or aerospace-specific cybersecurity applications.

University of Maryland Baltimore County (UMBC) offers programs in Computer Science and related computing disciplines with cybersecurity concentrations. While technically rigorous, these programs are structured around general computing and cybersecurity practice rather than aviation or aerospace environments.

Towson University offers Computer Science and Information Technology programs with cybersecurity coursework but does not offer an aerospace- or aviation-focused cybersecurity pathway.

Morgan State University offers Computer Science and Electrical Engineering programs that may include cybersecurity-related coursework; however, there is no degree that integrates aviation systems and aerospace infrastructure protection.

Rationale:
These programs provide strong foundations in general cybersecurity but do not incorporate aviation operations, airport technologies, aerospace platforms, FAA regulatory environments, or cyber-physical aviation systems. The proposed B.S. in Aerospace Cybersecurity is distinct in its integration of aviation system knowledge with cybersecurity practice.

b. Aerospace and Aviation Programs (CIP 14.0201 and Related)

University of Maryland, College Park offers a Bachelor of Science in Aerospace Engineering (CIP 14.0201). This program emphasizes aerodynamics, propulsion, structures, and flight dynamics. It does not include cybersecurity or digital aviation system protection as a core focus.

Capitol Technology University offers aviation and astronautical programs; however, none integrate cybersecurity as a primary discipline within aviation systems protection.

Other Maryland institutions offer aviation management or aviation science programs, typically focused on pilot training, airport operations, or aviation administration rather than cybersecurity integration.

Rationale:
Aerospace and aviation programs focus primarily on engineering design, flight systems, or operational management and do not address cybersecurity frameworks, digital risk management, aircraft network protection, or aviation cyber-physical infrastructure defense.

c. Engineering and Computer Engineering Programs (CIP 14.1001 and 14.0901)

Several Maryland institutions, including University of Maryland, College Park; UMBC; and Morgan State University, offer Bachelor of Science degrees in Electrical Engineering and Computer Engineering. These programs may include coursework in embedded systems, networks, or computer architecture but do not integrate aviation-specific cybersecurity or airport operational technologies as a defined academic pathway.

Rationale:
While engineering programs may provide technical depth in systems and networks, they

do not focus on aviation regulatory frameworks, aerospace operational environments, or sector-specific cybersecurity applications.

Conclusion Regarding Duplication

A review of the Maryland Higher Education Commission (MHEC) Academic Program Inventory confirms that no institution in Maryland currently offers a bachelor's-level program in Aerospace Cybersecurity or an equivalent interdisciplinary degree integrating cybersecurity with aviation systems and aerospace infrastructure protection.

The proposed program does not duplicate existing offerings. Rather, it builds upon established disciplines (cybersecurity and aviation) to create a specialized, sector-focused degree pathway that addresses a distinct and emerging workforce need within Maryland's aviation and aerospace sectors.

2. Provide Justification for the Proposed Program

The proposed B.S. in Aerospace Cybersecurity is justified by documented workforce demand, institutional differentiation, and alignment with state economic priorities.

a. Workforce Need for Aviation and Aerospace Cybersecurity Talent

Maryland's aviation and aerospace ecosystem—including BWI Thurgood Marshall Airport, regional airports, aerospace contractors, defense organizations, and multiple federal agencies—requires professionals capable of securing aircraft systems, airport operational technologies, unmanned platforms, and cyber-physical aviation infrastructure.

As aviation systems become increasingly digitized and interconnected, employers face rising cybersecurity risks tied to regulatory compliance requirements, operational continuity, and infrastructure protection. Employers report difficulty identifying graduates who possess both cybersecurity expertise and aviation system knowledge. The proposed program directly addresses this workforce gap.

b. Distinct Academic Focus and Program Differentiation

The B.S. in Aerospace Cybersecurity provides a specialized academic pathway not currently available in Maryland. Unlike general cybersecurity programs, the curriculum integrates:

• Aviation system operations
• Aircraft and airport network protection
• Cyber-physical aviation systems security
• Regulatory compliance considerations (FAA, DHS frameworks)
• Applied aviation-specific cybersecurity labs
• An interdisciplinary capstone sequence synthesizing aviation and cybersecurity competencies

This structure ensures graduates are prepared for aviation-aligned cybersecurity roles rather than general IT security positions.

c. Alignment with State and Regional Workforce and Economic Priorities

Maryland's economy includes strong aviation, aerospace, and federal cybersecurity sectors. The state continues to prioritize cybersecurity workforce development and critical-infrastructure protection. The proposed program strengthens Maryland's talent pipeline in a sector where aviation operations and cybersecurity intersect.

The program aligns with regional economic drivers including airport modernization, aerospace research and development, federal cybersecurity initiatives, and transportation infrastructure protection.

d. Competitive Advantage and Industry Collaboration

Capitol Technology University will leverage established partnerships with airport authorities, aerospace organizations, cybersecurity firms, and federal agencies to ensure curriculum relevance and workforce alignment. Industry engagement will support:

• Internships and cooperative education
• Applied research and capstone projects
• Advisory board participation
• Guest lectures and technical workshops

These collaborations strengthen the program's competitive advantage and ensure graduates are prepared for sector-specific professional practice.

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 (B.S.) in Aerospace Cybersecurity at Capitol Technology University is not expected to negatively affect the implementation, enrollment, or sustainability of high-demand programs at Maryland's Historically Black Institutions (HBIs), including Morgan State University, Bowie State University, Coppin State University, and the University of Maryland Eastern Shore.

A review of academic program inventories indicates that no Maryland HBI currently offers a bachelor's-level degree specifically focused on aerospace cybersecurity or a program integrating cybersecurity with aviation systems, aircraft network protection, airport operational technologies, and aerospace cyber-physical infrastructure. While HBIs

offer strong programs in computer science, cybersecurity, engineering, and related STEM disciplines, none provide an interdisciplinary aerospace-focused cybersecurity pathway.

The proposed program is designed to complement, rather than compete with, existing HBI offerings. Students completing associate or bachelor's-level coursework in cybersecurity, computer science, engineering, aviation management, or related STEM fields at HBIs may pursue advanced specialization through transfer or collaborative academic pathways. Capitol Technology University is committed to exploring articulation agreements, dual-enrollment discussions, and collaborative outreach initiatives that expand academic opportunities without reducing enrollment at HBIs.

The program may also enhance educational access for underrepresented students by providing an additional pathway into high-demand aviation and aerospace cybersecurity careers. By broadening sector-specific options within Maryland's higher education system, the proposed B.S. in Aerospace Cybersecurity strengthens the overall capacity of the state's institutions to meet workforce demand in cybersecurity and critical infrastructure protection.

Accordingly, the program does not duplicate or undermine existing HBI programs. Instead, it expands educational choice, supports workforce development, and aligns with statewide goals promoting collaboration, diversity, and equitable participation in high-demand STEM fields.

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 (B.S.) in Aerospace Cybersecurity at Capitol Technology University is not expected to interfere with, diminish, or alter the distinct identities or missions of Maryland's Historically Black Institutions (HBIs), including Morgan State University, Bowie State University, Coppin State University, and the University of Maryland Eastern Shore.

Each HBI maintains a mission grounded in expanding educational access, promoting student success, advancing community engagement, and fostering inclusive excellence. The proposed program neither replicates nor redefines these institutional missions. Instead, it reflects Capitol Technology University's established identity as a career-focused, applied STEM institution emphasizing industry-driven education and workforce preparation in specialized technical fields.

The B.S. in Aerospace Cybersecurity is structured as a niche, workforce-oriented program integrating cybersecurity with aviation and aerospace systems protection. Its focus on aircraft network security, airport operational technologies, cyber-physical aviation

systems, and regulatory compliance represents a specialized academic pathway rather than a broad-based expansion into general cybersecurity or engineering education traditionally offered across institutions.

The program does not alter the academic character or strategic positioning of HBIs. Rather, it expands statewide academic capacity within a defined technical specialty aligned with aviation and aerospace cybersecurity. Capitol Technology University remains committed to collaboration with HBIs through articulation agreements, transfer pathways, and cooperative initiatives that enhance student mobility and opportunity. These collaborative pathways support HBI student advancement into specialized aerospace cybersecurity roles without drawing resources or altering HBI programmatic priorities.

By maintaining a clearly differentiated mission and academic focus, the proposed program complements Maryland's higher education ecosystem. It strengthens workforce preparation in a specialized sector while respecting the unique institutional identities and historical missions of Maryland's Historically Black Institutions.

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

1. Describe How the Proposed Program Was Established and the Faculty Who Will Oversee the Program

The Bachelor of Science in Aerospace Cybersecurity was developed through a collaborative academic planning process involving faculty from cybersecurity, aviation, astronautical engineering, computer science, and engineering programs, in consultation with the Office of Academic Affairs and industry stakeholders. Input was received from cybersecurity professionals, aviation and aerospace employers, advisory board members, and workforce representatives who identified a growing need for graduates capable of securing aviation systems, aircraft networks, airport operational technologies, and aerospace cyber-physical infrastructure.

The program builds upon Capitol Technology University's established strengths in cybersecurity, aviation studies, astronautical engineering, computer science, and information assurance. Existing approved coursework has been integrated into a cohesive interdisciplinary structure emphasizing applied learning, aviation system awareness, cyber-risk management, regulatory compliance, and problem-solving within aerospace and transportation environments. The curriculum is intentionally designed to serve traditional undergraduate students, transfer students, adult learners, and those seeking career-focused preparation in aviation cybersecurity.

The program will be overseen by full-time faculty with expertise in cybersecurity operations, aviation systems, cyber-physical infrastructure protection, digital forensics,

regulatory compliance, and systems engineering. Faculty members hold advanced degrees and possess relevant academic, industry, and government experience. Adjunct faculty with specialized experience in aerospace systems, aircraft network security, and applied cybersecurity may support selected upper-division courses and senior projects to ensure alignment with evolving industry standards.

2. Describe Educational Objectives and Learning Outcomes Appropriate to the Rigor, Breadth, and Modality of the Program

The Bachelor of Science in Aerospace Cybersecurity is delivered primarily in an on-campus format, with selected courses offered in hybrid or online modalities to accommodate transfer students and working professionals. The curriculum emphasizes applied instruction through case studies, laboratory exercises, aviation-focused cybersecurity simulations, team-based projects, and structured analytical assignments. The program culminates in a two-semester senior design sequence integrating cybersecurity principles with aviation systems protection and regulatory considerations.

Program Goals

Graduates of the B.S. in Aerospace Cybersecurity will:

a. Be prepared for entry-level and early-career employment in aviation cybersecurity operations, cyber-physical system protection, and related roles within airports, airlines, aerospace organizations, and government agencies.
b. Apply cybersecurity and systems principles to aviation environments including aircraft networks, airport operational technologies, and aerospace digital infrastructure.
c. Demonstrate professional communication, ethical responsibility, and effective teamwork in technical and regulatory environments.
d. Understand aviation system architectures, regulatory frameworks (FAA, DHS, NIST, ICAO), and cyber-risk factors influencing aerospace infrastructure protection.
e. Engage in lifelong learning, professional development, and credential advancement in cybersecurity and aviation security.

Learning Outcomes

Upon completion of the program, graduates will be able to:

a. Apply cybersecurity concepts, risk-management frameworks, and network defense strategies to aviation and aerospace systems.
b. Analyze aviation technology systems and regulatory requirements to support informed cybersecurity decisions.
c. Communicate technical findings effectively to both technical and non-technical stakeholders.
d. Recognize and apply ethical, safety, professional, and regulatory standards in cybersecurity practice.
e. Function effectively within multidisciplinary cybersecurity teams addressing aviation security challenges.

f. Integrate cybersecurity and aviation system knowledge in a culminating senior design project addressing real-world aerospace cybersecurity problems.

3. Explain How the Institution Will

a) Provide for Assessment of Student Achievement of Learning Outcomes in the Program

Student learning outcomes will be assessed through direct and indirect measures. Course-level outcomes are mapped to program-level outcomes to ensure curricular alignment. Faculty evaluate student achievement using examinations, analytical assignments, laboratory exercises, cybersecurity simulations, case studies, applied aviation security projects, and presentations.

The two-semester Senior Design sequence serves as the primary culminating assessment experience. Students must demonstrate the ability to analyze aviation cybersecurity challenges, design and implement technically sound solutions, and communicate results effectively.

Assessment data are reviewed annually by program faculty and academic leadership. Findings inform curricular adjustments, instructional refinement, and continuous improvement efforts.

b) Document Student Achievement of Learning Outcomes in the Program

The University maintains a centralized academic assessment process. Course portfolios include syllabi, assignments, rubrics, and representative student work. Faculty submit annual outcome assessment reports documenting performance metrics, achievement levels, and improvement plans. Documentation supports institutional effectiveness, accreditation processes, and regulatory compliance.

4. Provide a List of Courses with Title, Semester Credit Hours and Course Descriptions, Along with a Description of Program Requirements

Bachelor of Science (B.S.) Aerospace Cybersecurity

Course Requirements

Bachelor of Science – 121 Credits

Aeronautical Science (9 credits)
Astronautical Engineering (12 Credits)
Computer Science (27 Credits)
Information Assurance (33 Credits)
Math (13 Credits)
English, Humanities, & Social Science (27 Credits)

Course Name	Credits	Prerequisites
AVT-201 – Air Traffic Control Systems	3	None
AVT-251 – Air Transportation	3	None
AVT-256 – Aviation Safety	3	None
AE-150 – Intro to Space	3	None
AE-250 – Ground Systems	3	AE-150 recommended
AE-210 – Spacecraft Subsystems	3	AE-150
AE-350 – Ground System Automation	3	MA-210
AE-325 – Space Systems Engineering	3	AE-210
AE-455 – Space Communications	3	MA-210
CS-120 – Intro to Programming Using Python	3	None
CS-150 – Intro to Programming Using C	3	None
CS-200 – Programming in C++	3	CS-150
CS-220 – Database Management	3	CS-120 or CS-150
CS-230 – Data Structures	3	CS-200
CS-250 – Intro to Network Programming Using C	3	CS-150
CS-300 – Secure Coding	3	CS-230
CS-418 – Operating Systems	3	CS-230
CT-152 – Introduction to UNIX	3	None
IAE-201 – Introduction to IA Concepts	3	None
IAE-250 – Comprehensive Computer & Network Security	3	IAE-201
IAE-260 – Secure System Administration & Operation (UNIX)	3	CT-152
IAE-350 – AI Governance and Security	3	IAE-201
IAE-325 – Secure Data Communications & Cryptography	3	CS-230
IAE-390 – Penetration Testing	3	IAE-250
IAE-402 – Intro to Incident Handling & Malicious Software	3	IAE-250
IAE-405 – Malware Analysis / Reverse Engineering	3	IAE-402
IAE-406 – Digital Forensics & Investigative Process	3	IAE-250
SDE-457 – Senior Design Project I	3	Senior standing
SDE-458 – Senior Design Project II	3	SDE-457
MA-112 – Algebra	3	None
MA-124 – Discrete Mathematics	3	MA-112
MA-128 – Introduction to Statistics	3	MA-112
MA-261 – Calculus I	4	MA-112 or placement
EN-101 – English Communications I	3	None
EN-102 – English Communications II	3	EN-101
HU-331 – Arts and Ideas	3	EN-102 recommended
SS-351 – Ethics	3	EN-102 recommended

Humanities Elective	3	Varies
Humanities Elective	3	Varies
Social Science Elective	3	Varies
Social Science Elective	3	Varies
Science Elective (Physics or Chemistry)	3	Varies

Detailed Course Descriptions

Aviation Courses (9 Credits)

AVT-201 Air Traffic Control Systems (3 Credits)
This course provides an introduction to Air Traffic Control (ATC), the history, development, and structure of the National Airspace System (NAS). The student will explore navigation aids, ATC radar systems, terminal and enroute traffic control, flight service, weather facilities, airspace, and FAA regulations.

AVT-251 Air Transportation (3 Credits)
This course provides an introduction to Air Traffic Control (ATC), the history, development, and structure of the National Airspace System (NAS). The student will explore navigation aids, ATC radar systems, terminal and enroute traffic control, flight service, weather facilities, airspace, and FAA regulations.

AVT-256 Aviation Safety (3 Credits)
This course will concentrate primarily on the major aspects of aviation safety and the organizations and processes that govern commercial and general aviation safety in the United States. This course will provide an introduction to aviation safety programs, risk management, and the associated components of pilot psychology, physiology, human factors, and accident review and investigation. It will also include an overview of modern techniques used in accident investigation.

Astronautical Engineering Courses (12 Credits)

AE-150 Intro to Space (3 Credits)
Introduces the student to elements of astronomy and space sciences, the history of NASA and earth missions and operations and simple physics of satellite orbits, types of orbits and orbital terminology. Space environment and its effects on satellite and equipment. Discussion of satellites, types of satellites and their uses. Offered during Fall semester only. Offered during Fall semester only.

AE-250 Ground Systems (3 Credits)
An introduction to the design of ground systems. Includes an overview of ground system hardware/software architectures as well as an introduction to satellite telemetry, command and control components. Also includes an introduction to spacecraft data standards and the tools used for mission planning. Prerequisite: AE-150, CS-120, and EN-102. Offered spring semester only. Offered spring semester only.

AE-210 Spacecraft Subsystems (3 Credits)
Covers major spacecraft Subsystems such as power, thermal control, attitude determination and control, propulsion, structures, and communications. Students learn Subsystems functions, interactions, and design considerations.

AE-350 Ground System Automation (3 Credits)
Provides an in-depth introduction to the components that compose satellite ground systems in the commercial, military, and civil sectors from the inception of the space program to present day. Discusses conceptual and planned software development, integration and testing, launch operations, sustainment engineering, decommissioning of ground systems components and the system engineering processes involved in these activities. Introduces students to the tools and methods needed to create dynamic ground system components based on automation and autonomic principles. Cover CCSDS, ISO-900X, CMMI, UML, mission planning, flight dynamics principles and risk mitigation/anomaly resolution practices. Provides an introduction to STOL, CECIL, XML, and XTCE languages. Offered Fall semester only. Offered Fall semester only.

Computer Science Courses (27 Credits)

CS-120 Intro 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 Intro to Programming Using 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.

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.

CS-220 Database Management (3 Credits)
An overview of database systems, with an emphasis on relational databases. Terminology, basic analysis and design using Entity-Relationship diagrams and relational schemas. Database implementation, queries and updates in a modern relational database management system. An overview of database administration, transactions and

concurrency. Data warehouses. Projects, which are assigned as homework, are implemented in Oracle.

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.

CS-250 Introduction to Network Programming Using C (3 Credits)
An introductory network programming course using the C programming language. Students will be provided an overview of the principles of computer networks with a detailed look at the OSI reference model and the TCP/IP stack. The emphasis is on understanding UNIX inter-process communication and developing network programs using connectionless and connection-oriented sockets. Extensive programming assignments will include the development of client/server and peer-to-peer network applications.

CS-300 Secure Coding (3 Credits)
This course introduces the secure coding process including designing secure code, writing code that can withstand attacks, and security testing and auditing techniques to detect secure coding weaknesses. The course focuses on the security issues a programmer face including, but not limited to, common code security weaknesses and modern security threats. The course explores core secure coding principles, strategies, coding techniques, and tools that aid programmers in developing more resilient and robust code. Students will develop and analyze C language code that demonstrates mastery of these secure coding principles. The course will also rely on industry standards and best practices such as SEI-CERT coding standards and OWASP top 10 web application security risks.

CS-418 Operating Systems (3 Credits)
Principles underlying computer operating systems are presented from a computer designer's perspective. Concepts explained include process concurrency, synchronization, resource management, input/output scheduling, job and process scheduling, scheduling policies, deadlock, semaphore, consumer/producer relationship, storage management (real storage management policies in a multiprogramming environment), virtual memory management (segmentation and paging), secure memory management, access control lists and kernel protection. An overview of contemporary operating systems with these principles. Students program in a high-level language. Projects are assigned as part of the homework requirements.

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.

Information Assurance Courses (33 Credits)

IAE-201 Introduction to IA 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.

IAE-250 Comprehensive Computer and Network Security (3 Credits)
Building on IAE-201, this course provides learners with detailed and hands-on knowledge of computer and network security. The course emphasizes current topics such as network security, compliance and operational security, threats and vulnerabilities, application security, access control, as well as cryptography. Additionally, underlying theory and concepts are presented in order to extend learners' understanding of computer and network security. Weekly laboratory exercises are utilized to reinforce practical, real-world security techniques. Classes are a mixture of lecture, current event discussions, and laboratory exercise review and will prepare learners for the CompTIA Security+ certification. Pre-requisite: IAE-201 *FORMERLY IAE-301 NOTE: Students enrolled in this course incur an additional lab fee of $100.

IAE-260 Secure System Administration and Operation – UNIX (3 Credits)
This course is an overview of securing the UNIX operating system. The content will include a basic introduction of: shell programming, process management, and processor management, storage management, scheduling algorithms, resource protection and system programming. The course will include programming projects focused on Information Assurance problem solving utilizing the C programming language primarily. Students are expected to be familiar with virtual machines, the UNIX command line interface (CLI) and a basic programming language. FORMERLY IAE 315 NOTE: Students enrolled in this course incur an additional lab fee of $100.

IAE-350 AI Governance and Security (3 Credits)
Explores cybersecurity implications of artificial intelligence, including model security, data integrity, governance frameworks, and ethical considerations.

IAE-325 Secure Data Communications and Cryptography (3 Credits)
This course follows the protocol education provided in IAE-250 with a more detailed and practical look at secure transactions and correspondence, as well as protection of data in storage. Within the confines of the ISO-OSI model, this course discusses data communication with emphasis on the security available at the layers, secure sockets layer, and both wired and wireless security topics. One-way message digests/hashes and

encryption history and protocols are explored in-depth. Topics include virtual private networks, one-way hashes/message digests, digital signatures, secret-key and public key cryptography processes and algorithms. NOTE: Students enrolled in this course incur an additional lab fee of $100.

IAE-390 Penetration Testing (3 Credits)
This course explores the foundational concepts, methods and techniques in preparing and conducting penetration tests. Throughout the course students are introduced to various tools as well as unravel complex methods for exploiting client-side, service side and privilege escalation attacks. Most importantly students learn how to construct a final report outlining discovered vulnerabilities, make suggested recommendations to remediate and/or mitigate those vulnerabilities. Students also learn how to describe the findings wherein non-technical personnel understand the ramifications of these vulnerabilities in a business sense. This course prepares students for the EC Council Certified Ethical Hacker (CEH) certification. *FORMERLY IAE-410 NOTE: Students enrolled in this course incur an additional lab fee of $100.

IAE-402 Introduction to Incident Handling and Malicious Software (3 Credits)
This course provides a detailed understanding of incidents from attacks of malicious software. This course addresses the history and practice of coding that occurs in viruses, worms, spyware, Trojan horses, remote management back doors and root kits. Students learn preventative measures and tools, and explore how to rid systems of malicious software and prevent re-infection. Recovery processes and backup methods are explored. In addition to covering basic incident handling preparation, response and recovery practices, the course goes into detail regarding malicious software. NOTE: Students enrolled in this course incur an additional lab fee of $100.

IAE-405 Malware Analysis and Reverse Engineering (3 Credits)
This course introduces students to malware research and analysis. The course will provide students an overview of malware research, intelligence gathering related to malware, and provide students basic skills required to analyze and dis-assemble malicious programs. Students will explore the tools required for analysis and reverse engineering of malicious code, learn malware defense techniques, how malware functions, and will perform live analysis and reverse engineering exercises. NOTE: Students enrolled in this course incur an additional lab fee of $100.

IAE-406 Digital Forensics and the Investigative Process (3 Credits)
Students explore forensics and the investigation processes. Students explore current computer forensics tools, conduct live computer forensic analysis, conduct e-mail investigations, recovery of graphics files and data carving, and engage in report writing for high-tech investigations. This course prepares students for the AccessData Certified Examiner (ACE) and Mobile Phone Examiner Plus (MPE+) Certifications. Lab fee required. NOTE: Students enrolled in this course incur an additional lab fee of $100.

SDE-457 Senior Design Project 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.

SDE-458 Senior Design Project II (3 Credits)
Students/teams build and test their selected designs (completed in IAE-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. *Note: Course must be completed with a grade of "C" or higher to meet undergraduate graduation requirements.

Mathematics Courses (13 Credits)

MA-112 Algebra (3 Credits)
Designed for students needing mathematical skills and concepts for MA-114 and MA-261. In this course students are introduced to equations and inequalities and learn the language of algebra and related functions, including polynomial, rational, exponential and logarithmic functions. Other topics include solving equations, inequalities and systems of linear equations; performing operations with real numbers, complex numbers and functions; constructing and analyzing graphs of functions; and using mathematical modeling to solve application problems.

MA-124 Discrete Mathematics (3 Credits)
This course focuses on logic sets and sequences; algorithms, divisibility, and matrices; proof, induction, and recursion; counting methods and probability; relations, closure and equivalence relations, graphs and trees; and Boolean algebra.

MA-128 Introduction to Statistics (3 Credits)
This course addresses probability: definitions, theorems, permutations and combinations; binomial, hypergeometric, Poisson and normal distributions; sampling distribution and central limit theorem; and estimation and hypothesis testing.

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.

English, Humanities, and Social Science Courses (27 Credits)

EN-101 English Communications I (3 Credits)
Emphasizes the development of college-level writing skills, with focus on clarity, organization, and support in essays and short reports. Students practice critical reading and writing related to academic and professional topics.

EN-102 English Communications II (3 Credits)
Builds on EN 101 with emphasis on research, documentation, and advanced composition. Students learn to locate, evaluate, and integrate sources into written work using appropriate citation formats.

HU-331 Arts and Ideas (3 Credits)
This course explores major artistic movements and cultural ideas that have shaped human expression across history. Students examine works from visual art, literature, music, architecture, and film to understand how artistic forms reflect social values, philosophical perspectives, and historical contexts. Emphasis is placed on critical interpretation, aesthetic analysis, and the relationship between creativity, culture, and technological change. Through readings, discussions, and analytical projects, students develop a deeper appreciation for the arts and their role in shaping human experience.

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.

Humanities Elective (3 Credits)
Student-selected course in humanities disciplines such as literature, philosophy, or history.

Humanities Elective (3 Credits)
Additional humanities course supporting cultural and intellectual breadth.

Social Science Elective (3 Credits)
Student-selected course in social sciences such as psychology, sociology, or political science.

Social Science Elective (3 Credits)
Additional social science course supporting societal and behavioral understanding.

Science Elective – Physics or Chemistry (3 Credits)
Introduces foundational scientific principles relevant to engineering, cybersecurity, and aerospace systems.

5. Discuss How General Education Requirements Will Be Met, if Applicable

The Bachelor of Science in Aerospace Cybersecurity fully satisfies the general education requirements defined by the Maryland Higher Education Commission (MHEC) and the

standards outlined in COMAR 13B.02.03. General education is intentionally embedded throughout the curriculum to ensure that students develop strong communication skills, critical thinking abilities, ethical reasoning, and an understanding of social, cultural, and civic responsibility relevant to professional practice in aerospace, aviation, and cybersecurity environments.

The program includes 27 credits of general education coursework, consisting of English composition (EN-101 and EN-102), humanities and critical thinking (HU-331 and a humanities elective), and social sciences including SS-351 Ethics. These courses support written and oral communication, analytical reasoning, ethical awareness, and understanding of human and societal factors that influence decision-making in aerospace operations, cybersecurity, and critical-infrastructure protection.

Quantitative reasoning and scientific literacy are addressed through required coursework in algebra, discrete mathematics, statistics, calculus, physics or chemistry, and foundational programming. Collectively, these requirements

ensure that students graduate with a broad intellectual foundation that supports informed technical decision-making, professional responsibility, and effective participation in aerospace cybersecurity and aviation security fields

6. Identify Any Specialized Accreditation or Graduate Certification Requirements

The Bachelor of Science in Aerospace Cybersecurity is not a licensure-based or certification-mandated program and does not seek specialized programmatic accreditation. The program is intentionally structured as an applied, industry-aligned degree designed to prepare students for roles in aerospace cybersecurity, aviation security operations, and the protection of cyber-physical aerospace systems, rather than pilot licensure or FAA technical certification.

The program adheres to all institutional and state requirements governing undergraduate degree programs and is subject to Capitol Technology University's internal academic review, assessment processes, and continuous improvement procedures. Program quality is maintained through curriculum oversight, qualified faculty, industry advisory input, and alignment with regional and national workforce needs in aerospace and cybersecurity.

While the degree itself does not confer professional licensure eligibility, coursework within the program may support preparation for industry-recognized cybersecurity and aviation-security credentials where appropriate. Examples may include certifications related to cybersecurity operations, network defense, risk management, or aviation safety and security frameworks. Preparation for such credentials is embedded within relevant courses but is not required for degree completion.

7. If Contracting with Another Institution or Non-Collegiate Organization, Provide a Copy of the Written Contract

This program does not involve any contractual agreements with another institution or non-collegiate organization. All instruction, curriculum development, academic oversight, and student support services for the Bachelor of Science in Aerospace Cybersecurity will be provided directly by Capitol Technology University using its existing faculty, facilities, and administrative resources.

8. Provide Assurance and Any Appropriate Evidence That the Proposed Program Will Provide Students with Clear, Complete, and Timely Information

Capitol Technology University affirms that students enrolled in the Bachelor of Science in Aerospace Cybersecurity will be provided with clear, complete, and timely information regarding all aspects of the program. This includes curriculum structure, course sequencing, degree requirements, faculty interaction, technology expectations, academic support services, and financial policies.

Information will be communicated through the following mechanisms:

a. The program curriculum, course descriptions, credit requirements, and degree expectations will be published in the university academic catalog and maintained on the program webpage. These materials are reviewed and updated regularly to ensure accuracy and compliance with institutional and state requirements.

b. Each student is assigned an academic advisor upon enrollment to support degree planning, prerequisite tracking, and timely progress toward graduation.

c. Course syllabi clearly outline instructional format, assessment methods, faculty availability, and communication expectations. Faculty-student interaction occurs through classroom instruction, advising sessions, office hours, and senior project mentoring.

d. Students are informed of assumptions related to computer literacy and required software skills. Any required technical equipment, such as laptops or software applications, is communicated in advance, with minimum hardware and software specifications published by the Office of Information Technology.

e. Canvas serves as the university's official learning management system and is used to deliver course materials, manage assignments, facilitate communication, and provide feedback. Training and technical support are available to students throughout the program.

f. Academic support services, including tutoring, library resources, writing assistance, and career development services, are available and described in the student handbook, academic catalog, and university website.

g. Information regarding tuition, fees, billing procedures, payment plans, and financial aid is provided by the Business Office and Financial Aid Office, including guidance on scholarships, federal aid, military benefits, and institutional funding options.

9. Provide Assurance and Any Appropriate Evidence That Advertising, Recruiting, and Admissions Materials Will Clearly and Accurately Represent the Proposed Program and the Services Available

Capitol Technology University affirms that all advertising, recruiting, and admissions materials related to the Bachelor of Science in Aerospace Cybersecurity will clearly and accurately represent the program, its curriculum, intended outcomes, and available student services.

The Office of Marketing and Communications works in collaboration with the Office of Admissions and the academic department to ensure that all promotional and recruitment materials are:

a. Factually accurate and reflective of the approved curriculum and degree requirements;
b. Consistent with the university's mission and commitment to academic integrity;
c. Reviewed and updated regularly to reflect program or policy changes.

Recruitment materials—including the university website, digital and print media, social media content, and admissions presentations—will provide transparent information regarding:

a. Program objectives and airport security focus;
b. Credit requirements, course structure, and instructional modalities;
c. Technology and equipment expectations;
d. Opportunities for academic advising, academic support, and career services;
e. Tuition, fees, and financial aid options.

Admissions counselors and faculty involved in recruitment activities will receive program-specific training to ensure consistent, accurate communication during outreach efforts, recruitment events, and transfer engagement activities.

H. Adequacy of Articulation

1. If Applicable, Discuss How the Program Supports Articulation With Programs at Partner Institutions

Capitol Technology University maintains established articulation and transfer agreements designed to facilitate student mobility, degree completion, and collaborative program development. These agreements support the proposed Bachelor of Science (B.S.) in Aerospace Cybersecurity by enabling qualified students from partner institutions to transfer seamlessly into the program.

The B.S. in Aerospace Cybersecurity is intentionally structured to be transfer-friendly. Lower-division coursework in cybersecurity, computer science, aviation operations, information technology, mathematics, and general education is aligned with commonly offered associate degree programs at Maryland community colleges and other partner institutions. This alignment supports efficient credit transfer while preserving the academic rigor and integrity of the bachelor’s program.

Capitol Technology University currently maintains articulation agreements with institutions including Cecil College, the Community College of Baltimore County (CCBC), and other Maryland community colleges offering associate degrees in cybersecurity, information systems, aviation operations, technology, and related disciplines. These existing agreements provide a framework for incorporating the Aerospace Cybersecurity program into formal transfer pathways.

Under updated and expanded articulation agreements, students completing associate-level coursework in cybersecurity, aviation operations, information technology, or related fields may transfer into the B.S. in Aerospace Cybersecurity at junior standing, provided they meet established academic criteria. Transfer credit evaluation follows institutional policy and ensures that accepted coursework aligns with program learning outcomes and prerequisite sequencing.

The curriculum has been designed to maximize acceptance of transfer credit in general education, foundational cybersecurity, programming, mathematics, and aviation-related coursework. This structure allows transfer students—including veterans, military-affiliated learners, and working professionals—to complete upper-division aerospace cybersecurity coursework within a standard two-year timeframe following transfer.

In addition to postsecondary partnerships, Capitol Technology University maintains engagement with secondary education institutions and workforce development initiatives. These relationships support early exposure to cybersecurity and aviation-technology pathways and encourage smooth transitions into undergraduate STEM programs.

The University will continue to pursue additional articulation agreements with Maryland community colleges, technical institutions, and workforce partners to strengthen statewide access to aviation and aerospace cybersecurity education. These efforts align with Maryland's higher education goals of promoting transfer efficiency, reducing time to degree, and supporting workforce development in high-demand technical fields.

I. Adequacy of Faculty Resources

1. Provide a Brief Narrative Demonstrating the Quality of Program Faculty

The Bachelor of Science in Aerospace Cybersecurity is supported by a qualified and interdisciplinary faculty team composed of full-time faculty, professors of practice, and adjunct instructors. Collectively, these faculty bring expertise in cybersecurity operations, aviation systems, cyber-physical infrastructure protection, digital forensics, unmanned systems, regulatory compliance, systems engineering, and organizational leadership. This breadth of knowledge ensures that students receive rigorous, applied instruction aligned with workforce expectations in aviation cybersecurity, airport technology protection, and aerospace system security.

The program is administered within the School of Engineering and Technology, with collaboration from the School of Business and Information Technology. Faculty members

possess advanced academic credentials and significant industry and government experience, including service in cybersecurity operations centers (SOCs), aviation and aerospace environments, federal cybersecurity framework implementation (NIST, FAA, DHS), and critical infrastructure protection. Instruction is grounded in both theoretical foundations and practical application.

Foundational coursework in cybersecurity, programming, quantitative analysis, and general education is delivered by established full-time faculty across the institution. Upper-division aerospace cybersecurity and cyber-physical systems courses are taught by faculty with experience in aircraft network security, airport operational technologies, aerospace systems engineering, cyber-risk management, and aviation regulatory environments. This structure ensures appropriate instructional depth, curricular continuity, and subject-matter specialization.

Summary of Faculty Qualifications and Teaching Responsibilities

Full-Time Faculty

Dr. Andrew Mehri, Ph.D. in Computer Science, holds additional degrees in information architecture and electronics engineering. He contributes expertise in technical systems, programming, and applied cybersecurity instruction.

Dr. Jeff Chi, Ph.D. in Project Management (University of Maryland), brings extensive professional experience managing infrastructure and technology projects. He supports coursework in project management and professional practice.

Dr. Tahani Baabdullah, Ph.D. in Computer Science, specializes in artificial intelligence, machine learning, cybersecurity, and data analytics. She teaches advanced programming and computational courses.

Dr. Nisma M. Omar, Ph.D. in Analytical Chemistry, supports quantitative reasoning and mathematics instruction essential to analytical literacy.

Dr. Gregory P. Behrmann, Ph.D. in Mechanical Engineering, contributes expertise in applied engineering and physics supporting systems-level understanding.

Dr. Kellep Charles, Ph.D. in Cybersecurity, teaches information assurance, network security, and applied cybersecurity courses.

Mr. Frank E. Turney, J.D., FAA-certified pilot and Chair of Aviation, contributes aviation operations, regulatory, and safety expertise.

Prof. Jeff Volosin, B.S. in Space Science with over 38 years of NASA and aerospace industry experience, contributes systems engineering and space systems instruction.

Dr. Craig Capano, Ph.D. in Civil Engineering, experienced academic leader and industry professional.

Mr. Chris Urdzik, aviation education leader with extensive international aviation management experience.

Professor of Practice (Part-Time)

Ms. Suzanne Hall, M.S., retired U.S. Air Force officer with extensive aviation operations experience.

Ms. Mary Smikle Peoples, experienced higher education administrator and business professional.

Adjunct Faculty (Part-Time)

Ms. Megan Miskovish, M.S. in Education, supports writing and communication coursework.

Faculty Teaching Assignments (Aerospace Cybersecurity Program)

Faculty Member	Appointment Type	Course Numbers
Mr. Frank Turney	Full-Time	AVT-201, AVT-251, AVT-256
Prof. Jeff Volosin	Full-Time	AE-150, AE-210, AE-250
Ms. Suzanne Hall	Professor of Practice (Part-Time)	AE-325, AE-350, AE-455
Dr. Andrew Mehri	Full-Time	CS-120, CS-150, CS-200, CS-220, IAE-390, IAE-402
Dr. Jeff Chi	Full-Time	BUS-301
Ms. Mary Smikle Peoples	Professor of Practice (Part-Time)	SDE-457, SDE-458
Dr. Tahani Baabdullah	Full-Time	CS-230, CS-250, CS-300, CS-418, IAE-405, IAE-406
Dr. Nisma Omar	Full-Time	MA-112, MA-124, MA-128, MA-261
Dr. Gregory P. Behrmann	Full-Time	PH-201, CH-120
Dr. Kellep Charles	Full-Time	IAE-201, IAE-250, IAE-260, IAE-325, IAE-350
Ms. Megan Miskovish	Adjunct Faculty (Part-Time)	EN-101, EN-102, HU-331
Dr. Craig Capano	Full-Time	Humanities Elective
Mr. Chris Urdzik	Full-Time	Social Science Elective

This staffing plan ensures adequate instructional coverage, appropriate faculty specialization, and continuity across lower-division, upper-division, and capstone coursework.

2. Demonstrate How the Institution Will Provide Ongoing Pedagogy Training for Faculty in Evidence-Based Best Practices

Capitol Technology University is committed to continuous faculty development and instructional excellence. The Center for Innovation in Teaching and Learning (CITL) provides structured professional development programs focused on evidence-based pedagogy, instructional technology integration, and student engagement.

a) Pedagogy That Meets the Needs of Students

Faculty participate in professional development activities emphasizing active learning strategies, formative assessment, inclusive teaching practices, experiential learning, and case-based instruction. Applied projects, team-based learning, and industry-relevant simulations are emphasized in aerospace cybersecurity coursework to support diverse learners, including transfer students, veterans, and working professionals.

b) Learning Management System

Canvas serves as the University's official learning management system. Faculty receive initial onboarding and ongoing training in course design, accessibility standards, assessment tools, rubric development, and effective communication practices. Support is provided through workshops and individualized consultations.

c) Evidence-Based Best Practices for Distance Education

Although the program is primarily delivered face-to-face, selected courses may be offered in hybrid or online modalities. Faculty teaching in these formats receive additional training in distance education best practices, including course organization, engagement strategies, academic integrity safeguards, and technology-supported instruction. These practices ensure instructional quality and student success across modalities.

J. Adequacy of Library Resources

1. Describe the Library Resources Available and Measures to Be Taken to Ensure Resources are Adequate to Support the Proposed Program

Capitol Technology University's Puente Library provides comprehensive academic and research support for students and faculty enrolled in the Bachelor of Science in Aerospace Cybersecurity. The library maintains a balanced collection of physical and electronic resources that are regularly evaluated and updated to align with curriculum content, student learning outcomes, and workforce-oriented educational objectives in

cybersecurity, aviation systems, aerospace operations, and critical infrastructure protection.

Students in the program have access to a broad range of scholarly journals, eBooks, technical publications, and reference materials in cybersecurity, aerospace engineering, aviation operations, information technology, digital forensics, systems security, and regulatory compliance. Major electronic databases include ProQuest, JSTOR, EBSCO Business Source, ScienceDirect, SpringerLink, and other multidisciplinary research platforms that provide full-text access to peer-reviewed journals, conference proceedings, applied research studies, and industry analyses relevant to aviation and aerospace cybersecurity.

The Puente Library also provides access to technical standards and government publications essential to the Aerospace Cybersecurity curriculum. These include Federal Aviation Administration (FAA) publications, Department of Homeland Security (DHS) cybersecurity frameworks, National Institute of Standards and Technology (NIST) standards and special publications, International Civil Aviation Organization (ICAO) guidance materials, and other regulatory and policy documents. These resources directly support coursework in aviation systems, aerospace communications, cybersecurity governance, digital forensics, risk management, and senior design projects.

In addition to discipline-specific materials, the library supports the program's general education and quantitative components through access to resources in mathematics, statistics, ethics, social sciences, and communication studies. Textbooks and supplemental instructional materials are available in print and electronic formats, ensuring accessibility for traditional students, transfer students, veterans, and working professionals.

Library services extend beyond collections to include individualized research consultations, interlibrary loan services, citation management assistance, and information literacy instruction. Students receive guidance in identifying credible sources, evaluating technical and regulatory materials, and applying scholarly research to aviation and aerospace cybersecurity challenges. These services support both course assignments and the two-semester senior design sequence.

Measures to Ensure Adequate Support

The University maintains an ongoing review process to ensure that library resources remain current and sufficient to support the Aerospace Cybersecurity program. Annual assessments of library holdings are conducted in collaboration with program faculty and academic leadership to identify emerging needs related to cybersecurity frameworks, aviation regulations, aerospace systems technologies, and cyber-physical infrastructure protection.

Faculty may submit acquisition requests for books, journals, standards documents, case studies, and specialized databases that support evolving curriculum requirements. Requests are evaluated based on program growth, course development, enrollment trends, and industry developments in aviation and cybersecurity.

The University will continue to expand digital collections and database subscriptions to ensure equitable access for both on-campus and remote learners. As the program matures, additional targeted acquisitions in aerospace cybersecurity, aviation network security, unmanned systems protection, and regulatory compliance will be prioritized to maintain alignment with workforce expectations and technological advancements.

Through continuous review, targeted acquisitions, and robust research support services, Capitol Technology University ensures that the Puente Library provides adequate and sustainable resources to support the academic rigor and applied focus of the Bachelor of Science in Aerospace Cybersecurity.

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

1. Provide an Assurance That Physical Facilities, Infrastructure, and Instructional Equipment Are Adequate to Initiate the Program

Capitol Technology University affirms that it possesses the physical facilities, infrastructure, and instructional equipment necessary to successfully initiate and sustain the Bachelor of Science in Aerospace Cybersecurity program. The University maintains modern classrooms designed to support lecture-based instruction, collaborative learning, applied exercises, and technology-enhanced delivery. These classrooms are equipped with multimedia projection systems, instructional technology interfaces, high-speed wireless connectivity, and presentation tools that support coursework in cybersecurity, aviation systems, aerospace operations, and applied computing.

The Aerospace Cybersecurity program will utilize existing instructional spaces that currently support cybersecurity, computer science, astronautical engineering, and aviation programs. These facilities are sufficient to meet projected enrollment and instructional needs at program launch and during the initial years of operation. No additional capital construction or major facility modification is required to implement the program.

Applied instruction is supported by existing cybersecurity laboratories and virtualized learning environments. Students will have access to:

- Dedicated cybersecurity laboratory spaces supporting network security, penetration testing, digital forensics, malware analysis, and secure systems administration.
- Virtualized cyber-range environments that simulate real-world cyber incidents and network defense scenarios.
- Aerospace and aviation instructional resources used in existing astronautical engineering and aviation programs.
- Industry-standard software applications for network defense, secure coding, systems analysis, risk assessment, and cyber-physical infrastructure evaluation.

These instructional resources support experiential learning in aerospace system security, aircraft and airport network protection, incident response, regulatory compliance, and critical infrastructure defense.

Faculty offices and administrative workspaces are adequate to support academic advising, student mentoring, curriculum oversight, and program administration. Office allocations are reviewed periodically to ensure alignment with enrollment growth and faculty staffing levels.

The University's information technology infrastructure supports instructional delivery across all modalities. This includes campus-wide wireless connectivity, secure network architecture, cloud-based instructional platforms, centralized data storage, and technical support services. The infrastructure is maintained and regularly upgraded to ensure reliable instructional operations and data security.

Collectively, existing facilities, laboratories, software resources, and IT systems are adequate to initiate and sustain the Aerospace Cybersecurity program without additional infrastructure expansion at launch.

2. Provide Assurance That the Institution Will Ensure Students Enrolled in and Faculty Teaching in Distance Education Will Have Adequate Access To

a) An Institutional Electronic Mailing System

All students and faculty are provided with official university email accounts through Microsoft Office 365. These accounts serve as the institution's primary communication platform for academic announcements, advising communication, course-related correspondence, and administrative notifications. Use of official institutional email ensures secure, consistent, and documented communication across the University community.

b) A Learning Management System That Provides the Necessary Technological Support for Distance Education

Canvas serves as Capitol Technology University's official learning management system. Canvas supports both face-to-face and hybrid or online instructional delivery and provides tools for content distribution, assignment submission, grading, discussion forums, collaborative group work, multimedia integration, and assessment management.

Faculty receive initial and ongoing training in effective course design, assessment strategies, accessibility compliance, and student engagement within Canvas. Students are provided orientation resources and ongoing technical support to ensure effective participation in online or hybrid coursework. The University's Information Technology department provides help desk services to assist both students and faculty with system access, troubleshooting, and platform functionality.

Through these systems and support services, the University ensures that students and faculty engaged in distance education components of the Aerospace Cybersecurity program have reliable and adequate technological access.

L. Adequacy of Financial Resources With Documentation

1. Complete Table 1: Resources and Narrative Rationale

The Bachelor of Science in Aerospace Cybersecurity will be implemented using existing instructional facilities, infrastructure, and academic support resources currently available at Capitol Technology University. The University is well positioned to support the program through existing classrooms, faculty offices, instructional technologies, and aerospace and cybersecurity-related academic resources. No new capital investment is required for program launch.

TABLE 1: RESOURCES

Resource Categories	Year 1	Year 2	Year 3	Year 4	Year 5
1. Reallocated Funds	$0	$0	$0	$0	$0
2. Tuition/Fee Revenue (c + g below)	$350,060	$707,940	$1,065,072	$1,449,072	$1,851,644
a. Number of F/T Students	8	16	24	32	40
b. Annual Tuition/Fee Rate	$27,808	$28,503	$29,216	$29,946	$30,695
c. Total F/T Revenue (a × b)	$222,464	$465,048	$701,184	$958,272	$1,227,800
d. Number of P/T 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 P/T Revenue (d × e × f)	$127,596	$242,892	$363,888	$490,800	$623,844
3. Grants, Contracts and Other External Sources	$0	$0	$0	$0	$0
4. Other Sources	$0	$0	$0	$0	$0
TOTAL (Add 1–4)	**$350,060**	**$707,940**	**$1,065,072**	**$1,449,072**	**$1,851,644**

Narrative Rationale for Table 1: Program Resources

a) Reallocated Funds
No reallocated funds are required for the Bachelor of Science in Aerospace Cybersecurity. The program leverages existing academic infrastructure, instructional spaces, and faculty expertise in cybersecurity, aviation, astronautical engineering, and applied technology. No existing programs will be reduced or eliminated to support this initiative. The interdisciplinary structure of the curriculum allows the University to utilize established courses, laboratories, and faculty resources already supporting related academic programs.

b) Tuition and Fee Revenue
Tuition and fee revenue projections are based on conservative enrollment assumptions, beginning with 8 full-time and 7 part-time students in Year 1 and increasing to 40 full-

time and 31 part-time students by Year 5. Tuition rates reflect current published rates with an assumed annual increase of approximately 2.5 percent.

Part-time enrollment projections assume an average annual course load of 12 credit hours per student. These assumptions are consistent with enrollment patterns observed in existing cybersecurity, aviation, and technology programs and support sustainable instructional staffing, advising, and academic services.

Projected enrollment growth and tuition revenue are sufficient to sustain operational costs, including faculty compensation, instructional materials, academic support services, and continuous program development.

c) Grants, Contracts, and External Sources
No external funding is included in the initial financial model. However, the University may pursue competitive grants, transportation-sector partnerships, federal cybersecurity initiatives, and industry-supported programs in future years to enhance experiential learning and workforce engagement.

d) Other Sources
No additional funding sources are anticipated at launch. Future opportunities may include philanthropic support, employer-sponsored training partnerships, or state-supported workforce development initiatives aligned with aerospace cybersecurity.

2. Complete Table 2: Program Expenditures and Narrative Rationale

TABLE 2: EXPENDITURES

Expenditure Category	Year 1	Year 2	Year 3	Year 4	Year 5
1. Faculty (b + c)	$113,468	$155,071	$238,421	$325,843	$417,486
a. # FTE	1.5	2	3	4	5
b. Total Salary	$94,557	$129,226	$198,684	$271,536	$347,905
c. Total Benefits (20%)	$18,911	$25,845	$39,737	$54,307	$69,581
2. Administrative Staff (b + c)	$5,942	$6,091	$6,244	$6,400	$6,559
a. # FTE	0.08	0.08	0.08	0.08	0.08
b. Total Salary	$4,952	$5,076	$5,203	$5,333	$5,466
c. Total Benefits	$990	$1,015	$1,041	$1,067	$1,093
3. Support Staff (b + c)	$59,885	$92,076	$125,837	$161,230	$198,313
a. # FTE	1	1.5	2	2.5	3
b. Total Salary	$49,905	$76,730	$104,864	$134,358	$165,261
c. Total Benefits	$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 (Add 1–7)	**$185,985**	**$268,873**	**$398,192**	**$535,948**	**$682,588**

Narrative Rationale for Table 2: Program Expenditures

a) Faculty
Faculty costs include salaries and benefits (estimated at 20 percent) for instructors teaching courses in cybersecurity, aerospace systems, aviation operations, cyber-physical infrastructure protection, and the senior design sequence. Faculty staffing increases from 1.5 FTE in Year 1 to 5 FTE by Year 5, reflecting enrollment growth and expansion of upper-division coursework. Instruction will be delivered through a combination of full-time faculty and qualified adjunct faculty with industry and government experience.

b) Administrative Staff
A fractional administrative allocation (0.08 FTE) supports advising coordination, scheduling, enrollment management, and reporting functions. Cost increases reflect standard annual adjustments.

c) Support Staff
Support staff include academic support personnel, laboratory coordination, advising support, and instructional assistance required for cybersecurity laboratories, simulation environments, applied aerospace coursework, and capstone projects. Staffing levels increase proportionally with enrollment growth.

d) Technical Support and Equipment
These costs cover instructional software licenses, cybersecurity simulation tools, virtual lab environments, aviation and aerospace system modeling tools, regulatory and standards database access (FAA, DHS, NIST), and technology maintenance. These resources support applied, industry-aligned instruction.

e) Library
No additional library expenditures are required at program launch. Existing electronic databases, regulatory publications, and technical standards adequately support the curriculum.

f) Facilities
No new construction or renovation is required. Existing classrooms, laboratories, and instructional spaces are sufficient to support the Aerospace Cybersecurity program.

g) Other Expenses
Other expenses include marketing, recruitment activities, faculty development, program assessment, accreditation compliance support, and continuous improvement initiatives. These costs scale proportionally with projected enrollment growth.

M. Adequacy of Provisions for Evaluation of Program

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

Capitol Technology University maintains a structured and systematic process for evaluating courses, faculty performance, and student learning outcomes to ensure continuous improvement and academic quality.

Course Evaluation

Each course in the B.S. Aerospace Cybersecurity program includes clearly defined course-level learning outcomes that are mapped to program-level outcomes. Course effectiveness is evaluated through:

- Analysis of student performance on exams, laboratory exercises, applied projects, simulations, and written assignments;
- Review of grade distributions and achievement of benchmark performance thresholds;
- Student course evaluations administered at the conclusion of each term;
- Faculty peer review and chair oversight, where applicable.

Assessment results are reviewed during departmental meetings and scheduled program review cycles to identify strengths, address gaps, and guide curricular and instructional improvements. This structured review process ensures that course content remains aligned with evolving aerospace cybersecurity practices, regulatory expectations, and workforce needs.

Faculty Evaluation

Faculty are evaluated through established institutional procedures that include:

- Annual performance reviews conducted by academic leadership;
- Review of teaching effectiveness based on student evaluations and course assessment data;
- Peer observations, where applicable;
- Evaluation of professional development, scholarship, industry engagement, and service contributions.

These processes ensure that instructional quality remains high and that faculty maintain currency in cybersecurity, aviation systems, and aerospace-related technologies.

Evaluation of Student Learning Outcomes

Student learning outcomes are assessed through both direct and indirect measures. Direct measures include examinations, laboratory assignments, cybersecurity simulations, applied aerospace case studies, technical reports, and capstone deliverables. Indirect measures include student surveys, internship feedback, and advisory board input.

In the B.S. Aerospace Cybersecurity program, the culminating academic experience is the two-semester Senior Design sequence (SDE-457 and SDE-458). Senior Design provides students with a structured, faculty-guided environment in which they apply cybersecurity engineering principles to aviation and aerospace systems. Students progress through formal design stages including:

- Problem definition and threat identification;
- Requirements analysis and regulatory alignment;
- Secure system architecture development;
- System modeling and testing strategies;
- Validation against FAA, DHS, and NIST frameworks;
- Final prototype demonstration and technical defense.

Senior Design emphasizes analytical rigor, secure-by-design methodologies, aviation system awareness, cyber-physical infrastructure protection, and professional documentation. Successful completion of this sequence demonstrates the student's ability to integrate cybersecurity expertise with aviation system operations and regulatory compliance requirements. This experience serves as a comprehensive measure of readiness for professional practice.

2. Explain How the Institution Will Evaluate the Proposed Program's Educational Effectiveness

The educational effectiveness of the Bachelor of Science in Aerospace Cybersecurity will be evaluated using quantitative and qualitative measures aligned with Capitol Technology University's institutional assessment framework.

a) Assessment of Student Learning Outcomes

The program will maintain a systematic process for mapping, measuring, and reviewing learning outcomes related to:

- Aerospace cybersecurity principles;
- Aviation systems and network security;
- Cyber-physical infrastructure protection;
- Regulatory compliance and risk management;
- Professional communication and teamwork;
- Ethical and professional responsibility.

Each course includes embedded assessments aligned with program-level outcomes to ensure consistent measurement across the curriculum. Data from exams, laboratory exercises, cybersecurity simulations, applied projects, and the Senior Design sequence will be collected each semester and analyzed annually.

Faculty and academic leadership review assessment findings to identify trends, determine areas for improvement, and implement curriculum refinements. Industry advisory input is

incorporated to ensure that learning outcomes remain aligned with employer expectations and emerging aerospace cybersecurity challenges.

b) Student Retention and Graduation Rates

Program-level retention, progression, and graduation data will be monitored regularly. The University utilizes academic advising, early alert systems, tutoring services, and targeted student support initiatives to promote persistence and timely degree completion. Data-driven interventions will be implemented where necessary to address retention challenges.

c) Student and Faculty Satisfaction

Student satisfaction is evaluated through course evaluations, program-level surveys, advising feedback, and capstone reflections. Faculty satisfaction is assessed through annual reviews and institutional surveys addressing workload, instructional resources, and administrative support.

Findings are reviewed by academic leadership to inform program enhancements and resource allocation decisions.

d) Cost-Effectiveness

The Business and Finance Division, in collaboration with the Office of Academic Affairs, will conduct periodic reviews of enrollment trends, instructional expenditures, and resource utilization. These analyses ensure financial sustainability while maintaining instructional quality and student support services.

e) Industry and Advisory Input

The program will engage airport authorities, aerospace organizations, cybersecurity firms, and advisory board members in periodic review processes. Industry input will inform curriculum updates, emerging technology integration, regulatory alignment, and workforce skill development.

Through these coordinated evaluation processes, the University ensures that the B.S. Aerospace Cybersecurity program remains academically rigorous, industry-aligned, financially sustainable, and responsive to workforce needs in aviation and aerospace cybersecurity.

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

1. Discuss How the Proposed Program Addresses Minority Student Access and Success

The proposed Bachelor of Science in Aerospace Cybersecurity aligns with Maryland's minority student achievement goals as articulated in COMAR 13B.02.03.05 and the Maryland State Plan for Postsecondary Education. Capitol Technology University maintains a demonstrated institutional commitment to diversity, inclusion, and equitable access to career-focused STEM education, particularly in cybersecurity and aviation sectors where minority representation has historically been limited.

The Aerospace Cybersecurity program is intentionally structured to expand access to high-demand cybersecurity and aviation-technology careers for students from underrepresented populations, including African American, Hispanic/Latino, female, first-generation, military-affiliated, and adult learners. By integrating cybersecurity, aviation systems, and critical-infrastructure protection into a single interdisciplinary degree, the program provides an accessible entry point into a high-growth workforce sector without requiring a traditional engineering background.

The Bachelor of Science in Aerospace Cybersecurity supports minority student access and success through the following institutional strategies:

Transfer-Friendly Pathways
The University maintains articulation agreements and transfer partnerships with Maryland community colleges, many of which serve diverse and high proportions of minority students. Clear transfer maps, course equivalencies, and advising coordination support seamless entry into the program at the junior level, reducing excess credit accumulation and time to degree.

Comprehensive Academic Advising and Student Support
Students are assigned academic advisors upon enrollment. Early alert systems, tutoring services, writing support, and structured academic monitoring promote persistence and academic achievement. These services are designed to address barriers that may disproportionately affect first-generation and underrepresented students.

Financial Access and Affordability Initiatives
The University offers institutional scholarships, federal and state financial aid access, military and veteran education benefits, and flexible enrollment options. These measures reduce financial barriers and support economically disadvantaged and working students in completing their degrees.

Applied and Experiential Learning
The program incorporates case-based instruction, aviation-focused cybersecurity scenarios, hands-on laboratory exercises, internships, and a two-semester Senior Design sequence. Experiential learning has been shown to increase engagement and retention, particularly among students from diverse backgrounds who benefit from applied and career-connected instruction.

Inclusive Instructional Practices
Faculty participate in professional development that emphasizes culturally responsive teaching, Universal Design for Learning (UDL), inclusive pedagogy, and active learning methodologies. These practices ensure that instruction is accessible and responsive to students with varied learning styles, educational backgrounds, and lived experiences.

In addition, Capitol Technology University supports diversity through inclusive recruitment practices, outreach to underrepresented communities, multicultural programming, student organizations, and dedicated services for veterans and military-affiliated students. Equity and inclusion principles are integrated into institutional planning and academic governance processes.

Through these coordinated strategies, the Bachelor of Science in Aerospace Cybersecurity advances Maryland's minority student achievement priorities by:

- Expanding equitable access to high-demand cybersecurity and aviation-technology careers (Goal 1: Student Access);
- Promoting retention, persistence, and timely completion through structured academic support (Goal 2: Student Success);
- Strengthening workforce readiness in sectors critical to Maryland's economic development.

The program is therefore consistent with and supportive of the State's objectives for minority student access, achievement, and long-term professional advancement.

O. Relationship to Low Productivity Programs Identified by the Commission

1. If the Proposed Program is Directly Related to an Identified Low Productivity Program, Discuss How the Fiscal Resources May Be Redistributed to This Program

The proposed Bachelor of Science in Aerospace Cybersecurity is not directly related to, nor derived from, any low-productivity program identified by the Maryland Higher Education Commission. The program does not represent a continuation, consolidation, or restructuring of an existing low-enrollment academic offering. Rather, it has been developed through Capitol Technology University's formal academic planning and program development processes, informed by labor-market demand analysis, institutional strategic priorities, and enrollment forecasting in cybersecurity, aviation systems, and critical-infrastructure protection.

The Aerospace Cybersecurity program is a newly proposed, workforce-responsive degree designed to address documented demand for professionals capable of securing aviation systems, aircraft networks, airport operational technologies, unmanned systems, and aerospace cyber-physical infrastructure. The program is not dependent upon the

elimination, reduction, or redistribution of resources from any currently approved academic program.

Although not associated with a low-productivity program, the Bachelor of Science in Aerospace Cybersecurity is structured to ensure fiscally responsible implementation and efficient use of institutional resources. Specifically, the program will:

• Leverage existing faculty expertise in cybersecurity, aviation systems, astronautical engineering, information assurance, regulatory compliance, and organizational leadership. Faculty currently teaching in related programs will provide instructional coverage where appropriate, ensuring efficient allocation of instructional capacity.

• Utilize existing instructional facilities, including cybersecurity laboratories, aviation and aerospace instructional spaces, computer classrooms, and general academic facilities already supporting related degree programs. No duplication of facilities or capital expansion is required.

• Operate within established administrative, advising, library, and student support structures, thereby avoiding the creation of new overhead units or redundant services.

• Contribute to institutional productivity by attracting new student populations—including transfer students, adult learners, military-affiliated students, and working professionals—who may not otherwise enroll in traditional cybersecurity or aviation programs.

Through this approach, the Bachelor of Science in Aerospace Cybersecurity strengthens institutional efficiency and academic productivity by aligning existing faculty, facilities, and support services with high-demand workforce sectors. While not directly connected to a low-productivity program identified by the Commission, the proposed program reflects prudent resource management and strategic academic growth consistent with the University's long-term sustainability objectives.

P. Adequacy of Distance Education Programs

1. Provide Affirmation and Any Appropriate Evidence That the Institution is Eligible to Provide Distance Education

Capitol Technology University is authorized by the Maryland Higher Education Commission (MHEC) to offer distance education programs. The University has extensive experience delivering undergraduate and graduate programs in fully online, hybrid, and blended formats across disciplines including cybersecurity, engineering, computer science, business, and information technology.

Capitol Technology University is an approved participant in the National Council for State Authorization Reciprocity Agreements (NC-SARA). Participation in NC-SARA authorizes the University to provide distance education to students residing in other SARA member states and affirms compliance with interstate distance education

regulations. This participation demonstrates institutional adherence to nationally recognized standards governing distance education authorization, consumer protection, and academic quality.

The University maintains established administrative, academic, and technological systems to support online and hybrid delivery consistent with institutional and regulatory expectations.

2. Provide Assurance That the Institution Complies With the C-RAC Guidelines

Capitol Technology University affirms that it complies with the Council of Regional Accrediting Commissions (C-RAC) Interregional Guidelines for the Evaluation of Distance Education. Institutional policies, instructional practices, and student support services ensure that courses delivered through distance modalities maintain academic quality equivalent to face-to-face instruction.

Specifically, the University ensures that:

• Curriculum content, academic rigor, credit hour requirements, and learning outcomes are consistent across on-campus, hybrid, and online formats.
• Regular and substantive interaction between faculty and students is maintained through structured engagement, including scheduled virtual sessions (when applicable), discussion forums, assignment feedback, project mentoring, and direct communication.
• Student identity verification is conducted through secure authentication protocols within the Canvas learning management system and associated assessment platforms to safeguard academic integrity.
• Distance education students have full access to academic advising, tutoring services, library resources, writing assistance, technical support, disability services, and career development resources.
• Institutional technology infrastructure supports reliable access to course materials, communication tools, cybersecurity laboratory platforms, and virtual learning environments.
• Faculty assigned to teach online or hybrid courses receive training in instructional design, online pedagogy, accessibility standards, and effective use of the learning management system.

The Bachelor of Science in Aerospace Cybersecurity is designed to be delivered primarily in an on-campus modality, reflecting its emphasis on applied instruction, laboratory exercises, cybersecurity simulations, and project-based learning. However, selected courses—particularly in general education, computing fundamentals, management, and selected theoretical components—may be delivered in hybrid or online formats as appropriate. All distance-delivered components will adhere fully to institutional policies, C-RAC guidelines, and applicable accreditation and state requirements.