CAPITOL
Technology University

Bradford L. Sims, PhD
President

December 2, 2020

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

Dear Dr. Fielder,

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

The requirement for experts at the highest level in Space Cybersecurity now exists and is growing. This program is in response to that need. The **Ph.D. in Space Cybersecurity** degree is primarily for experienced Space Cybersecurity personnel who desire to advance in their careers by earning a doctoral degree.

We respectfully submit for approval a Doctor of Philosophy (Ph.D.) in Space Cybersecurity. The required proposal is attached as well as the letter from me, as university president, confirming the adequacy of the university's library to serve the needs of the students in this degree.

Respectfully,

Bradford Sims
Digitally signed by Bradford Sims
DN: cn=Bradford Sims, o, ou, email=bsims@captechu.edu, c=US
Date: 2020.12.02 16:14:30 -05'00'

Bradford L. Sims, PhD

CAPITOL
Technology University

Bradford L. Sims, PhD
President

December 2, 2020

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

Dear Dr. Fielder,

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

Respectfully,

Bradford Sims Digitally signed by Bradford Sims
DN: cn=Bradford Sims, o, ou, email=bsims@captechu.edu, c=US
Date: 2020.12.02 16:14:55 -05'00'

Bradford L. Sims, PhD

Office Use Only: PP#

MHEC
Creating a state of achievement

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

Institution Submitting Proposal	Capitol Technology University

Each action below requires a separate proposal and cover sheet.

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

Department Proposing Program	Department of Doctoral Programs	
Degree Level and Degree Type	Doctor of Philosophy (Ph.D.)	
Title of Proposed Program	Ph.D. in Space Cybersecurity	
Total Number of Credits	60	
Suggested Codes	HEGIS: 701	CIP: 29
Program Modality	○ On-campus ◉ Distance Education (*fully online*) ○ Both	
Program Resources	◉ Using Existing Resources ○ Requiring New Resources	
Projected Implementation Date	○ Fall ○ Spring ◉ Summer Year: 2021	
Provide Link to Most Recent Academic Catalog	URL: https://www.captechu.edu/current-students/academic-resources	
Preferred Contact for this Proposal	Name: Professor Soren Ashmall	
	Title: Director, Assessment and Accreditation	
	Phone: (571) 332-4344	
	Email: spashmall@captechu.edu	
President/Chief Executive	Type Name: Dr. Bradford Sims	
	Signature: Bradford Sims Digitally signed by Bradford Sims DN: cn=Bradford Sims, o, ou, email=bsims@captechu.edu, c=US Date: 2020.12.02 16:19:29 -05'00'	Date: 12/02/2020
Approval/Endorsement by Governing Board	Type Name: Dr. Bradford Sims	
	Signature: Bradford Sims Digitally signed by Bradford Sims DN: cn=Bradford Sims, o, ou, email=bsims@captechu.edu, c=US Date: 2020.12.02 16:19:53 -05'00'	Date: 12/02/2020

Revised 5/15/18

PROPOSAL FOR:

__X__NEW INSTRUCTIONAL PROGRAM

_____ SUBSTANTIAL EXPANSION/MAJOR MODIFICATION

_____ COOPERATIVE DEGREE PROGRAM

__X__WITHIN EXISTING RESOURCES or____REQUIRING NEW RESOURCES

CAPITOL Technology University

Institution Submitting Proposal

Summer 2021
Projected Implementation Date

Doctor of Philosophy (Ph.D.)
Award to be Offered

Doctor of Philosophy in Space Cybersecurity
Title of Proposed Program

0701
Suggested H.E.G.I.S. Code

29.0407
Suggested C.I.P. Code

Doctoral Programs
Department of Proposed Program

Dr. Ian McAndrew
Name of Department Head

Dr. Soren Ashmall
Director, Assessment and Accreditation

spashmall@captechu.edu
Contact E-Mail Address

571-332-4344
Contact Phone Number

Bradford Sims Digitally signed by Bradford Sims DN: cn=Bradford Sims, o, ou, email=bsims@captechu.edu, c=US Date: 2020.12.02 16:16:07 -05'00'

Signature and Date

President/Chief Executive Approval

December 2, 2020

Date

Date Endorsed/Approved by Governing Board

Proposed Doctor of Philosophy in Space Cybersecurity
Department of Doctoral Programs
Capitol Technology University
Laurel, Maryland

A. Centrality to Institutional Mission and Planning Priorities:

1. **Provide a description of the program, including each area of concentration (if applicable), and how it relates to the institution's approved mission.**

Doctor of Philosophy in Space Cybersecurity Program Description:

The **Doctor of Philosophy (Ph.D.) in Space Cybersecurity** degree is a unique program designed to meet the evolving needs of today's Space Cybersecurity in an ever-changing world of conflict. The **Ph.D. in Space Cybersecurity** program provides students with the opportunity to conduct extensive and sustained, original research at the highest level in the field of Space Cybersecurity. The **Ph.D. in Space Cybersecurity** is designed to meet the demands of the highest-skilled professionals to become leaders who will be involved in the advancement, expansion, and support of Space Cybersecurity on a national and international level. The **Ph.D. in Space Cybersecurity** is for current professionals in the field who desire to elevate their skills to the highest level and to contribute to the body of knowledge in Space Cybersecurity.

The proposed **Ph.D. in Space Cybersecurity** degree is for current professionals in the field. The degree provides a path for Space Cybersecurity personnel to explore new ground in the rapidly evolving world of commercial and governmental Space Cybersecurity. The University is in a unique position to give those students an avenue to pursue a deep proficiency in this area using an interdisciplinary methodology, cutting-edge courses, and dynamic faculty. Graduates will contribute significantly to the Space Cybersecurity field through the creation of new knowledge, ideas, and technology. The **Ph.D. in Space Cybersecurity** program is designed as a doctorate by research where students will quickly become able to engage in leadership, research, and publishing.

The **Ph.D. in Space Cybersecurity** program is structured for experienced professionals in the Space Cybersecurity field with an appropriate master's degree and professional experience. It is possible for a student with an appropriate master's degree and no professional experience to enter the program, but it would be less common than experienced professionals. During the program, students will conduct original research in an approved area of Space Cybersecurity. Successful completion of the program culminates in the award of the **Doctor of Philosophy (Ph.D.) in Space Cybersecurity** degree.

The completion of the **Ph.D. in Space Cybersecurity** program requires the student to produce, present, and defend a doctoral dissertation after receiving the required approvals from the student's Committee and the Ph.D. Review Board.

There are two options for completion of the **Ph.D. in Space Cybersecurity** program. Under the dissertation option, the student will produce, present, and defend a doctoral dissertation after receiving the required approvals from the student's Committee and the Ph.D. Review Board.

Under the publication option, the student will produce, present, and defend their original doctoral research after receiving the required approvals from the student's Committee and the Ph.D. Review Board. The student must also publish three works of original research in a scholarly peer-reviewed journal(s) of high stature. Two of the three published works may be in a peer reviewed conference proceeding if the conference is international.

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

Capitol Technology University operates on four strategic goals:

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

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

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

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

The proposed **Ph.D. in Space Cybersecurity** program supports all the University's four strategic goals. The proposed degree builds upon the existing areas of degrees at the undergraduate level: B.S. in Astronautical Engineering, B.S. in Aviation Professional Pilot, B.S. in Computer Engineering, B.S. in Computer Engineering Technology, B.S. in Computer Science, B.S. in Construction Information Technology and Cybersecurity, B.S. in Construction Management and Critical Infrastructure, B.S. in Construction Safety, B.S. in Counterterrorism, B.S. in Cyber Analytics, B.S. in Cybersecurity, B.S. in Data Science, B.S. in Electrical Engineering, B.S. in Electrical Engineering Technology, B.S. in Engineering Technology, B.S. in Facilities Management and Critical Infrastructure, B.S. in Information Technology, B.S in Management of Cyber and Information Technology, B.S. in Mechatronics Engineering, B.S. in Mechatronics and Robotics Engineering Technology, B.S. in Mobile Computing, B.S. in Professional Trades Administration, B.S. in Software Engineering, and B.S. in Technology and Business Management, B.S in Unmanned and Autonomous Systems, and B.S. in Web Development.

The proposed degree also supports the existing areas of degrees of graduate study, including the Master of Business Administration (M.B.A.), Master of Science (M.S.) in Astronautical Engineering, M.S. in Aviation, M.S. in Aviation Cybersecurity, M.S. in Computer Science, M.S. in Construction Cybersecurity, M.S. in Construction Safety, M.S. in Critical Infrastructure, M.S. in Cyber Analytics, M.S. in Cybersecurity, M.S. in Information Systems Management, M.S. in Engineering Technology, M.S. in Internet Engineering, M.S. in Product Management, M.S. in

Unmanned and Autonomous Systems Policy and Risk Management, Technical Master of Business Administration (T.M.B.A.) in Business Analytics and Data Science, and T.M.B.A. in Cybersecurity, Doctor of Science (D.Sc.) in Cybersecurity, Doctor of Philosophy (Ph.D.) in Artificial Intelligence, Ph.D. in Aviation, Ph.D. in Business Analytics and Data Sciences, Ph.D. in Construction Science, Ph.D. in Counterterrorism, Ph.D. in Critical Infrastructure, Ph.D. in Cybersecurity Leadership, Ph.D. in Emergency and Protective Services, Ph.D. in Human Factors, Ph.D. in Manufacturing, Ph.D. in Occupational Health and Safety, Ph.D. in Operational Technology, Ph.D. in Product Management, Ph.D. in Quantum Computing, Ph.D. in Technology, Ph.D. in Technology/M.S. Research Methods Combination Program, and Ph.D. in Unmanned Systems Applications.

The University's programs have been preparing professionals for the rapid advances in information technology, intense global competition, and increasingly sophisticated technological environments for decades. The **Ph.D. in Space Cybersecurity** follows that tradition.

The proposed **Ph.D. in Space Cybersecurity** is fully supported by the University's Vision 2025 and Strategic Plan 2017-2025. Funding to support the **Ph.D. in Space Cybersecurity** is already available within the existing budget.

The University has active partnerships in the private and public areas (e.g., Parson Corporation, Leidos, Patton Electronics, Lockheed Martin, Northrup Grumman, Cyber Security Forum Initiative, Internal Revenue Service, and National Cryptologic School). The **Ph.D. in Space Cybersecurity** degree will provide new opportunities for partnerships. The increase in alliances and the placement of our graduates in our partner institutions will serve to expand the University's enrollment and reputation. While additional students will increase financial resources, new partnerships, and grants in the Space Cybersecurity field will help diversify and increase financial resources.

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

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

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

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

      The proposed degree is an integral part of the University's Strategic Plan for FY 2017-2025 and forward. The institutional and departmental budgets for FY 2020-2021, as well as the forecasted budgets going forward, include funding for the administrative, financial, and technical support of the new degree.

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

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

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

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

a. The need for advancement and evolution of knowledge.

Space has become the latest cyber battleground. Many satellites in orbit were not designed with cybersecurity protection. In October 2020, the Wilson Center held an event, "Seeking Strategic Advantage: How Geopolitical Competition and Cooperation are Playing Out in Space," to highlight growing threat and the need for advancement in Space Cybersecurity.

Much of the world's critical infrastructure is heavily dependent on space, specifically space-based assets, for its daily functioning. Essential systems -- such as communications, air transport, maritime trade, financial services, weather monitoring and defense -- all rely heavily on space infrastructure, including satellites, ground stations and data links at the national, regional and international level. This dependence poses a serious, and yet frequently underrecognized, security dilemma -- especially cyber threats -- for critical infrastructure providers and policymakers alike.

Like any other increasingly digitized critical infrastructure, satellites and other space-based assets are vulnerable to cyberattacks. These cyber vulnerabilities pose serious risks not just for space-based assets themselves but also for ground-based critical infrastructure. If not contained, these threats could interfere with global economic development and, by extension, international security. What's more, these concerns are no longer merely hypothetical. Within the past decade, more countries and private actors have acquired and employed counter-space capabilities in novel applications, which now pose a greater existential threat to critical space assets.

Why are space systems vulnerable?

Many space systems are old, created before cybersecurity became a top policy priority. They have vulnerabilities like hardcoded credentials — used by ships, planes and the military — making access by sophisticated actors fairly easy.

We are witnessing a transformation of spaceflight from a public endeavor to a commercial industry. As more commercial actors can access space through commercial providers, they can provide a variety of services in space increasing the scope and scale of activity in this domain. The successful completion of NASA's SpaceX Demo-2 mission on August 2, 2020 made history by proving that space exploration is no longer a domain confined to the government agencies of wealthy space-faring nations and their academic affiliates. Not only will NASA no longer have to rely exclusively on Russia's

Roscosmos to transport its astronauts to the International Space Station (ISS) — saving more than $30 million per astronaut per trip — but SpaceX's Crew Dragon spacecraft will become the first certified commercial launch vehicle for operational human space transport. Today, modern technology is enabling states, international organizations, corporations and individuals alike to harness space capabilities when, just a decade ago, such a triumph was unthinkable. But this transformation of spaceflight from a public endeavor to a commercial industry raises questions about how to regulate the activities of private entities in space.

And more means more: the attack surface is becoming exponentially larger as more spacecraft connect with ground-based assets and users. But absent implementation of cybersecurity best practices by all companies operating in space, this poses a risk.

What are the vulnerabilities?

Vulnerabilities to space systems and infrastructure vary across a range of potential attack surfaces. As the Aerospace Corporation explains in a recent paper, there are four main segments of space infrastructure that need to be hardened against cyber attack. Spacecraft could be vulnerable to command intrusions (giving bad instructions to destroy or manipulate basic controls), payload control and denial of service (sending too much traffic to overload systems). Malware could be used to infect systems on the ground (like satellite control centers) and for users, and links between the two and spacecraft could be spoofed (disguising communication from an untrusted source as a trusted one) or suffer from replay (interrupting or delaying communication by malicious actors).

On an individual level, it might be easy to dismiss the dangers posed by vulnerabilities to space assets located hundreds or even thousands of miles away. But as Brian Weeden, Director of Program Planning at the Secure World Foundation, reminded us at the recent event, our inability to deter such interference could have large-scale and catastrophic effects. For instance, take GPS, a technology whose precision is often taken for granted. All it takes is the production of a relatively inexpensive spoofer, and an attacker is able to command and control the uplink signal to a satellite. If the downlink from a satellite is spoofed, false data can be injected into a target's communications systems, fooling the receiver — GPS — into calculating an incorrect position.

In the near-term, these kinds of attacks will likely remain posed by nation state actors but as more communications capabilities come online via space, the group of actors could expand to well-resourced non-state actors (e.g., criminal groups) seeking financial gain.

(Source: https://www.wilsoncenter.org/blog-post/cybersecurity-threats-space-roadmap-future-policy)

The evolution of senior leadership and effective use of advanced technology in Space Cybersecurity can only be achieved with a holistic and cutting-edge approach. Those advanced skills and strategies will be covered in this proposed degree.

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

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

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

While Capitol Technology University is not a historically black institution, the university is a diverse multiethnic and multiracial institution with a long history of serving minority populations. The University has a 51% minority student population, with 7% undisclosed. The Black/African American population is 34%. The University has a military/veteran population of 22%. The university also has a 22% female population – a significant percentage given its status as a technology institution. If approved, the proposed **Ph.D. in Space Cybersecurity** will expand the field of opportunities for minorities and disadvantaged students. Given the substantial minority population of Capitol Technology University, it is also reasonable to assert that the **Ph.D. in Space Cybersecurity** program will add to the base of minority participation in the Space Cybersecurity field.

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

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

1. Access
2. Success
3. Innovation

Goal 1: Access

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

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

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

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

Achievement gaps: The University provides leveling courses in support of individuals attempting a career change to a field of study not necessarily consistent with their current skills. There are situations where undergraduate courses best serve student needs in subject areas. The University makes those courses available.

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

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

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

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

The proposed **Ph.D. in Space Cybersecurity** program and University Financial Aid will be available to all Maryland residents who qualify academically for admission. The University has successfully managed to support Financial Aid for its students since its founding in 1927.

The **Ph.D. in Space Cybersecurity** program, with its academic rigor, will produce highly qualified Space Cybersecurity leaders with the highest level of skills and abilities to advance their careers. The University has a proven record of rigorous high-quality education in all of its degrees. The University is fully accredited by five accrediting organizations. The University receives its regional accreditation from the Middle States Commission on Higher Education (MSCHE). The University also has specialized accreditation from the International Accreditation Council of Business Education (IACBE), Accreditation Board for Engineering and Technology (ABET), National Security Agency (NSA), and Department of Homeland Security (DHS). The **Ph.D. in Space Cybersecurity** program is consistent with the MSCHE criteria for regional accreditation of the delivery of high-quality higher education.

Goal 2: Success

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

The courses for the **Ph.D. in Space Cybersecurity** degree will be offered online using the Canvas Learning Management System and Zoom. The University provides a tuition structure that is competitive with its competitors. The University tuition structure does not differentiate between in-state and out-of-state students. The University's Student Services provide advising, tutoring, virtual job fair attendance, and other activities supporting student completion and employment for both on-ground and online students.

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

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

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

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

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

Goal 3: Innovation

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

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

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

Example: The University engages its students in fusion projects that allow students to contribute their skills in interdisciplinary projects such as those in our Astronautical Engineering and Cyber Labs. In those labs, students become designers, builders, and project managers (e.g., to send a CubeSat on a NASA rocket) and data analysts (e.g., to analyze rainforest data for NASA). The University's students recently launched their latest satellite aboard a NASA rocket from a location in Norway at the beginning of the 2019 Fall Semester. The University is also recruiting additional partners for the proposed **Ph.D. in Space Cybersecurity** for which real-world projects will provide students integrative learning opportunities in the Space Cybersecurity field.

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

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

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

Graduates with the **Ph.D. in Space Cybersecurity** degree will be expected to fill technical executive and senior-level positions in commercial companies as well as local, state, and federal government with a variety of titles such as:

- Chief Executive Officer, Commerical Space Cybersecurity Company
- Chief Space Cybersecurity Operations Officer
- Chief Cybersecurity Officer, Space Vehicles
- Senior Director, Space Cybersecurity
- Cybersecurity Officer, U.S. Space Force
- Senior Scientist, Space Cybersecurity
- Senior Vice President, Space Cybersecurity

- Senior Penetration Chief, Space Cybersecurity Division
- Senior Director, Red Team, Space Cybersecurity

Graduates from the proposed **Ph.D. in Space Cybersecurity** will possess the highest knowledge in Space Cybersecurity with the ability to serve as top leaders in their field. Graduates will also possess the required knowledge in Space Cybersecurity to serve as a subject matter expert and form their own private company.

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

The U.S. Bureau of Labor Statistics (BLS) does not have a category yet for Space Cybersecurity positions. As a result, there are no concise government statistics for this sector of the field. However, there is a growing demand in the field. The new U.S. Space Force is expected to increase in numbers from its current manpower of 2,500 to over 20,000 within a decade. There are also over 3,000 commercial satellites in orbit with just as many that are non-operational. (Source: webform.org). There are 2,000 commercial satellites in Low Earth Orbit (LEO) that are part of communication systems and Global Positioning Systems. Commercial companies operate or play a significant role in the operation of those systems. The U.S. military also has additional satellites, but the numbers are not released officially. Plus, there are estimates that the next decade will see at least another 1,500 commercial satellites launched worldwide. (Source: bbc.co.uk) It is clear that many of the existing satellites, and those to be built, require a much more robust and highly sophisticated cybersecurity capability in order to be secure in LEO or High Earth Orbit (HEO). The leaders in this evolving and expanding field will need to have the highest levels of skill and research ability. The importance of preparing the U.S. military services for Space Cybersecurity is also a U.S. Government priority. (Source: House Committee on Armed Services, Testimony of Michelle Flournoy, Future of Defense Task Force Hearing: Theories of Victory, Oct. 29, 2019, https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=110154)

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

The U.S. Bureau of Labor Statistics (BLS) does not have a category yet for Space Cybersecurity positions. The field is new and growing. As a result, there are no concise government statistics for this sector of Cybersecurity. The proposed doctoral degree is designed to address senior leaders' needs within Space Cybersecurity over the next 25 years.

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

There are no doctoral degrees in Space Cybersecurity in Maryland or the rest of the United States. The proposed **Ph.D. in Space Cybersecurity** would be the first. As a result, there is no data on the current and projected supply of prospective graduates. However, in the broader cybersecurity field, there is virtually no unemployment. The current positions in Maryland also earn a mean salary of $120,000 per year (source: indeed.com). The number of satellites worldwide is expected to increase substantially. In the United States alone, there eight major satellite manufacturers with significant numbers of orders for new satellites over the next five years (source:

interactivesatellitetoday.com).

D. Reasonableness of Program Duplication

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

   There are no doctoral degrees in Space Cybersecurity in Maryland or the rest of the United States. The proposed **Ph.D. in Space Cybersecurity** would be the first. Capitol Technology University has a Doctor of Science (D.Sc.) in Cybersecurity and Ph.D. in Cybersecurity Leadership -- both are broader fields of study not focused solely on Space Cybersecurity. The University of Maryland College Park (UMCP) offers three doctoral degrees in much broader areas involving different aspects of space studies (i.e., Ph.D. in Aerospace Engineering, Ph.D. in Astronomy, and Ph.D. in Physics). UMCP's Ph.D. Aerospace Engineering has four core areas (Aerodynamics Propulsion, Flight Dynamics and Control, Space Systems, and Structural Mechanics and Composites) – areas that are significantly broader in scope and focus. UMCP also has a Space Physics Group devoted to space research. The University of Maryland Baltimore County (UMBC) has two doctoral degrees in much broader fields of study involving different aspects of space studies (i.e., Ph.D. in Atmospheric Physics and Ph.D. in Physics). UMBC's Ph.D. in Atmospheric Physics allows students to participate in research opportunities in astrophysics such as remote sensing, atmospheric modeling, and climate dynamics -- areas that are significantly broader in scope and focus. UMBC's Ph.D. in Physics provides research opportunities in active galaxies, galactic microquasars, gamma-ray bursts, and black holes -- areas that are significantly broader in scope and focus. Johns Hopkins University (JHU) offers a Ph.D. in Earth and Planetary Science – an even broader area of study. JHU's degree covers studies on the atmosphere, biosphere, oceans, geochemistry, geology, geophysics, and planets. However, UMCP, UMBC, and JHU do not offer a doctoral degree solely focused on Space Cybersecurity. If approved, the proposed **Ph.D. in Space Cybersecurity** would be the first such degree in the State of Maryland and the United States.

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

   The proposed **Ph.D. in Space Cybersecurity** program is strongly aligned with the University's strategic priorities and is supported by adequate resources. The proposed **Ph.D. in Space Cybersecurity** degree will strengthen and expand upon the existing technology, management, and applied engineering degree programs at the University. In addition, the **Ph.D. in Space Cybersecurity** program will be an option for all students as the field integrates well with the market needs of the University's other programs. There is a thorough discussion of the need for the program in Sections B and C of this document.

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

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

   The University does not anticipate any impact on the implementation or maintenance of high-demand programs at HBIs. There are no Ph.D. programs, or other doctoral degrees, in Space

Cybersecurity in Maryland or the rest of the United States. The proposed **Ph.D. in Space Cybersecurity** degree would be the first.

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

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

The University does not anticipate any impact on the uniqueness and institutional identities and missions of HBIs. There are no Ph.D. programs, or other doctoral degrees, in Space Cybersecurity in Maryland or the rest of the United States. The proposed **Ph.D. in Space Cybersecurity** would be the first.

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

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

The University's New Programs Group established the proposed program through a rigorous review of unmet needs. The group includes selected representation from the University's faculty, administrators, and Executive Council. Please see Section I for a detailed list of the faculty's backgrounds and qualifications.

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

Learning Objectives:

1. Students will evaluate the need for robust protection of space cybersecurity within the field of military and commercial Space Cybersecurity.
2. Students will demonstrate advanced knowledge and competencies needed for the future in Space Cybersecurity.
3. Students will analyze theories, tools, and frameworks used in Space systems.
4. Students will execute a plan to complete a significant piece of scholarly work in Space Cybersecurity.
5. Students will develop skills to implement Space Cybersecurity plans needed for advanced global protection of national assets.

Learning Outcomes:

Upon graduation:

1. Graduates will incorporate the theoretical basis and practical applications of Space Cybersecurity into their professional work.
2. Graduates will demonstrate the highest mastery of the needs of Space Cybersecurity.
3. Graduates will evaluate complex problems, synthesize divergent/alternative/contradictory perspectives and ideas fully, and develop advanced solutions to Space Cybersecurity challenges.

4. Graduates will contribute to the body of knowledge in the study of Space Cybersecurity in commercial or military applications.

3. Explain how the institution will:

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

Capitol Technology University will assess student achievement of the learning outcomes per the regulations specified by the University's regional accreditation organization: the Middle States Commission on Higher Education (MSCHE).

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

> Assessment of student learning and achievement demonstrates that the institution's students have accomplished educational goals with their program of study, degree level, the institution's mission, and appropriate expectations for institutions of higher education.
>
> (Source: https://www.msche.org/standards/, retrieved 7/22/2019)

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

> An accredited institution possesses and demonstrates the following attributes or activities:
>
> 1. [C]learly stated educational goals at the institution and degree/program levels, which are interrelated with one another, with relevant educational experiences, and with the institution's mission;
>
> 2. [O]rganized and systematic assessments, conducted by faculty and/or appropriate professionals, evaluating the extent of student achievement of institutional and degree/program goals. Institutions should:
>
> > a. define meaningful curricular goals with defensible standards for evaluating whether students are achieving those goals;
> >
> > b. articulate how they prepare students in a manner consistent with their mission for successful careers, meaningful lives, and, where appropriate, further education. They should collect and provide data on the extent to which they are meeting these goals;
> > c. support and sustain assessment of student achievement and communicate the results of this assessment to stakeholders;
>
> 3. [C]onsideration and use of assessment results for the improvement of educational effectiveness. Consistent with the institution's mission, such uses include some combination of the following:
>
> > a. assisting students in improving their learning;
> > b. improving pedagogy and curriculum;

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

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

5. [P]eriodic assessment of the effectiveness of assessment processes utilized by the institution for the improvement of educational effectiveness.

(Source: http://www.msche.org/wp-content/uploads/2018/06/RevisedStandardsFINAL.pdf)

The University will also evaluate student achievement of the learning outcomes using the Quality Assurance Agency for Higher Education (QAA) Framework for Higher Education Qualifications and its related assessment tools. The following tables provide a high-level view of the QAA Qualification Frameworks for doctoral programs:

QAA Qualifications Framework for Ph.D.

4.18 Descriptor for a higher education qualification at level 8 on the FHEQ and SCQF level 12 on the FQHEIS: doctoral degree

The descriptor provided for this level of the frameworks is for any doctoral degree which should meet the descriptor in full. This qualification descriptor should also be used as a reference point for other level 8/level 12 qualifications.

Doctoral degrees are awarded to students who have demonstrated:

- the creation and interpretation of new knowledge, through original research or other advanced scholarship, of a quality to satisfy peer review, extend the forefront of the discipline, and merit publication
- a systematic acquisition and understanding of a substantial body of knowledge which is at the forefront of an academic discipline or area of professional practice
- the general ability to conceptualise, design and implement a project for the generation of new knowledge, applications or understanding at the forefront of the discipline, and to adjust the project design in the light of unforeseen problems
- a detailed understanding of applicable techniques for research and advanced academic enquiry.

Typically, holders of the qualification will be able to:

- make informed judgements on complex issues in specialist fields, often in the absence of complete data, and be able to communicate their ideas and conclusions clearly and effectively to specialist and non-specialist audiences
- continue to undertake pure and/or applied research and development at an advanced level, contributing substantially to the development of new techniques, ideas or approaches.

And holders will have:

- the qualities and transferable skills necessary for employment requiring the exercise of personal responsibility and largely autonomous initiative in complex and unpredictable situations, in professional or equivalent environments.

QAA Qualifications Framework for Ph.D. (Continued)

4.18.1 Doctoral degrees are awarded for the creation and interpretation, construction and/or exposition of knowledge which extends the forefront of a discipline, usually through original research.
4.18.2 Holders of doctoral degrees are able to conceptualise, design and implement projects for the generation of significant new knowledge and/or understanding. Holders of doctoral degrees have the qualities needed for employment that require both the ability to make informed judgements on complex issues in specialist fields and an innovative approach to tackling and solving problems.
4.18.3 Doctoral programmes that may have a substantial taught element in addition to the research component (for example, professional doctorates), lead usually to awards which include the name of the discipline in their title (for example, EdD for Doctor of Education or DClinPsy for Doctor of Clinical Psychology). Professional doctorates aim to develop an individual's professional practice and to support them in producing a contribution to (professional) knowledge.
4.18.4 The titles PhD and DPhil are commonly used for doctoral degrees awarded on the basis of original research.
4.18.5 Achievement of outcomes consistent with the qualification descriptor for the doctoral degree normally requires study equivalent to three full-time calendar years.
4.18.6 Higher doctorates may be awarded in recognition of a substantial body of original research undertaken over the course of many years. Typically a portfolio of work that has been previously published in a peer-refereed context is submitted for assessment. Most degree awarding bodies restrict candidacy to graduates or their own academic staff of several years' standing.

(Source: UK Quality Code for Higher Education, Part A: Setting and Maintaining Academic Standards, The Frameworks for Higher Education Qualifications of UK Degree-Awarding Bodies, October 2014)

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

Program description, as it will appear in the catalog:

The **Doctor of Philosophy (Ph.D.) in Space Cybersecurity** degree is a unique program designed to meet the evolving needs of today's Space Cybersecurity in an ever-changing world of conflict. The **Ph.D. in Space Cybersecurity** program provides students with the opportunity to conduct extensive and sustained, original research at the highest level in the field of Space Cybersecurity. The **Ph.D. in Space Cybersecurity** is designed to meet the demands of the highest-skilled professionals to become leaders who will be involved in the advancement, expansion, and support of Space Cybersecurity on a national and international level. The **Ph.D. in Space Cybersecurity** is for current professionals in the field who desire to elevate their skills to the highest level and to contribute to the body of knowledge in Space Cybersecurity.

The proposed **Ph.D. in Space Cybersecurity** degree is for current professionals in the field. The degree provides a path for Space Cybersecurity personnel to explore new ground in the rapidly evolving world of commercial and governmental Space Cybersecurity. The University is in a unique position to give those students an avenue to pursue a deep proficiency in this area using an interdisciplinary methodology, cutting-edge courses, and dynamic faculty. Graduates will contribute significantly to the Space Cybersecurity field through the creation of new knowledge, ideas, and technology. The **Ph.D. in Space Cybersecurity** program is designed as a doctorate by research where students will quickly become able to engage in leadership, research, and publishing.

Description of program requirements:

Entrance Requirements

To be accepted into the **Ph.D. in Space Cybersecurity** program, students must have completed an appropriate master's degree with a cumulative GPA of no less than 3.0 on a 4.0 scale. Students must also possess a high level of experience in the field, or a closely related field, and show the academic promise of their future ability to produce original research of publishable quality (suitable for a scholarly peer-reviewed journal or publication and presentation of high stature).

Students must also provide a prospectus of at least 1000 words that details their existing expertise and preparation for success in conducting original research within Capitol Technology University's **Ph.D. in Space Cybersecurity** program. International students are required to take the TOEFL and score at least 550 on the paper-based test or 79 on the internet-based test.

Degree Requirements:

The **Ph.D. in Space Cybersecurity** program is designed for students with an appropriate master's degree and significant years of field experience. During the program, students will conduct original research in an approved area of study. Successful completion of the program culminates in the award of the **Doctor of Philosophy (Ph.D.) in Space Cybersecurity** degree.

There are two options for completion of the **Ph.D. in Space Cybersecurity** program. Under the thesis option, the student will produce, present, and defend a doctoral dissertation after receiving the required approvals from the student's Committee and the Ph.D. Review Board. Under the publication option, the student will produce, present, and defend their original doctoral research after receiving the required approvals from the student's Committee and the Ph.D. Review Board. The student must also publish three works of original research in a scholarly peer-reviewed journal(s). One of the three published works may be in a peer-reviewed conference proceeding.

Degree Requirements:

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

Doctor of Philosophy in Space Cybersecurity
Courses
Total Credits: 60

SPACE CYBERSECURITY DOCTORAL CORE: 30 CREDITS

SCS-800 Space Cybersecurity Research Background (6 Credits)
The student will focus on the study of the latest Space Cybersecurity strategies, tactics developments, and technology. The student will synthesize the growing need for upgraded Space Cybersecurity on current and future operations in the field and identify areas for improvement or failings. The focus will be to start identifying areas for research and explore the background of Space Cybersecurity. The faculty will directly support and mentor the exploration phase of the planning. Prerequisite: None.

SCS-810 Space Cybersecurity Research Methodologies (6 Credits)
Under a Chair and Committee, the student will continue evaluating and develop research methodologies and strategies suitable for understanding Space Cybersecurity and address

the data sources, information, and intelligence to test a hypothesis or research question. The student is expected to be building upon SCS-800 in refining and developing their research task and plan. Prerequisite: SCS-800.

SCS-820 Space Cybersecurity Future Demands (6 Credits)
Under a Chair and Committee, a student will research the future demands in the Space Cybersecurity field and how these influence specific research questions. Data collection and applications will be central to evaluating Space Cybersecurity's needs in the short, medium, and long term. The literature review will be more specific in focus and direction at this stage. Prerequisite: SCS-810.

SCS-830 Strategies for Space Cybersecurity (6 Credits)
The student will undertake a robust and comprehensive analysis of the strategies for the growth and evolution of the Space Cybersecurity field under the direction of their Chair and Committee. The student will produce a concise direction for research and a draft methodology. Prerequisite: SCS-820.

SCS-840 Space Cybersecurity Research Proposal (6 Credits)
The student will produce a proposal for research that is comprehensive in detail and planning (i.e., research topic, scope and aims, objectives, and timing plan). The doctoral student will then complete the research milestones according to the proposal and research plan. The student's work will need to pass the IRB and ARB at this stage. Prerequisite: SCS-830.

SPACE CYBERSECURITY DOCTORAL RESEARCH AND WRITING: 30 CREDITS

SCS-900 Space Cybersecurity Doctoral Writing I (6 Credits)
The student will compose and complete Chapters 1 and 2 within the proposal's boundaries and research plan. The student's Chair and Committee will review Chapters 1-2. The Chair and Committee must approve the chapters for the student to advance. The Dean of Doctoral Programs will review any disagreement within the committee. Prerequisite: SCS-840.

SCS-910 Space Cybersecurity Doctoral Writing II (6 Credits)
The student will compose and complete Chapter 3 (methodology chapter that is robust and identifies all implications) according to the approved proposal. After receiving the necessary approvals, the student will conduct data collection and analysis activities consistent with the research plan. Prerequisite: SCS-900.

SCS-920 Space Cybersecurity Doctoral Writing III (6 Credits)
The student will compose and complete Chapter 4. The student will provide a complete and substantive presentation of the research results in Chapter 4. The student's Chair and Committee must review and approve Chapter 4 for the student to advance. Prerequisite: SCS-910.

SCS-930 Space Cybersecurity Doctoral Writing IV (6 Credits)
The student will compose and complete Chapter 5 and submit the work to the student's Chair and Committee. The student will also finalize all required elements of their research.

eestThe student's Chair and Committee must review and approve the complete document. The student's Chair and Committee will then submit the complete document to the University Reviewers and Ph.D. Review Board for approval. The student must receive approval from the University Reviewers and Ph.D. Review Board to advance forward. Prerequisite: SCS-920.

SCS-940 Space Cybersecurity Doctoral Defense (6 Credits)
Upon approval from the University Reviewers and Ph.D. Review Board, the student will prepare and deliver an oral presentation summarizing the body of research and defend the same through *viva voce* (i.e., oral examination). The student's Chair, Committee, and Ph.D. Review Board will confer to determine if the student has provided a sufficient and necessary final oral defense of the research. Prerequisite: SCS-930.

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

   N/A. This is a graduate program.

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

   The program will be accredited regionally by Middle States Commission on Higher Education (MSCHE). The University will also evaluate student achievement of the learning outcomes using the UK Quality Assurance Agency for Higher Education (QAA) Framework for Higher Education Qualifications.

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

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

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

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

   Curriculum, course, and degree information will be available on the university website and via e-mail as well as regular mail (by request). The expectations for faculty/student interaction are available to students during virtual open house events, literature, website, etc. This information is also part of the material distributed for each course. Students receive guidance on proper behavior/interaction with their Department Chair and faculty members both in-person and online to facilitate a high-level experience. Technology competence and skills and technical equipment requirements are part of the material distributed for each course. The technical equipment

requirements are also listed on our website and provided to students in the welcome package.

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

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.**

   The **Ph.D. in Space Cybersecurity** program's advertising, recruiting, and admissions materials will clearly and accurately represent the proposed program and the services available. The content for every new program is derived from the new program request sent to the Maryland Higher Education Commission is the source of the content for every new program at the University.

H. Adequacy of Articulation:

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

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

I. Adequacy of Faculty Resources (as outlined in COMAR 13B.02.03.11):

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

   Almost all of the faculty listed below have been engaged with the University for at least several years. Dr. Ashmall, Dr. Bajracharya, Dr. Baker, Dr. Butler, and Dr. McAndrew are fulltime faculty members. All of the faculty members hold terminal degrees. The University leadership is confident in the quality of the faculty and their abilities to provide a learning environment supportive of the University goals for student success. Additional Ph.D.-qualified faculty will be added as needed.

   Instructors who will be engaged with the **Ph.D. in Space Cybersecurity** are:

Dr. Tariq Abughazaleh Adjunct	Ph.D. Technology M.Sc. Quality Engineering B.S Mechanical Engineering	SCS 800 courses

Dr. Lt. Col. Soren Ashmall, USMC (Ret.) Full time	Ph.D. Technology M.A. Broadcast Journalism MOS 0202 Intelligence Officer MOS 2602 Signals Intelligence Officer/ Electronic Warfare Officer MOS 3450 Planning, Programming, & Budget Systems Officer MOS 8055 Information Management Officer Facilities Security Officer, National Industrial Security Program (NISP)	SCS 800 and 900 courses
Dr. Chandra Bajracharya Full time	Ph.D. Electrical and Computer Engineering M.S. Applied Computing M.S. Electrical Power Engineering B.E. Electrical Engineering	SCS 800 and 900 courses
Dr. Richard Baker Full time	Ph.D. Information Systems M.S. Computer Science B.S. Mathematics	SCS 800 and 900 courses
Dr. Malcolm Beckett Adjunct	D.B.A. Quality Systems Management in Homeland Security and Defense M.S. Information Systems Management B.S. Criminal Justice CISSP PMP	SCS 800 and 900 courses
Dr. William Butler Full-time	D.Sc. Cyber Security M.S. Strategic Studies B.S. Computer Science NSTISSI No. 4011 CNSSI No. 4012 NSTISSI No. 4015 CNSSI No. 4016	SCS 800 and 900 courses
Dr. Raymond Letteer Adjunct	D.Sc. Cyber Security M.S. Network Security/Information Assurance B.A. Political Science A.A.S. Communications Technology	SCS 800 and 900 courses
Dr. Ian McAndrew Full time	Ph.D. Mechanical Engineering M.Sc. Manufacturing Engineering M.A. Education Management Post-Graduate Diploma in Education B.Sc. (Hons) Mechanical Engineering B.A. Production Engineering	SCS 900 courses
Dr. Mark Opeka Adjunct	Ph.D. Materials Engineering M.S. Materials Engineering B.S. Mechanical Engineering	SCS 800

Dr. Steven Wood Adjunct	D.Sc. Cyber Security M.S. Computing and Cyber B.S. Systems Engineering	SCS 800 and 900 courses

ADDITIONAL JUSTIFICATION FOR KEY FACULTY:
Capitol Technology University's instructors for this program are leading experts in cybersecurity, terrorism, counterterrorism, technology, and supporting fields, including:

Dr. LtCol. Soren Ashmall, USMC (Ret.)
Dr. LtCol. Ashmall is a seasoned professor at Capitol Technology University. In addition to his career in academia, Dr. LtCol. Ashmall has also worked as a Senior Director of Business Development for General Dynamics Information Technology, involving major projects in the United States and overseas. He has held other senior positions at commercial companies and U.S. government agencies. Dr. LtCol. Ashmall is an expert in terrorism, counterterrorism, intelligence, and signals intelligence. He retired as a Lieutenant Colonel from the United States Marine Corps in 2009 following over 21 years of continuous active duty military service. He served as an Intelligence Officer, Signals Intelligence Officer, and Electronic Warfare Officer during his military career. Dr. LtCol. Ashmall conducted operations worldwide in support of national and international missions. He held positions of increasing authority throughout his career, including service as a Vice Chairman, Commanding Officer, Executive Officer, Operations Officer, Officer-In-Charge, and Division Head multiple times at Headquarters, U.S. Marine Corps. He is also an expert in resources, having directed all resourcing and budgeting for Marine Corps Intelligence, regularly briefed U.S. Congressional Committees, directed all signals intelligence policy for the Marine Corps, led a large national event for the Marine Corps, and held fiscal responsibility for hundreds of millions of dollars during his military career.

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

a) Pedagogy that meets the needs of the students

The primary pedagogy for faculty at Capitol Technology University is the Active Learning model. The university believes strongly in a highly-interactive, thinking, and hands-on experience for students in each class to the maximum extent possible.

> It was two Missouri State professors, historian Charles Bonwell and psychologist James Eison, who coined the term "active learning." In their 1991 book on the subject, Active Learning: Creating Excitement in the Classroom, they offered this definition of the concept: "active learning involves students in doing things and thinking about the things they are doing."
>
> The definition, though it seems circuitous, marks a definitive pedagogical shift in college teaching and learning. Rather than think about what they are watching, hearing, or reading, students are first encouraged to be "doing" something in class, and then to apply critical thought and reflection to their own classroom work and activity. Their argument was backed up by research. Even Bligh, 20 years earlier, had pointed out that the immediate rehearsal of new information and knowledge had a significant impact on learning.

> This approach is as helpful in the sciences as it is in the arts or humanities: whether it's organic chemistry, creative writing, or behavioral economics, concepts are all best understood through repeated practice and open, social exploration. The central tenet of active learning is that practice matters, and that classroom time is better spent giving students opportunities to work with concepts over and over, in a variety of ways and with opportunities.
>
> The central tenet of active learning — that practice and interaction matters— can be applied across disciplines for immediate feedback, so that knowledge can take hold in their own minds.
>
> (Source: Preville, P. Active Learning: The Perfect Pedagogy for the Digital Classroom: An Essential Guide for the Modern Professor)

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

b) The Learning Management System

The University's Department of Online Learning and Information Technology Division supports the online program needs of faculty and students. The Department of Online Learning and IT Help Desk provide 24-hour support to the faculty. Canvas is the University's online Learning Management System. When a new faculty member is assigned to teach an online course, the Department of Online Learning provides formal training for the instructor. New faculty are assigned an experienced faculty mentor to ensure a smooth transition to the online environment as well as to ensure compliance with the institution's online teaching pedagogy. The University believes this provides the highest-level learning experience for the faculty member and, in turn, students attending online classes.

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

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

> A model used in the online delivery of teaching and learning to increase learner motivation is Keller's ARCS motivational model. This model has been considered an important element in online education because of its implications on increased learner motivation and learning outcomes. The Keller's model consists of motivating students by maintaining and eliciting attention (A), such as virtual clinical simulations; making the content and format relevant (R), by modeling enthusiasm or relating content to future use; facilitating student confidence (C), by providing "just the right challenge"; and promoting learner satisfaction (S), by providing reinforcement and praise when appropriate. Examples of Keller's model include increasing motivation including the arousal of curiosity of students, making the connection between learning objectives and future learning goals, autonomous thinking and learning, and fostering student satisfaction.

Keller's ARCS model has been researched by various educational online programs to analyze student motivation and learning outcomes. Keller's model serves as an example and guide for instructors to motivate and increase online engagement with their students as wells as research purposes.

A qualitative study by Chan Lin investigated online student learning and motivation. Discussion boards, student projects, and reflection data were collected and analyzed from a 12-week web-based course. Respondents indicated the importance of online feedback from the instructor and peer modeling of course tasks to visualize learning progress. The study revealed using Keller's ARCS strategies fosters greater student online engagement by fostering self-efficacy and a sense of accomplishment.

In a mixed-method study, assessing the use of Keller's ARCS on instructional design, the use of educational scaffolding fostered positive levels of student motivation. Relevancy, attention, confidence, and satisfaction were all common factors associated with student success in the course and course completion.

(Source: Pinchevsky-Font T, Dunbar S. Best Practices for Online Teaching and Learning in Health Care Related Programs. The Internet Journal of Allied Health Sciences and Practice. January 2015. Volume 13 Number 1.)

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

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

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

Library Services: The Puente Library offers extensive services and a wide collection for Capitol Technology University students to be academically successful. Library resources are available digitally. The library also provides a mailing service for materials borrowed through the Maryland system.

The library is currently supporting the following degrees at the undergraduate level: B.S. in Astronautical Engineering, B.S. in Aviation Professional Pilot, B.S. in Computer Engineering, B.S. in Computer Engineering Technology, B.S. in Computer Science, B.S. in Construction Information Technology and Cybersecurity, B.S. in Construction Management and Critical Infrastructure, B.S. in Construction Safety, B.S. in Counterterrorism, B.S. in Cyber Analytics, B.S. in Cybersecurity, B.S. in Data Science, B.S. in Electrical Engineering, B.S. in Electrical Engineering Technology, B.S. in Engineering Technology, B.S. in Facilities Management and Critical Infrastructure, B.S. in Information Technology, B.S in Management of Cyber and

Information Technology, B.S. in Mechatronics Engineering, B.S. in Mechatronics and Robotics Engineering Technology, B.S. in Mobile Computing, B.S. in Professional Trades Administration, B.S. in Software Engineering, and B.S. in Technology and Business Management, B.S in Unmanned and Autonomous Systems, and B.S. in Web Development.

The library is currently supporting the following degrees at the graduate level: Master of Business Administration (M.B.A.), Master of Science (M.S.) in Astronautical Engineering, M.S. in Aviation, M.S. in Aviation Cybersecurity, M.S. in Computer Science, M.S. in Construction Cybersecurity, M.S. in Construction Safety, M.S. in Critical Infrastructure, M.S. in Cyber Analytics, M.S. in Cybersecurity, M.S. in Information Systems Management, M.S. in Engineering Technology, M.S. in Internet Engineering, M.S. in Unmanned and Autonomous Systems Policy and Risk Management, Technical Master of Business Administration (T.M.B.A.) in Business Analytics and Data Science, and T.M.B.A. in Cybersecurity, Doctor of Science (D.Sc.) in Cybersecurity, Doctor of Philosophy (Ph.D.) in Artificial Intelligence, Ph.D. in Aviation, Ph.D. in Business Analytics and Data Sciences, Ph.D. in Construction Science, Ph.D. in Counterterrorism, Ph.D. in Critical Infrastructure, Ph.D. in Cybersecurity Leadership, Ph.D. in Emergency and Protective Services, Ph.D. in Human Factors, Ph.D. in Manufacturing, Ph.D. in Occupational Health and Safety, Ph.D. in Operational Technology, Ph.D. in Product Management, Ph.D. in Quantum Computing, Ph.D. in Technology, Ph.D. in Technology/M.S. Research Methods Combination Program, and Ph.D. in Unmanned Systems Applications.

Therefore, the library is fully prepared to support a **Ph.D. in Space Cybersecurity.**

Services provided to online students include:

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

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

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

research and academic libraries provide the Puente Library with quick access to these materials as well.

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

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

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

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

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

a. An institutional electronic mailing system

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

b. A Learning Management System that provides the necessary technological support for distance education

Capitol Technology University provides a robust Learning Management Systems (LMS) through the use of the Canvas LMS by Instructure (www.canvaslms.com). The University pairs Canvas with Zoom (zoom.us) to provide a platform for every student and faculty member to meet face-to-face in a synchronous "live" mode of communication. The University requires Canvas for every class; as a result, every course has a classroom on Canvas and Zoom. All syllabi, grades, and assignments must be entered into Canvas on a timely basis throughout the semester.

Canvas provides the world's most robust LMS. It is a 21st Century LMS; Canvas is a native cloud, Amazon Web Service hosted system. The system is adaptable, reliable, and customizable. Canvas is easy to use for students and faculty. The system is fully mobile and

has proven to be timesaving when compared to other systems. The following list provides the features of the system:

Time and Effort Savings

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

- SPEEDGRADER
  Grade assignments in half the time.

  Student Engagement

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

- PROFILE
  Introduce yourself to classmates with a Canvas profile.

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

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

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

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

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

- WEB CONFERENCING
  Engage in synchronous online communication.

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

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

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

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

  Lossless Learning

- CANVAS POLLS
  Gauge comprehension and incorporate formative assessment without the need for "clicker" devices.

- MAGICMARKER

Track in real-time how students are performing and demonstrating their learning.

- QUIZ STATS
  Analyze and improve individual assessments and quiz questions.
- LEARNING MASTERY FOR STUDENTS
  Empower students to take control of their learning.

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

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

L. Adequacy of Financial Resources with Documentation (as outlined in COMAR 13B.02.03.14):

1. **Table 1: Resources.**

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)	$235,116	$361,368	$546,282	$667,998	$906,696
a. Number of F/T Students	0	0	0	0	0
b. Annual tuition/Fee rate	$0	$0	$0	$0	$0
c. Total F/T Revenue (a x b)	$0	$0	$0	$0	$0
d. Number of P/T Students	14	21	31	37	49
e. Credit Hour Rate	$933	$956	$979	$1,003	$1,028
f. Annual Credit Hour	18	18	18	18	18
g. Total P/T Revenue (d x e x f)	$235,116	$361,368	$546,282	$667,998	$906,696
3. Grants, Contracts and Other External Sources	0	0	0	0	0
4. Other Sources	0	0	0	0	0
TOTAL (Add 1 – 4)	$235,116	$361,368	$546,282	$667,998	$906,696

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

1. **Reallocated Funds**
   The University will not need to reallocate funds for the program.
2. **Tuition and Fee Revenue**
   Tuition is calculated to include an annual 2.5% tuition increase. A 20% attrition rate has been calculated.
3. **Grants and Contracts**
   There are currently no grants or contracts.
4. **Other Sources**
   There are currently no other sources of funds.
5. **Total Year**
   No additional explanation or comments needed.

2. **Table 2: Program Expenditures.**

TABLE 2: EXPENDITURES

Expenditure Category	Year 1	Year 2	Year 3	Year 4	Year 5
1. Faculty (b + c below)	$113,468	$155,071	$238,421	$325,843	$417,486
a. #FTE	1.5	2	3	4	5
b. Total Salary	$94,557	$129,226	$198,684	$271,536	$347,905
c. Total Benefits (20% of salaries)	$18,911	$25,845	$39,737	$54,307	$69,581
2. Admin Staff (b + c below)	$5,942	$6,091	$6,244	$6,400	$6,559
a. #FTE	.08	.08	.08	.08	.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 below)	$59,885	$92,076	$125,837	$161,230	$198,313
a. #FTE	1.00	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	$980	$1,575	$2,480	$3,145	$4,140
5. Library	$0	$0	$0	$0	$0
6. New or Renovated Space	$0	$0	$0	$0	$0
7.Other Expenses	$6,832	$15,708	$27,125	$39,331	$56,105
TOTAL (ADD 1-7)	$190,107	$270,521	$400,107	$535,949	$682,603

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

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

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

c. **Support Staff**
Capitol Technology University will add additional support staff to facilitate the program.

d. **Equipment**
Software for courses is available free to students or is freeware. Additional licenses for the LMS will be purchased by the University at the rate of $70 per student in Year 1. The rate is estimated to increase by $5 per year.

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

f. **New or Renovated Space**
No new or renovated space is required.

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

h. **Total Year**
No additional explanation or comments needed.

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

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

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

Academic Year Assessment Events:

Fall Semester:

- At the August Faculty Retreat, the faculty reviews any outstanding student learning challenges that have not been adequately addressed. The issues are brought to the Academic Deans for review and development of implementation plans.
- Faculty submit performance plans consistent with the mission and goals of the University and department. The documents are reviewed and approved by the Academic Deans.
- Department Chairs and Academic Deans review the Graduating Student Survey data.
- Department Chairs and Academic Deans review student internship evaluations.
- Department Chairs and Academic Deans review grade distribution reports from the spring and summer semesters.
- Department Chairs and Academic Deans review student course evaluations from the Summer Semester.
- Departments conduct Industrial Advisory Board meetings to review academic curriculum recommendations. The Advisory Board meets to begin curriculum review or address special

issues that may arise related to the curriculum. Based on an analysis and evaluation of the results, the Academic Deans, faculty, and the advisory boards will develop the most effective strategy to move the changes forward.

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

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

Spring Semester:

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

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

The Faculty Senate meets monthly from August through April. The Faculty Senate addresses issues that impact student outcomes as those issues emerge. The leadership of the Faculty Senate then provides a report on the matter to the Academic Deans. The report may include a recommendation or a request to move forward with a committee to examine the issue further. In most cases, the changes only require the Academic Deans to inform the Vice President of Academic Affairs and University President and provide a report that includes a justification and the impact of changes as well as a strategic plan. Significant changes typically require the approval of the Executive Council.

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

satisfaction, and cost-effectiveness.

Student Learning Outcomes:

Student learning outcomes for the proposed **Ph.D. in Space Cybersecurity** will be measured using the instruments identified in Section G and Section M as well as the assessment measures dictated by the accreditation requirements of the University's regional accreditor [i.e., Middle States Commission in Higher Education (MSCHE)]. This program is designed to meet the requirements of MSCHE. The University will also evaluate student achievement of the learning outcomes using the UK Quality Assurance Agency for Higher Education (QAA) Framework for Higher Education Qualifications and its related assessment tools. The University is in good standing with all its accrediting bodies.

Student Retention:

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

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

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

Student and Faculty Satisfaction:

Evaluations and assessment of Student and Faculty satisfaction occur every semester. Faculty members are evaluated every semester by students enrolled in their courses. Students are required to complete a course evaluation online within a specified time frame at the end of the semester for every enrolled course, or they are locked out of Canvas (the University's Learning Management System) until they complete each survey. Every faculty member is also required to review each of their courses after each semester; the goal is to ensure up-to-date content, effective and efficient methods of delivery, and appropriate outcomes.

The Department Chairs and Academic Deans review the student evaluations for every course offered at the University. The Department Chairs and Academic Deans also review faculty satisfaction every semester. If changes are needed at the course level, the changes are developed and implemented by the faculty upon approval of the Department Chairs and Academic Deans. If changes are required at the faculty level, the Department Chairs will make the changes. At the end of the following semester, appropriate stakeholders analyze the results of a follow-on evaluation for the effectiveness of the changes. This cycle is an ongoing process.

Cost Effectiveness:

Based on the year-long inputs, evaluations, and reviews described in Section M.1, the Department Chairs and Academic Deans prepare the proposed academic budget for each program for the upcoming year. Budget increases are tied to increasing student learning and performance as well as critical strategic initiatives.

The Interim Vice President of Finance and Administration also monitors each academic program throughout every semester and term for its cost-effectiveness. Additionally, the revenue and costs of every University program are reviewed annually by the Executive Council and Board of Trustees before approving the next year's budget.

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

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

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

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

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

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

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

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

   Capitol Technology University is fully eligible to provide distance education. The University has a long history of providing high-quality distance education. The University is accredited regionally by the Middle States Commission in Higher Education (MSCHE) and through four specialized accrediting organizations: International Accreditation Council of Business Education (IACBE), Accreditation Board for Engineering and Technology (ABET), NSA, and DHS. All five accrediting organizations have reviewed the University's distance education program as part of their accreditation process. Capitol Technology University is fully accredited by MSCHE, IACBE, ABET, NSA, and DHS. The University is in good standing with all its accrediting bodies.

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

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

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

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

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

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

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

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

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

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

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

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

   Online programs/courses meet the same accreditation standards, goals, objectives, and outcomes as traditional classroom delivery. The University selects the learning platforms

to ensure the high standards of the technical elements of each course. The Academic Deans monitor any course conversion from in-class to online to ensure the online course is academically equivalent to the traditionally offered course and that the technology is appropriate to support the expected rigor and breadth of the course.

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

   The Department of Doctoral Programs, where this degree will be sponsored, is staffed by a qualified University Academic Dean, Dr. Ian McAndrew, and supported by a Director of Doctoral Programs. Other appropriately credentialed faculty with multi-disciplinary level skills will be part of the delivery process.

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

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

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

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

   Laboratories (on ground and virtual) are available for use by all students. Faculty and highly-qualified tutors staff the laboratories and provide academic support.

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

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

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

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

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

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

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

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