Office Use Only: PP#

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

Institution Submitting Proposal	Capitol Technology University

Each action below requires a separate proposal and cover sheet.

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

Payment Submitted:	Payment Type:	Payment Amount:	Date Submitted:
◉ Yes ○ No	○ R*STARS # 97219 ◉ Check # 97219	$850	10-1-24

Department Proposing Program	Graduate School	
Degree Level and Degree Type	Master of Science	
Title of Proposed Program	Joint M.S. in Cyber Intelligence and Security	
Total Number of Credits	48	
Suggested Codes	HEGIS: 799.10	CIP: 29.0270
Program Modality	○ On-campus ◉ Distance Education (fully online) ○ Both	
Program Resources	◉ Using Existing Resources ○ Requiring New Resources	
Projected Implementation Date (must be 60 days from proposal submisison as per COMAR 13B.02.03.03)	○ Fall ◉ Spring ○ Summer	Year: 2025
Provide Link to Most Recent Academic Catalog	URL: https://catalog.captechu.edu	
Preferred Contact for this Proposal	Name: Dr. William Butler	
	Title: VP Cyber Science Outreach and Partnerships	
	Phone: (240) 965-2458	
	Email: whbutler@captechu.edu	
President/Chief Executive	Type Name: Bradford L. Sims	
	Signature: B L. S	Date: 10-15-2024
	Date of Approval/Endorsement by Governing Board: Oct. 15, 2024	

Revised 1/2021

CAPITOL
Technology University

September 16, 2024

Dr. Sai ay Rai
Secretary of Maryland Higher Education
Maryland Higher Education Commission
6 N. Liberty Street
Baltimore, MD 21201

Dear Dr. Rai,

Capitol Technology University is requesting approval to offer a joint **M.S. Cyber Intelligence and Security with IWP, the Institute of World Politics.** The degree curriculum will be taught using the existing faculty at our university, at the Institute of World Politics 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 **M.S. Cyber Intelligence and Security** is consistent with this mission.

The requirement for experts in Artificial Intelligence at the highest level is experiencing significant growth. This program is in response to that need. The **M.S. Cyber Intelligence and Security** degree is primarily for experienced Cyber Intelligence personnel who desire to advance in their careers by earning a Masters' degree.

To 1·espond to needs of the Cyber Intelligence and Security field, we respectfully submit for approval a M.S. in Cyber Intelligence and Security. Please find the required, letter confirming the adequacy of the university's library to senie the needs of the students in this degree.

Respectfully,

Bradford L. Sims, PhD
President

CAPITOL
Technology University

September 16, 2024

Dr. Sanjay Rai
Secretary of Maryland Higher Education
Maryland Higher Education Commission
6 N. Liberty Street
Baltimore, MD 21201

Dear Dr. Rai,

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

Respectfully,

Bradford **L.** Sims, PhD
President

PROPOSAL FOR:

_X_NEW INSTRUCTIONAL PROGRAM

SUBSTANTIAL EXPANSION/MAJOR MODIFICATION

_X_ COOPERATIVE DEGREE PROGRAM

_X_WITHIN EXISTING RESOURCES or_REQUIRING NEW RESOURCES

CAPITOL Technology University

Institution Submitting Proposal

Spring 2025
Projected Implementation Date

Master of Science (MS)
Award to be Offered

Joint Master of Science in Cyber Intelligence and Security

Title of Proposed Program

799.101

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

29.0207

Suggested C.I.P. Code

Graduate School
Department of Proposed Program

Dr. John LaNear
Name of Department Head

Dr. John LaNear	**jalanear@captechu.edu**	**240.965.2461**
Director Graduate Studies	Contact E-Mail Address	Contact Phone Number

9-24-24
Signature and Date

President/Chief Executive Approval

SEPT. 24, 2024
Date /

Date Endorsed/Approved by Governing Board

Proposed Joint Master of Science in Cyber Intelligence and Security
Department of Graduate 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.**

   Joint *Master of Science in Cyber Intelligence and Security Program Description*:

   The Joint **Master of Science (MS) in Cyber Intelligence and Security** degree is a unique program that is in demand by local, national, and international organizations. It is designed to meet the long-standing needs of combining intelligence and national security with the technical skills for cybersecurity and understanding cyberspace. The proposed Joint **Capitol Technology University will jointly offer MS in Cyber Intelligence and Security** (Capitol) and the Institute of World Politics (IWP). The degree is designed for current professionals in cyber intelligence and security. Capitol is uniquely positioned 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 cybersecurity field.

   The **MS in Cyber Intelligence and Security** program is designed as a master's qualification but in a subject-specific to their work. Cyber security is becoming more technical and managing this requires higher skills in a larger percentage of the workforce. Capitol has significant experience in cyber security subjects. Many faculty are seasoned professionals in the field as well as academicians. Meanwhile, IWP provides extensive expertise in the realm of intelligence and national security. Their distinguished faculty members are not just academics; they are scholar-practitioners with a wealth of experience in the subjects they teach. With backgrounds as ambassadors, senior intelligence officials, military officers, presidential advisers, and senior congressional staff members, IWP's faculty brings a unique blend of academic credentials and high-level practical knowledge.

   Thus, Capitol Technology University's partnership with The Institute of World Politics will provide a joint degree that gives a competitive advantage to students and secures influential positions in Cyber Intelligence and Security where a convergence of strategy and technology is essential. This degree is also clearly aligned with both schools' missions. The mission of Capitol Technology University is to educate individuals for professional opportunities in engineering, computer and information sciences, and business. We provide relevant learning experiences that lead to success in the evolving global community The Institute of World Politics is a graduate school of national security, intelligence, and international affairs, dedicated to developing leaders with a sound understanding of international realities and the ethical conduct of statecraft, based on knowledge and appreciation of the founding principles of the American political economy and the Western moral tradition.

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 450 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.*

5. This program also supports the Institute of World Politics' strategic goals, including increasing enrollment, increasing IWP's visibility, and enhancing IWP's curriculum. Specific references in the Strategic Plan related to this degree include building out the Cyber Intelligence Initiative by establishing new MOU partnerships (under Increasing Enrollment) and prioritizing the near-term addition of new courses focusing on cyber (under Enhancing Curriculum).

The proposed Joint **MS in Cyber Intelligence and Security** program supports all of Capitol's four strategic goals. The proposed degree builds upon the existing areas of degrees at the graduate level: including the Master of Business Administration (M.B.A.), 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 Uncrewed 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.

Capitol's programs have prepared professionals for the rapid advances in STEM and aviation, intense global competition, and increasingly sophisticated technological environments for decades. The Joint **MS in Cyber Intelligence and Security** follows that tradition and links with the Cyber Intelligence and Security sectors both locally and nationally.

The proposed Joint **MS in Cyber Intelligence and Security** fully supports the Capitol's Vision 2025 and Strategic Plan 2017-2025. Funding to support this degree is already available within the existing budget.

Capitol has active partnerships in the private and public areas (e.g., NASA, Parsons Corporation, Libidos, Patton Electronics, Lockheed Martin, Northrup Grumman, Cyber Security Forum Initiative (CSFI), Internal Revenue Service (IRS), and the NSA National Cryptologic School). The **MS in Cyber Intelligence and Security** degree will provide new partnership opportunities. The increase in alliances and the placement of our graduates in our partner institutions will serve to expand the University's enrollment and reputation.

Meanwhile, this program supports The Institute of World Politics' strategic goals, including increasing enrollment, increasing IWP's visibility, and enhancing IWP's curriculum. Specific references in the Strategic Plan related to this degree include building out the Cyber Intelligence Initiative by establishing new MOU partnerships (under Increasing Enrollment) and prioritizing the near-term addition of new courses focusing on cyber (under Enhancing Curriculum).

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. The institution has no substantial impact due to the advanced budgeting of these funds. If approved, the program will be self-sustaining going forward. The case is the same for The Institute of World Politics. Funding to support the MS in Cyber Intelligence and Security is already available within the existing budget.

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 integral to Capitol 'FY 2017-2025 Strategic Plan'. The institutional and departmental budgets for FY 2024-2025 and the forecasted budgets going forward include funding for the new degree's administrative, financial, and technical support. The case is the same for The Institute of World Politics. The institutional and departmental budgets for FY 2023-2024 and the forecasted budgets going forward include funding for the new degree's administrative, financial, and technical support.

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

      Capitol Technology University and The Institute for World Politics are fully committed to continuing the proposed Joint **MS in Cyber Intelligence and Security** degree program for a sufficient period to allow enrolled students to complete the program. The attached Memorandum of Agreement offers assurance of both institutions' commitment.

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.**

      Cyber Intelligence and Security is the subject of maximizing your resources by science and technology. Americans are the leading experts in Cyber Intelligence and Security. However, that position is being challenged by India, Russia and China. To be the best Intelligence Analyst, more technical knowledge is needed and this MS is focused for those where a convergence of strategy and technology is essential.

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 Joint **MS in Cyber Intelligence and Security** 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 Joint **MS in Cyber Intelligence and Security** 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 **Joint MS in Cyber Intelligence and Security** program will add to the base of minority participation in the Cyber Intelligence and Security career field.

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

The 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 based on 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:** A broad intellectual grounding in technical and general subjects is required to successfully embrace future technical and managerial opportunities.
- **Professionalism:** Commitment to life-long learning, ethical practice, and participation in professions and communities.

The proposed **Joint MS in Cyber Intelligence and Security** 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.

With its academic rigor, the Joint MS in Cyber Intelligence and Security program will produce highly qualified Cyber Intelligence and Security 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 Accreditation Board for Engineering and Technology (ABET), National Security Agency (NSA), and Department of Homeland Security (DHS). The Joint **MS in Cyber Intelligence and Security** 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 Joint **MS in Cyber Intelligence and Security** degree will be offered online while allowing for real time communication 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 of attending 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 and 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 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 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, alums, 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 compliance with its accreditation and regulations of 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 members. The approach is intentionally designed to increase engagement, improve outcomes, and improve retention and graduation rates. The University believes 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 Cyber Intelligence and Security 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 Norway at the beginning of the 2019 Fall Semester. We partnered with IWP for the proposed **Joint MS in Cyber Intelligence and Security** to provide real-world projects for students with integrative learning opportunities in the Cyber Intelligence and Security field.

The University also supports prior learning assessment. A portfolio analysis is available. The University accepts professional certifications for credit for specific courses. The University also allows students to take a validation exam for credit for required courses up to the current state limits. These are all on an individual basis and approval is needed from the Dean of Graduate Programs. Credit can be given for published research specific to the degree.

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 Joint **MS in Cyber Intelligence and Security** 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:

- Cybersecurity Specialists
- Directors of Cyber
- Researchers
- Scientists
- Cyber planners

- Systems architects
- Designers
- Cyber Intelligence Analysts
- Open-source Researchers
- Cyber Security Threat Analysts
- Information Systems Security Officers
- Cyber Security Engineers
- Chief Information Security Officers (CISOs)

In addition to just seeking a promotion in one's current position, there are hundreds of opportunities/positions in other verticals. For example:

- Cyber Claims Attorney
- HIPAA Administrator
- Cyber Warfare Technician (military)
- Security & Compliance Consultant
- Process & Quality Manager
- Risk Manager
- Financial & Forensics Manager

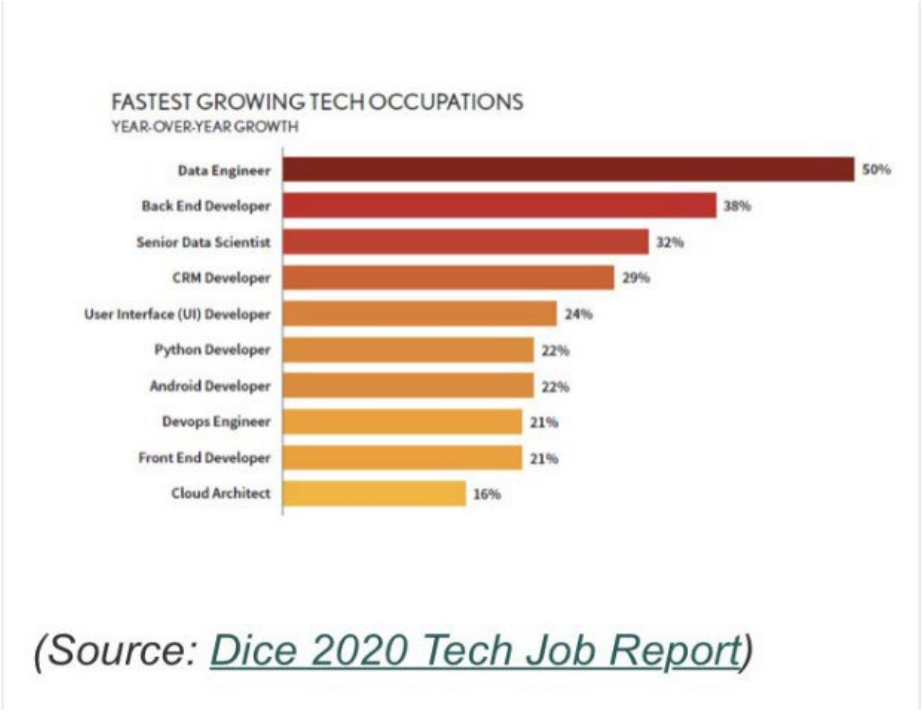
2. Present data and analysis projecting market demand and the availability of openings in a job market to be served by the new program.

Maryland is one of the key employers of cyber analysts in this area. Cyber analysts forms the backbone of defense and many agencies plus all the critical infrastructure sectors.

Security engineers who work in California make an average of $99,024 annually. US security engineers earn $104,425, on average, each year. The District of Columbia and Maryland are the next highest paying states for salary. Security engineers in Arizona must get paid well though — their annual median salary is $83,914. 43% of employed software security engineers make more annual than the national average; only 8% less. Here is a list of top city's salaries:

City	Avg. Salary/Year
Washington, DC	$142,059
San Fransisco	$133,131
San Diego	$107,478
Denver	$106,138
Chicago	$98,264
Los Angeles	$86,287
New York	$78,611

Source: DICE 2020 Tech Job Report



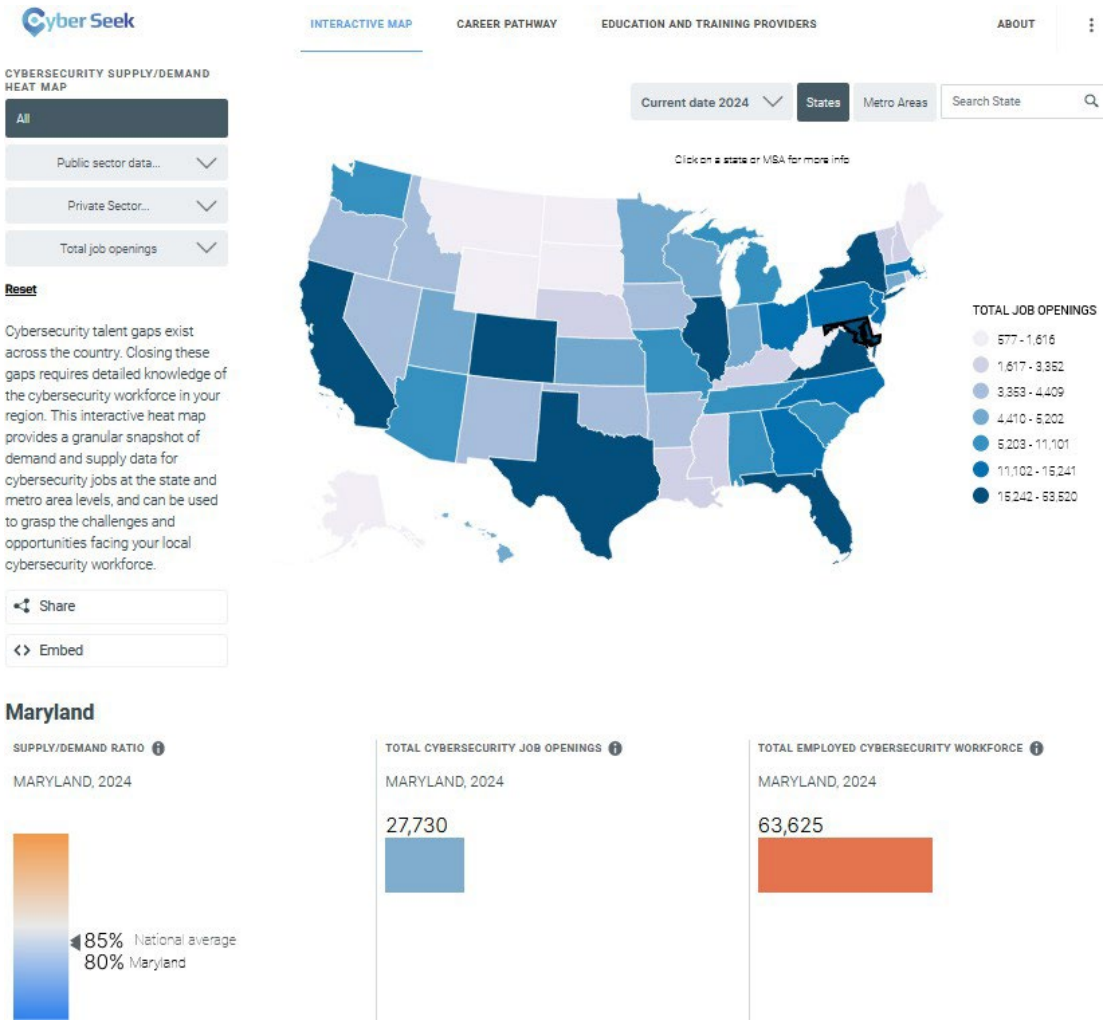
(Source: Dice 2020 Tech Job Report)

There is a shortage of specialists with intelligence skills regionally, nationally, and globally. As seen the demand outstrips supply. Long term the shortfall is going to be significant unless the problem is addressed now.

https://www.indeed.com/career-advice/careers/what-does-an-intelligence-analyst-do

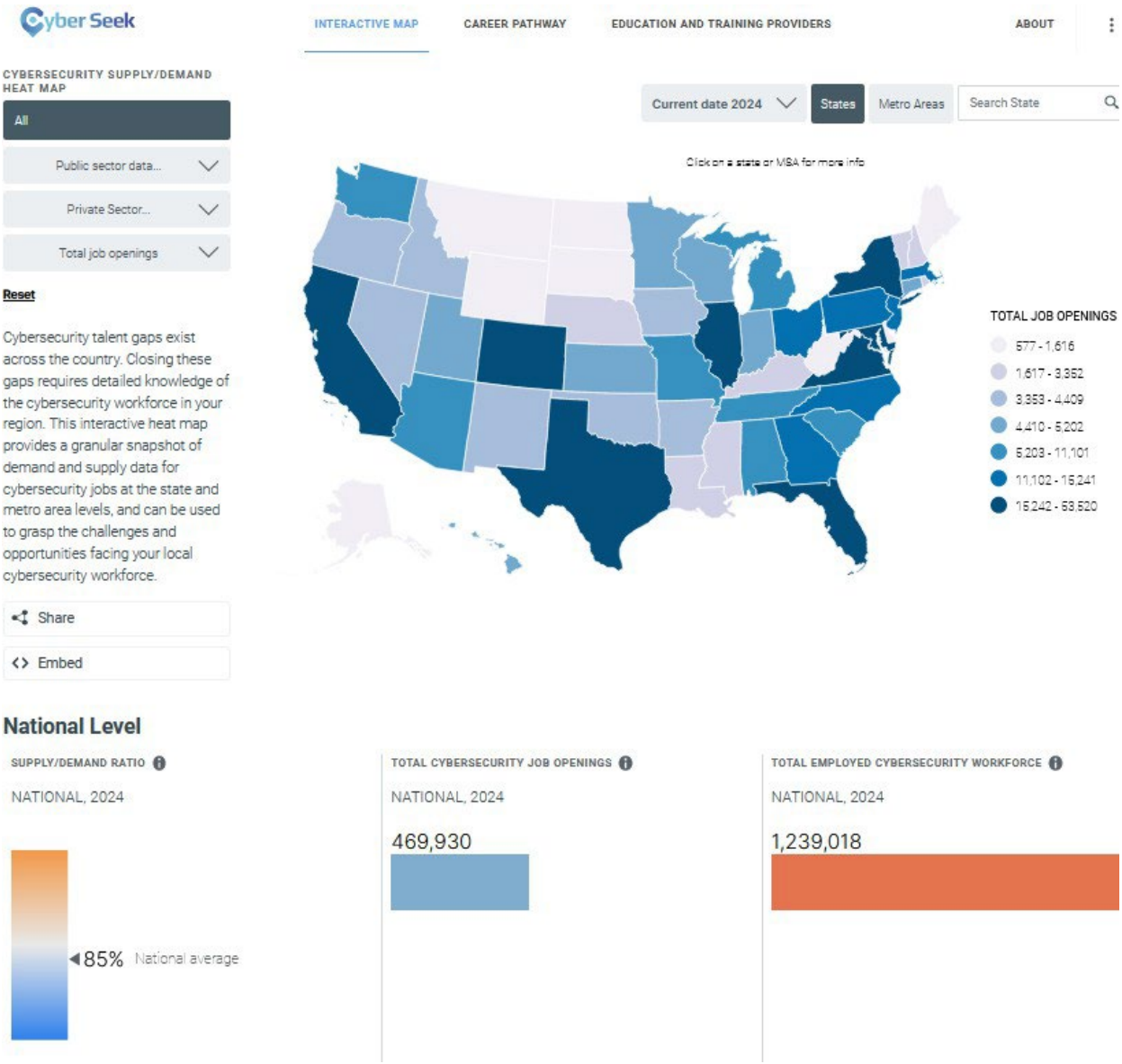
3. **Discuss and provide evidence of market surveys that clearly provide quantifiable and reliable data on the educational and training needs and the anticipated number of vacancies expected over the next 5 years.**

There are many jobs, but they are professional and high-paying compared to many others. Cyber Specialists need a Master's degree as a minimum to attain high-level positions, and this degree offers a balance in technology and strategy to give it that added competitive edge.



Source: www.cyberseek.com)

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



(Source: https://www.cyberseek.org/heatmap.html)

Cyber Specialists are among the most in demand outside the military. Maryland is a leader directly and indirectly in Cyber Intelligence and Security, and this degree will serve those in need of enhancing their studies and careers.

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 exist two Master of the Arts programs offered in the state of Maryland of similar name, which focus on intelligence analysis and diplomacy. These programs are Morgan State University's 33-credit Master's of the Arts (MA) in International Studies with a concentration in International Politics and Foreign Policy (CIP 45.0901). The second is Johns Hopkins University 36-credit Masters of the Arts (MA) in Intelligence Analysis (CIP 29.0201). The **Joint Master of Science (MS) in Cyber Intelligence and Security** program combines core cybersecurity coursework from Capitol Technology University's MS Cybersecurity program with strategic studies and security coursework from the Institute of World Politics (IWP). This blend of cybersecurity and strategic studies prepares graduates for roles that intersect cyber defense and strategic intelligence, tailored for a world where cyber and geopolitical threats are increasingly intertwined.

The proposed **Joint MS in Cyber Intelligence and Security** at Capitol Technology University is a truly innovative program. By integrating core cybersecurity coursework with strategic studies and security insights from the Institute of World Politics (IWP), it offers a comprehensive, interdisciplinary approach that few other programs can provide. This combination equips graduates with both the technical expertise and strategic acumen required to tackle complex cyber threats on a national and international level.

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

The proposed Joint **MS in Cyber Intelligence and Security** program strongly aligns with the University's strategic priorities and is supported by adequate resources. This degree will strengthen and expand upon the University's existing technology, management, and cybersecurity degree programs. In addition, this degree will be an option for all students as the field integrates well with the market needs of the University's other programs. This document thoroughly discusses the need for the program in Sections B and C.

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 implementing or maintaining high-demand programs at HBIs. While there are no Masters of Science degree programs in Cyber Intelligence and Security in Maryland there exists a Master of the Arts program of similar name: Morgan State University's 33-credit Master's in International Studies with a concentration in International Politics and Foreign Policy (CIP 45.0901). The proposed jointly offered **MS in Cyber Intelligence and Security** would be the first degree of its kind focused on senior leaders and top experts in Cyber Intelligence and Security in Maryland and the United States to include allied nations.

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 is only one program similar to the proposed Joint **MS in Cyber Intelligence and Security** in Maryland. The proposed degree would be the first to be offered jointly.

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.

Capitol Technology University's New Programs Group partnered with The Institute of World Politics leadership to establish the proposed program through a rigorous review of unmet needs. The group includes selected representations from the University's faculty, administrators, and Executive Council. Please see Section I for a detailed list of the faculty's backgrounds and qualifications. Capitol Technology University is a primary STEM teaching university for Undergraduates and Graduates; this degree adds a specific focus to our core programs.

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

Learning Objectives:

1. Students investigate and learn basic terms, concepts, history, theories, and geography related to the U.S. foreign policy process, international affairs, and the current world order.
2. Students will learn to integrate various tools of statecraft into a coherent whole.
3. Students will obtain an understanding of the major national security challenges facing the United States.
4. Students will gain knowledge and appreciation of the Western moral tradition and its applicability to national security and foreign policy.
5. Students will gain knowledge of basic terms, concepts, history, theories, and geography related to cyber statecraft.
6. Students will gain an understanding of the increasing importance of the cyber domain to U.S. national security strategy and an appreciation for the challenges of bringing cyber operation theories into practice.

Learning Outcomes:

Upon graduation, students will be able to:

1. Dmonstrate knowledge of essential terms, concepts, history, theories, and geography related to the U.S. foreign policy process, international affairs, and the current world order.
2. Integrate various tools of statecraft into a coherent whole.
3. Understand the major national security challenges facing the United States.
4. Appreciate Western moral tradition and its applicability to national security and foreign policy.
5. Apply knowledge of basic terms, concepts, history, theories, and geography related to cyber statecraft.

6. Evaluate the increasing importance of the cyber domain to U.S. national security strategy and an appreciation for the challenges of bringing cyber operation theories into practice.

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). Capitol Technology University has a rigorous assessment schedule that adheres to both MSCHE and ABET guidelines. The Assistant Vice President of Assessment, Learning, and Educational Effectiveness (AVPLEE) is responsible for developing and implementing a rigorous and sustainable assessment process. Therefore, all assessment activities are supported and facilitated by the AVPLEE. Thus, the AVPLEE ensures that assessment activities are occurring according to schedule and that findings are utilized for continuous improvement to student learning and the program. Every five years the Cybersecurity program develops an assessment plan that identifies the program outcomes and courses that will be assessed.

Components of the five-year assessment cycle

- Completion of a curriculum map for each program
- Schedule of the program objectives/outcomes to be assessed and reassessed at least once during the cycle
- Identification of the activity (i.e., data collection or analysis) that will occur each semester
- At the end of every academic year, completion of an assessment report that summarizes findings which will be submitted to the Assistant Vice President of Assessment, Learning & Educational Effectiveness
- Assessment of the various elements of the assessment process at the end of the five-year cycle
- Completion of a review of the program

The end of the five-year assessment cycle provides data that informs the review of the program and incorporates requirements of the ABET self-study process and internal requirements.

Educational Effectiveness Assessment at IWP

The Institute of World Politics (IWP) conducts educational effectiveness assessments to ensure student achievement of its Institutional Learning Outcomes (ILOs), which are as follows:

1. **US National Security, Intelligence, & Foreign Policy:** Students will be able to analyze the sources and development of current major national security, intelligence, and foreign policy challenges facing the United States and its interests globally.

2. **Specialized Knowledge:** Students will be able to demonstrate detailed knowledge in one or more specific areas of study.

3. **Integrated Statecraft:** Students will be able to develop a deeper understanding of all the instruments of statecraft as well as how to use and integrate them strategically and ethically.

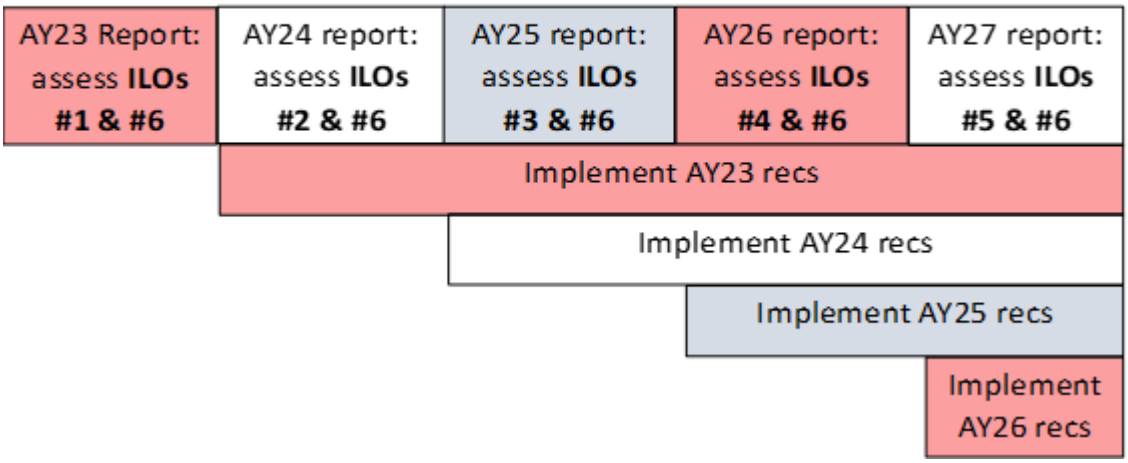
4. **Western Moral Tradition & American Founding:** Students will be able to appreciate the nature of the Western Moral Tradition and the founding principles of the American system along with their continued relevance to public policymaking.

5. **Foreign Political Culture & Statecraft:** Students will be able to recognize the importance of different political cultures, the ideas and belief systems that animate them, their forms of statecraft, and their foreign policy purposes.

6. **Effective Communication:** Students will be able to communicate effectively with well-developed reasoning, writing, and rhetorical skills.

Each year, one ILO is selected for assessment across all relevant degree programs (both in-person and online). ILO #6 for effective communication is automatically assessed every year and is already incorporated throughout all courses with rubrics the faculty use for both written and oral assignments toissue grades: IWP Oral Presentation Grading Rubric and IWP Written Product Grading Rubric. Please see Diagram 1 for reference to the current assessment schedule of ILOs.

Diagram 1. Multi-Year Continuous Improvement and Assessment of Institutional Learning Outcomes.



Based on IWP's curriculum mapping for its Joint Master of Science in Cyber Intelligence and Security (Joint Cyber MS) with Capital Technology University (Capitol), Table 1 below shows the alignment of ILOs to this Cyber MA's Program Learning Outcomes (PLOs), which are as follows, in that students will be able to:

1. Demonstrate knowledge of basic terms, concepts, history, theories, and geography related to the U.S. foreign policy process, international affairs, and the current world order (ILO 1, 5)

2. Integrate various tools of statecraft into a coherent whole. (ILO 3)

3. Analyze the major national security challenges facing the United States. (ILO 1)

4. Appreciate Western moral tradition and its applicability to national security and foreign policy. (ILO 4)

5. Apply knowledge of basic terms, concepts, history, theories, and geography related to cyber statecraft. (ILO 2)

6. Evaluate the increasing importance of the cyber domain to U.S. national security strategy and the challenges to bring cyber operation theories into practice. (ILO 2)

Table 1. IWP's ILO connection to PLOs for Joint Cyber MA

Degree	ILO 1	ILO 2	ILO 3	ILO 4	ILO 5	ILO 6 ALL COURSES
Joint Cyber MS	PLO 1, 3	PLO 5, 6	PLO 2	PLO 4	PLO 1	

Meanwhile, Table 2 below shows how each course and its Course Learning Outcomes (CLOs) align with IWP's ILOs.

Table 2. IWP's ILOs connection to CLOs for Joint Cyber MS (Note: All CTU courses connect to ILO 2 for Specialized Knowledge).

ILO 1	ILO 2	ILO 3	ILO 4	ILO 5	ILO 6
IWP 605 (CLO 1, 3)	IWP 605 (CLO 5)	IWP 605 (CLO 2)	IWP 605 (CLO 4)	IWP 605 (CLO 5)	ALL COURSES
IWP 610 (CLO 1, 2, 4)	IWP 610 (CLO 3)	IWP 627 (CLO 2)	IWP 615 (CLO 1-4)	IWP 610 (CLO 3)	
IWP 627 (CLO 1, 3)	IWP 699 (All CLOs)		IWP 627 (CLO 4)	IWP 627 (CLO 5)	
	IAE 500				
	IAE 671				
	IAE 674				
	IAE 675				
	IAE 677				
	IAE 679				
	IAE 680				
	IAE 682				
	IAE 685				
	CS 620				

The Institute uses various direct and indirect measures for evaluation (see Table 3 below). Some measures are qualitative, while most are quantitative, with benchmarks set to establish trends and ensure outcomes are met. In the case of the Joint Cyber MS, IWP's relevant courses will be assessed as usual per the relevant ILO (Table 2) and schedule (Diagram 1) indicated above. CAPITOL's courses are connected to IWP's ILO 2, so they will likely be assessed in the next cycle (AY 2029) since AY 2024 will be too soon. At that time, IWP will coordinate with CAPITOL to obtain the necessary assessment data where applicable: CAPITOL's relevant course assessments (including from its Capstone IAE-674) to show results of student learning outcome achievement, faculty evaluations, number of completions per year disaggregated by race/ethnicity and gender (see green highlights on Table 3). While studying at IWP, Joint Cyber MS students may also be included among those who receive remedial writing and financial support as well as participate in relevant surveys listed under Indirect Measures. Joint Cyber MS alumni may also participate in relevant surveys and alumni networking and speed mentoring. For simplicity in coordinating with CAPITOL, data collection from CAPITOL for all measures will only occur when ILO 2 is being assessed since this is a specialized, joint degree distinct from IWP's other degrees.

Table 3. IWP's Direct and Indirect Measures		
Assessment Categories	**Direct Measures**	**Indirect Measures**
Course Level	*I.A. Course Assessments of Learning Outcome Achievement *I.B. Remedial Writing Support *I.C. Faculty Evaluation by the Academic Dean	*Student course evaluations are already incorporated into measures for Remedial Writing Course and Faculty Evaluation.*
Program Level	*II.A. MA and Doctoral Comprehensive Examination Evaluations **(N/A)** *II.B. Completions by Degrees Awarded **(N/A)** *II.C. Post-Completion Job Placement **(N/A)**	*II.D. Further Education, Five-Year Alumni Survey *II.E. PLO Achievement from Survey of Recent Graduates
Institutional Level	*III.A. IWP's MA Capstone Course **(N/A)** *III.B. Retention Rates **(N/A)** *III.C. Thesis Evaluations at both MA and Doctoral Levels **(N/A)** *III.E. Alumni Networking & Speed Mentoring *III.H. Financial Support of Student Achievement III.I. Student Completion (Graduation) Rates by Race/Ethnicity	*III.D. ILO Achievement, Five-Year Alumni Survey *III.F. Meaningful Life, Five-Year Alumni Survey *III.G. Climate Survey

The assessment committee scrutinizes this assessment's results (which would include a CAPITOL representative when ILO 2 is assessed) to determine if IWP should consider any changes to maintain or improve the educational achievements of students. This, in turn, helps to inform any adjustments that need to be made to our strategic operations, resources, and budget. Any changes require approval by IWP's Academic Council. Financial implications or impact to departments outside of Academic Affairs must also involve approval by IWP's Executive Vice President.

Curriculum and Program Review Process (CPRP) at IWP

As a complement to the EEA Plan (and vice versa), the Curriculum and Program Review Process (CPRP) plan is a five-year cycle that entails IWP academic staff and faculty conducting an extensive review of the curriculum (usually beginning in late spring). The first year of the cycle entails assessment of learning outcomes to confirm they are realistic, rigorous, appropriate to higher education (i.e., taxonomies), consistent with the IWP Mission (via curriculum mapping), and accurately reflected throughout the curriculum and evaluation processes. During the second through fifth year of the cycle, Program Reviews of all degrees (and Certificates but with a modified approach) will occur, which include analysis of student achievement data to help interpret educational effectiveness assessment results/summaries. The Joint Cyber MS would likely fall under "New Programs" for Academic Year (AY) 2027 Program Reviews (see Diagram 2 below). The subcommittee selected to review this degree would also include a CAPITOL faculty representative.

Diagram 2. Five-Year Learning Outcomes and Program Review Schedule

AY24 Program Reviews (Year 2) 1. Certificates	AY25 Program Reviews (Year 3) 2. MA SNSA 3. MA SIA 4. MA SIS	AY26 Program Reviews (Year 4) 5. Online MA 6. Exec MA 7. Online ExecMA 8. DSNS	AY27 Program Reviews (Year 5) 9. ProfMA 10. Online ProfMA 11. New Program(s)	AY28 Learning Outcomes Review (Year 1)	AY29 Program Reviews (Year 2) 1. Certificates

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 **Joint MS in Cyber Intelligence and Security** degree is a unique program designed to meet the long-standing needs of combining intelligence and national security with the technical skills for cybersecurity and understanding cyberspace. This degree gives a competitive advantage to students and secures influential positions in Cyber Intelligence and Security, where a convergence of strategy and technology is essential. It is designed to meet the demands of the highest-skilled professionals to become influential leaders who will be involved in advancing and expanding the Cyber Intelligence and Security environment on a large and small scale. This degree is for current professionals in the cyber, intelligence, or national security fields who desire to elevate their skills to attain executive and senior-level cyber intelligence and security positions in commercial companies as well as local, state, and federal government.

The **Joint MS in Cyber Intelligence and Security** program is designed as a master's degree where students can quickly engage in leadership, research, and publishing. It can serve as a preamble to a doctorate and equip students with the balance of skills for a higher degree.

Description of program requirements:

Entrance Requirements

The Joint **MS in Cyber Intelligence and Security** program is designed for students with at least a bachelor's degree in an appropriate discipline and relevant work experience. To be accepted into the Joint **MS in Cyber Intelligence and Security** program, students must have completed an appropriate bachelor'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).

International students are required to take the TOEFL and score at least 600 on the paper-based test or 95 on the internet-based test if their degree was not from a university where it was taught in English.

Degree Requirements:

The following is a list of courses for the **MS in Cyber Intelligence and Security** degree. Students expecting to complete this degree must meet all prerequisites for the courses listed below. Completing this program requires a Cybersecurity Capstone course (IAE-674).

Master of Science in Cyber Intelligence and Security
Courses
Total Credits: 48

48 CREDITS

The curriculum consists of 48 credits. All courses will be conducted online. To earn these degrees, students will take the following courses:

IWPO 601 National Security Policy Process – 4 credits (online)

This course is an introduction to the design, administration, and management of U.S. national security – the foundation, structure, functions, and processes among competing branches of government, departments, and agencies, and personalities that all exist within a common framework to secure the nation, but whose perspectives and methods frequently clash. Policies often emerge after following a long and tortuous path. When they emerge, they sometimes do so with only a bare resemblance to the original plan; at times, they do not emerge. We will examine why. Many courses on U.S. national security concentrate primarily on the results of a policy but rarely on how a policy is made, maintained, or modified. This course introduces students to critical but largely ignored aspects of how U.S. national security policies are developed, decided upon, implemented, executed, and reviewed within the government – and frequently influenced beyond it.

IWPO 605 Intelligence and Policy – 4 credits (online)

This course examines the elements and purpose of intelligence, requirements of successful intelligence analysis, intelligence processes, counterintelligence and security, the relationship between intelligence and policy, and how American political and cultural values affect the role of intelligence in America.

This course addresses several major intelligence issues:

1. The intelligence process and methodology, including the structure of the intelligence system.
2. The necessity of coherent intelligence policy.
3. The limits and utility of intelligence.
4. The importance of political intelligence, particularly concerning foreign methods of statecraft.
5. The role of counterintelligence and the importance of counterintelligence analysis to the making of foreign policy.
6. The problems of intelligence epistemology, including deception, propaganda, perceptions management, and internal cultural and perceptual predispositions and biases.

IWPO 608 Sources of American Political Thought – 2 credits (online)

American foreign policy rests in part on the character of America. The American political order is a particular expression of Western political thought. Thus, an understanding of what fuels American foreign policy is in part dependent on a solid understanding of Western political thought: ancient, medieval, and modern. The course emphasizes the way in which the American political order and its philosophic foundations affect U.S. foreign policymaking. Particular attention will be given to the Federalist and the writings and speeches of George Washington and Abraham Lincoln and other American statesmen of renown.

IWPO 627 International Relations, Statecraft, and Integrated Strategy – 4 credits (online)

This course introduces the field of international relations in a way that blends issues of theory and practice. It is designed to give students an understanding of those questions of international relations theory that have a direct bearing on the ability of policy practitioners to accomplish their mission. The issues of war and peace will be examined in relation to the international system, the problem of sovereignty, and alternative concepts of world order, including the balance of power and the need to create new political forms. The course will then introduce the various statecraft methods available to policymakers and examine how they have been used successfully in pursuing national interests and purposes. These include the instruments of power, such as: military power; economic strategy; intelligence; the use of information, disinformation, and propaganda; various types of diplomacy, political, moral, and psychological influence; and other instruments of "soft power."

IWPO 699 Cyber Intelligence Overview – 4 credits (online)

This course will introduce the student to the study and practice of Cyber intelligence, from a government and commercial perspective. This course is not intended to be a comprehensive area study but rather an introduction to the various aspects of cyber intelligence. It will deal with both practical application and theory. The student will be exposed to current intelligence and counterintelligence methods as well as current and emerging technologies. Cyber intelligence is the acquisition and analysis of information to identify, track, and predict cyber capabilities, intentions, and activities. Students will learn how to add value to the information and to present actionable courses of action to the decision maker. They will understand the traditional intelligence tradecraft and how it is used in the cyber world to assess cyber threats. This will be done by understanding the history and application of intelligence technology, intelligence analysis and counterintelligence. Students will learn about diverse types of cyber threat actors; state, non-state, and rogue actors.

IAE 685 Principles of Cyber Security – 3 credits (online)

This class explores the overarching security architectures and vectors of information assurance from a management perspective to allow the learner to formulate the basis for sound business decisions. Students gain an appreciation for systems, networks, processes, methodologies, documentation requirements, recovery processes, certification, and accreditation processes as well as "best practice" implementation, training and continuous improvement. Discussions in this course give the correct acumen of personnel security, physical security, and technical operational security as these principles relate and interface with information security principles. Defense-in-depth principles also are covered for designing proper physical security programs. At the completion of the course students should be able to manage an IA function and evaluate an organization's Contingency Planning process for adequacy.

IAE 671 Legal Aspects of Computer Security and Information Privacy – 3 credits (online)

This course provides an overview of the legal rights and liabilities associated with operation and use of computers and information, including the legal and regulatory compliance issues critical for chief information security officers. It discusses the key statutes, regulations, treaties, and court cases (in the United States and abroad) that establish legal rights and responsibilities as to computer security and information privacy. The course also helps students to learn how to reduce their risk of potential legal liability for computer security or information privacy failures, and how to enforce their security and privacy rights against other parties. Case studies and lessons learned from information security failures are used throughout the course.

IAE-675 Computer Forensics and Incident Handling – 3 credits (online)

This course begins with lectures discussing the laws and rights to privacy by individuals and what organizations may or may not do. Online ethics are considered. It then moves on to understanding incident handling and how incident response teams work, managing trouble tickets, and basic analysis of events to determine if an incident has occurred. It concludes with computer forensics issues and practices, and rules of evidence. This course prepares students for the Access Data Certified Examiner (ACE) and Mobile Phone Examiner Plus (MPE+) Certifications. Prerequisite: IAE-685 and CS-620 or waiver.

IAE-677 Malicious Software – 3 credits (online)

This course examines malicious software detection and malicious software defenses including tripwire and signature software techniques. Viruses, worms and Trojan horses, logic bombs and malicious CGI scripts will be discussed. Students will review the anatomy of well-known viruses and worms to understand how they work. Mobile code issues as they apply to web and application technologies and resulting insecurities will be discussed in detail. Students will then review the underlying methodologies used by the anti-virus vendors and freeware offerings to protect electronic assets from harm or other compromise. Prerequisite CS-620 or waiver.

IAE-682 Internal Protection – 3 credits (online)

This course explores the protections available to the practitioner through host operating systems and third-party equipment and software, to protect the inner network from the attacker who has successfully

circumvented the perimeter or from the disgruntled insider. Use of methodologies including host-based intrusion detection methods, audit settings and review PC Firewalls, host operating hardening for Linux and Windows operating systems, and Virtual LANs will be reviewed. It is recommended that students complete IAE-685 before taking this course, but this is not a requirement.

IAE-680 Perimeter Protection – 3 credits (online)

In this "defense-in-depth" course, firewalls and network IDS issues are discussed. A detailed understanding of security systems, firewall configuration and rule sets, load balancing, web farms, wireless access, web security issues and network intrusion detection is explored to prepare the student with the basic tools to coordinate the design and implementation of perimeter network defenses for a high volume, high access site. Prerequisite: Completion of at least 24 credit hours in IAE coursework. This class is best completed in the last term.

IAE-674 Security Risk Management (capstone course) – 3 credits (online)

This course begins with an understanding of why risk management evaluations are useful. The general methodologies for security risk assessment and security test and evaluation, including the interviews are discussed and documentation research necessary, the student is provided practical lab exercises to provide a hands-on analysis of a fictitious site. Detection, recovery, and damage control methods in contingency/disaster recovery planning research, documentation and training; methods of and procedures for contingency planning and security policy formulation and enforcement.

IAE-679 Vulnerability Mitigation – 3 credits (online)

This "Defense-in-Depth" course provides the student detailed understanding of the need for internal and external vulnerability assessment. An integral technical part of any risk management program, this course goes hand-in-hand with the more analytical practices in IAE-674. Prerequisite CS-620 or waiver. Co-requisites: IAE-685.

IAE 500 Introduction to Information Assurance* - 3 credits (online) (leveling course)

This course will provide the requisite computer, data communications, Internet and database skills to students embarking on careers in information assurance, at the senior levels. It is designed primarily for professionals who seek concentrated professional education in one or more of the many fields associated with IA. Students who complete this course successfully will be able to master the more technical application and analysis skills demanded by the Master of Science in Cybersecurity degree program, and the several certificate programs offered in various IA concentrations. Labs, simulations and special problems will be used throughout the course.

CS 620 Operating System Principles for Information Assurance** - 3 credits (online) (leveling course)

This course is an overview of the UNIX operating system. The content will include shell programming, process management, processor management, storage management, scheduling algorithms, resource protection and system programming. The course will include programming projects focused on information assurance problem solving, primarily utilizing the C programming language. Students are expected to be familiar with virtual machines, the UNIX command line, and an introductory programming language. Basic knowledge of C programming and UNIX is helpful.

***Students who can demonstrate knowledge of information assurance topics at an undergraduate level through undergraduate transcripts, certifications, or work experience may have IAE500 waived with appropriate documentation evaluated at the time of admission.**

****Students who can demonstrate knowledge of the UNIX operating system and C programming language may have CS620 waived with appropriate documentation, which will be evaluated at the time of admission.**

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.**

   There are no such requirements.

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

   Capitol Technology University has agreed with The Institute of World Politics to offer the cooperative MS in Cyber Intelligence and Security. The MOU is attached as an appendix to this proposal.

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 Joint **MS in Cyber Intelligence and Security** 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 both of the universities' websites and via e-mail and regular mail (by request). Faculty/student interaction expectations are available to students during virtual open house events, literature, websites, etc. This information is also part of the material distributed for each course. Students receive guidance on proper behavior/interaction with their Department Chair (or Dean of Students for IWP) 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.

Capitol's academic support services, financial aid resources, costs, 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. IWP follows a similar approach.

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 **Joint MS in Cyber Intelligence and Security** 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. It is the content source for every new program at the University. CAPITOL has also coordinated with the Institute of World Politics to ensure the content is in sync for its application to the District of Columbia's Higher Education Licensure Commission (DC HELC).

H. Adequacy of Articulation:

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

Capitol Technology University has agreed with The Institute of World Politics to offer the cooperative MS in Cyber Intelligence and Security. The MOU is attached as an appendix to this proposal

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. Kellep Charles, Dr. William Butler, Dr. Richard Hansen, Dr. Clifford Benedict, et al. are full-time faculty members. All of the faculty members hold relevant 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's goals for student success. Additional qualified faculty will be added as needed.

Professors who will be engaged with the Joint **MS in Cyber Intelligence and Security** are:

Capitol Technology University			
Dr. Kellep Charles		DSc Cybersecurity MS Telecommunications BS Computer Science	IAE-675 Computer Forensics and Incident Handling IAE 500 Introduction to Information Assurance IAE 671 Legal Aspects of Computer Security and Information Privacy CS 620 Operating System Principles for Information Assurance IAE-679 Vulnerability Mitigation IAE 685 Principles of Cyber Security
Dr. William Butler		DSc Cybersecurity MS Telecommunications BS Computer Science	IAE-677 Malicious Software IAE-674 Security Risk Management IAE-682 Internal Protection IAE-680 Perimeter Protection
Dr. Richard Hansen		PhD Technology MS Computer Science BS Electrical Engineering	IAE-674 Security Risk Management IAE-679 Vulnerability Mitigation IAE 685 Principles of Cyber Security IAE 500 Introduction to Information Assurance CS 620 Operating System Principles for Information Assurance
Dr. Clifford Benedict		DSc Cybersecurity MS Computer Information Systems, BS Electronics and Computer Engineering	CS 620 Operating System Principles for Information Assurance IAE 685 Principles of Cyber Security
Institute of World Politics			
Jeffrey Johnson, Adjunct Faculty		Education Master of Arts in Strategic & International Studies, Concentration in Intelligence, 2021 The Institute of World Politics Bachelor of Science in History, Minor in Military Science, 2003	IWPO 601

		Southern Illinois University, Edwardsville Certifications: Building Partner Capacity | Host Nation/ Foreign Weapon Fundamentals ▏ Tactical Combat Casualty Care ▏ SERE C Full Spectrum Instructor ▏ Special Programs Heavy Weapon Operators Course Pathfinder, Airborne, and Air Assault Course ▏ Advanced Counter Insurgency Leader Course Honors & Achievements: Bronze Star Medal Recipient Letter of Recommendation-United States Ambassador to Somalia Valorous Unit Award ▏ Army Commendation Medal ▏ Army Achievement Medal ▏ National Defense Service Medal Afghanistan Campaign Medal ▏ Iraq Campaign Medal ▏ Global War on Terrorist Expeditionary Medal Army Service Ribbon ▏ NATO Ribbon ▏ Combat Infantryman Badge ▏ Pathfinder Badge ▏ Airborne Badge Air Assault Badge ▏ US AF Enlisted Aircrew Badge	
Aaron Danis, Adjunct Faculty		Norwich UniversityNorwich University Bachelor's degree, Government and Military StudiesBachelor's degree, Government and Military Studies The George Washington University Master's degree, National Security Policy StudiesMaster's degree, National Security Policy Studies	IWPO 605
James Robbins, Full-Time Faculty and Dean of Academics		Doctor of Philosophy, The Fletcher School of Law and Diplomacy, Tufts University, 1991 Master of Arts in Law and Diplomacy, The Fletcher School	IWPO 608

		of Law and Diplomacy, Tufts University, 1988 Master of Arts in Political Science, The University of Cincinnati, 1986 Bachelor of Arts Cum Laude with High Honors in Political Science, The University of Cincinnati, 1984	
John Lenczowski, Full-Time Faculty and Chancellor		Dr. Lenczowski's Education; B.A., 1972, University of California, Berkeley M.A., 1975 Johns Hopkins University School of Advanced International Studies Ph.D., 1980, Johns Hopkins University School of Advanced International Studies	IWPO 627
Paul Davis, Adjunct Faculty		Professional Experience: Significant active-duty and reserve service in Army intelligence Began working cyber intelligence in the early 1990s, looking at North Korean cyber operations Both while a reservist and after retiring, worked as a contractor for USG clients, both on counterintelligence and cyber security Vice President of Government Business Development, SecureDAM Senior Research Fellow, Soran University Iraq Founder and President, JANUS Think Education: B.A., 1979, Kean College of New Jersey M.A., 2010, American Military University	IWPO 699

Lead experts

Dr Kellup Charles completed his Doctorate in Cybersecurity at Capitol Technology University. He also holds a Master of Science in Telecommunication Management from the University of Maryland University College and a Bachelor of Science in Computer Science from North Carolina Agricultural and Technical State University.
Dr. Charles worked as a government contractor in the Washington, DC area as an information security analyst for over 20 years in the areas of incident response, computer forensics, security assessments, malware analysis, and security operations. He is the creator and executive editor of SecurityOrb.com (@SecurityOrb), an information

security & privacy knowledge-based website with the mission to share and raise awareness of the motives, tools, and tactics of the black-hat community, and provide best practices and countermeasures against malicious events. Dr. Charles has appeared and made regular contributions to local media outlets such as PGCTV, WPGC 95.5 FM, Politc365.com, WPFW 89.3, and Examiner.com to discuss technology, security, and privacy matters.
He has served as an adjunct professor at Capitol Technology University since 2001in their computer science & cybersecurity departments. His industry certifications include Certified Information Systems Security Professional (CISSP), Cisco Certified Network Associate (CCNA), Certified Information Systems Auditor (CISA), National Security Agency – INFOSEC Assessment Methodology (NSA-IAM), and Information Technology Infrastructure Library version 3 (ITILv3) among others. Dr. Charles serves as a professor, Director of Cyber Labs, and Director of Center for Cybersecurity Research and Analysis (CCRA) for Capitol Technology University's Cybersecurity department. He is Chair of Cybersecurity programs at the university.

Dr. William Butler
Dr. William (Bill) Butler was previously Cybersecurity Chair for 8 years at Capitol Tech. Earlier in his career, he worked in the networking and IT industries as a network engineer and consultant for over 20 years. Dr. Butler also served as a joint qualified communications information systems officer in the U.S. Marine Corps and retired as a Colonel with 30 years of service (active and reserve). He is very active in various working groups such as the National Institute of Standards and Technology Cloud Computing Security Forum Working Group (NIST CCSFWG), Cloud Security Alliance (CSA) Big Data and Mobile Computing Working Group, and the National CyberWatch Center Curriculum Taskforce and the National Cybersecurity Student Association Advisory Board. Dr. Butler holds degrees from Brenau University, Marine Corps University, U.S. Army War College, National Defense University, University of Maryland and Capitol Technology University. He earned his DSc in Cybersecurity at Capitol in 2016 researching consumer countermeasures to illegal cellphone intercept.

Dr. Richard Hansen
Dr. Rick Hansen is a Professor of Practice in Unmanned & Autonomous Systems and Astronautical Engineering for Capitol Technology University and has experience in research, development, and operations for UAS & AE. His research focuses on low-cost methods of communication with near space (High Altitude Balloons) and orbital systems (satellites) as well as developing inexpensive sensing platforms using commonly available components. Dr. Hansen works with government, industry, and academia to ensure the program is addressing their needs and that students are qualified for internships and full-time employment. He also oversees the activities below to develop students' skills, abilities, and knowledge so they can become leaders in their field. Dr. Hansen enjoys helping students develop technologies and publish research. He received his doctoral and bachelor's degrees from Capitol and his master's degree from Johns Hopkins University. His entrepreneurial projects include supporting the U.S. Department of Defense's (DoD) Cybersecurity Maturity Model Certification (CMMC) program, research in quantum computing and other platforms, and technology that supports CubeSat and drone operations.

Dr. Clifford Benedict
The Director of the Cyber Labs and Assistant Cybersecurity Professor at Capitol Technology University. Dr. Benedict brings a wealth of expertise, holding a Bachelor of Science in Electronics and Computer Engineering, a Master of Science in Computer Information Systems, and a Doctor of Science in Cybersecurity, with a focus on the application of artificial intelligence (AI) and machine learning (ML) in security contexts. With an impressive track record spanning more than two and a half decades, Dr. Benedict has excelled in infrastructure management, architecture design, cybersecurity, machine learning, software development, integration, implementation, and process enhancement. His consulting experience includes reputable organizations such as Apple, PayPal, SAP, CareFirst, Cigna, JPMorgan Chase, Symantec, Boeing, US Space Force, US Navy, and more.

Jeffrey Johnson

Jeff Johnson is a former Army Combat Arms Officer and Foreign Affairs Specialist. He has expertise in Security Cooperation; Political-Military Relationships; National Security Policy; Unconventional Warfare; Low Intensity Conflict; Title 10, 22, and 50; AFRICOM and CENTCOM Operational Variables; and Interagency Operations.

Aaron Danis

Mr. Danis is a career terrorism and counterterrorism specialist, holding a Bachelor's degree in Military Studies and a Master's degree in Security Policy Studies. He is a retired U.S. Army intelligence officer and has served in the Naval Criminal Investigative Service, U.S. Coast Guard Intelligence, the Treasury Department, the U.S. Nuclear Regulatory Commission, the National Counterterrorism Center, and the National Defense University. He recently retired from the U.S. government after serving as the Office of the Director of National Intelligence (ODNI) faculty chair at the National Intelligence University for 4 years during its transition from the Defense Intelligence Agency to ODNI.

James Robbins

Dr. James S. Robbins is a national security columnist for *USA Today* and Senior Fellow in National Security Affairs at the American Foreign Policy Council. Dr. Robbins is a former special assistant in the Office of the Secretary of Defense, and in 2007 was awarded the Chairman of the Joint Chiefs of Staff Joint Meritorious Civilian Service Award. He is also the former award-winning Senior Editorial Writer for Foreign Affairs at *The Washington Times*. His work has also appeared in *The Wall Street Journal*, *National Review*, and other publications. He appears regularly on national and international television and radio. Dr. Robbins holds a Ph.D. from the Fletcher School of Law and Diplomacy and has taught at the National Defense University and Marine Corps University, among other schools. His research interests include terrorism and national security strategy, political theory, and military history. Dr. Robbins is the author of five books, including *The Real Custer: From Boy General to Tragic Hero*, *This Time We Win: Revisiting the Tet Offensive*, and the critically acclaimed *Last in Their Class: Custer, Pickett and the Goats of West Point*.

John Lenczowski

John Lenczowski is Founder, President Emeritus, and Chancellor of The Institute of World Politics. From 1981 to 1983, Dr. Lenczowski served in the State Department in the Bureau of European Affairs and as Special Advisor to Under Secretary for Political Affairs Lawrence Eagleburger. From 1983 to 1987, he was Director of European and Soviet Affairs at the National Security Council. In that capacity, he was principal Soviet affairs adviser to President Reagan. He has been associated with several academic and research institutions in the Washington area, including Georgetown University, the University of Maryland, the American Enterprise Institute, the Ethics and Public Policy Center, the Council for Inter-American Security, and the International Freedom Foundation. He has also served on the staff of Congressman James Courter. He is the author of Soviet Perceptions of U.S. Foreign Policy (1982); The Sources of Soviet Perestroika (1990), Cultural Diplomacy: A Multi-faceted Strategic Asset of Soviet Power (1991); Full-Spectrum Diplomacy and Grand Strategy (2011) and numerous other writings and addresses on U.S. foreign policy, public diplomacy, cultural diplomacy, counter-propaganda, political warfare, Soviet/Russian affairs, comparative ideologies, intelligence, strategic deception, counterintelligence, and integrated strategy. Dr. Lenczowski attended the Thacher School, earned his B.A.

at the University of California, Berkeley, and received his M.A. and Ph.D. from the Johns Hopkins University School of Advanced International Studies.

Paul Davis

Paul Davis has experience in both strategic and tactical political/military analysis that has spanned from the Cold War to the current upheaval in the Middle East. Beginning as a Soviet analyst, Prof. Davis assessed tactical capabilities and senior political issues that arose within the politburo and its impact on U.S. doctrine. Following the collapse of the Soviet Union, he began to focus on analysis of North Korea, assessing its new tactics and technologies, including cyber operations. Later, he moved to the Middle East and transitioned his focus to the analysis of Iran, Syria, and Iraq. In the U.S. Army, Prof. Davis was the lead analyst for MNA-3 Syria/Lebanon and coordinated with the IC on military and political issues affecting the tasked countries in regional and international activities. From 2003 to 2005, Prof. Davis served as lead intelligence analyst with the DIA's Iraq Division, where he was responsible for Military and Political intelligence production in support of Operation Iraqi Freedom. He received his B.A. from Kean College of New Jersey and his M.A. from the American Military University. He is the founder and president of JANUS Think, a consulting organization dedicated to supporting government contractors and commercial companies in business development. He also serves as vice president of government business development at SecureDAM, where he works on cyber security and cyber intelligence issues. Prof. Davis is also a senior research fellow at Soran University in Iraq. He works with the university to explain U.S. Government decisions and support research initiatives on relevant issues.

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

   > Two Missouri State professors, historian Charles Bonwell and psychologist James Eison, coined the term "active learning." In their 1991 book, Active Learning: Creating Excitement in the Classroom, they offered this definition: "active learning involves students in doing things and thinking about the things they are doing."
   >
   > Though it seems circuitous, the definition 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 " do" something in class and then apply critical thought and reflection to their classroom work and activity. Their argument was backed up by research. Even 20 years earlier, Bligh pointed out that the immediate rehearsal of new information and knowledge significantly impacted 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 repeatedly, in various ways, and with opportunities.

The central tenet of active learning — that practice and interaction matter— 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 full-time 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.

For IWP, all faculty (online asynchronous and in-person synchronous) receive training from the e-Learning Designer and Director of IWP Media on how to best create, structure, and deploy course content to take advantage of the online learning medium. The faculty are continually supported throughout the semester by the e-learning team in providing valuable and efficient education to the students. Online resources are consistently updated and provided to the faculty through online courses and live sessions.

IWP borrows from several sources of best practices for pedagogical methods, such as Edgar Dale's Cone of Experience and the Jigsaintegrated and cooperative learning technique. Some examples of methods used by IWP faculty for online learning are as follows:

- Case-Based Learning Approach (e.g., case study analysis or professor sharing personal experience in the field to help teach concept)
- Guest Lecturing
- Directed Discussion by Professor (i.e., direct, specific, or open-ended questions that are connected to learning outcome)
- Reflective Dialogue/Writing (e.g., requiring students to keep a journal to write their own thoughts about each lesson)
- Having students participate in hands-on experience as an assignment (e.g., writing a President's Daily Brief or Strategy memorandum)
- Interactive Lecture or Collaborative Lessons (e.g., Group/Class debates or exercises, free interactive response polls that allow students to respond to questions anonymously)
- Collaborative Research Project with Professor or Group of Classmates
- Simulating, Modeling, or Experiencing a Lesson (e.g., crisis simulation, use of free or low-cost government/other credible training tools to practice a skill, etc.)

These methods are encouraged through the course assessment process and training is provided through Faculty meetings and from the Academic Affairs department.

b) The Learning Management System

Capitol'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 provides 24-hour support to the faculty. Meanwhile, IWP has a Media Development & Production Team that coordinates with Academic Affairs to support the online program needs of its faculty and students. Canvas is the online Learning Management System for both universities. When a new faculty member is assigned to teach an online course, Capitol's 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 and compliance with the institution's online teaching pedagogy. Capitol believes this provides the highest-level learning experience for faculty members and, in turn, students attending online classes. IWP follows a similar process.

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 its associated strategies for distance education/online learning.

> Keller's ARCS motivational model is used in the online delivery of teaching and learning to increase learner motivation. This model has been considered an important element in online education because of its implications on increased learner motivation and learning outcomes. Keller's model consists of motivating students by maintaining and eliciting attention (A), such as through 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 in students, making the connection between learning objectives and future learning goals, autonomous thinking and learning, and fostering student satisfaction. Various educational online programs have researched Keller's ARCS model 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 well 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 full-time and adjunct faculty to ensure all members receive the training. Additionally, the live sessions are recorded for those faculty who cannot attend the live training session due to other professional commitments or who teach classes at the training delivery time.

IWP uses the same approach and training as described above.

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.**

Capitol Technology University

Library Services: The Puente Library offers extensive services and a wide collection for Capitol Technology University students to succeed academically. 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 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 Aviation Maintenance, B.S. in Cyber Analytics, B.S. in Cybersecurity, B.S. in Data Science, B.S. in Electrical Cyber Psychology, B.S. in Electrical Technology, B.S. in Aviation, 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, B.S. in Mechatronics and Robotics Technology, B.S. in Software, and B.S. in Technology and Business Management, B.S in Uncrewed 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 Internet Cybersecurity, M.S. in Uncrewed 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, Master of Research (PhD) in Artificial Intelligence, PhD. in Aviation, PhD. in Business Analytics and Data Sciences, PhD. in Construction Science, PhD. in Critical Infrastructure, PhD. in Emergency and Protective Services, PhD. in Human Factors, PhD. in Manufacturing, PhD. in Occupational Health and Safety, PhD. in Product Management, PhD in Quantum Computing, PhD. in Technology, PhD. in Technology/M.S. Research Methods Combination Program, PhD. in Uncrewed Systems Applications.

Therefore, the library is fully prepared to support an MA **in Cyber Intelligence and Security.**

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 areas 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 necessary documents. 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 Aviation 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 also provides the Puente Library with quick access to these materials.

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

The Institute of World Politics

A suite of electronic databases is available to researchers. This suite includes such tools as:

- HeinOnline Academic
- JSTOR
- EBSCO Political Science Complete
- EBSCO Religion and Philosophy Collection
- EBSCO Military and Government Collection
- EBSCO International Security & Counter Terrorism Reference Center
- EBSCO Academic Search Premier
- EBSCOhost for Electronic Books
- Columbia International Affairs Online (CIAO)
- Britannica Online
- Taylor & Francis Online
- Interpretation Journal – A Journal of Political Philosophy
- The Journal of Political Risk
- The Vatican Apostolic Library
- Military Strategy Magazine
- Project MUSE
- Forgotten Books

- World Politics Review
- Homeland Security Digital Library

Other electronic resources include e-books, newspapers, and other materials. The IWP library is developing topical pathfinders to assist researchers. In addition to the advice and research instruction available from the library staff in person, the library maintains an extensive list of online research tools, including:

- Tutorials on research and writing skills
- Electronic books and other scholarly texts available online
- Online databases for other area libraries

To help students understand the depth and breadth of material by attending IWP, the library offers scheduled orientation sessions to meet with library staff and receive a detailed description of the resources available. Additionally, the library staff encourages students to request individual or small-group research instructions at any time throughout the semester. "IWP Library resources can disproportionately impact student papers, presentations, and research," commented Director of Library Services Dmitry Kulik. "I encourage students to take advantage of this opportunity."

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 Uncrewed Systems Lab meet the potential research needs of the students. The labs provide both local and virtual support. IWP will not require any additional facilities to provide its course of instruction.

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 and the Institute of World Politics provide students and faculty with an institutional electronic mailing system. The universities require all students and faculty to use the email system in all the institution's course delivery modalities. Capitol

and IWP students and faculty are required to use the institution's email addresses (e.g., xxxxxxxx@captechu.edu, xxxxxxx@iwp.edu) in all university matters and communications. Both universities use email capabilities in Microsoft Office 365 and Microsoft Outlook.
A Learning Management System that provides the necessary technological support for distance education

Capitol Technology University and the Institute of World Politics provid a robust Learning Management System (LMS) through the use of the Canvas LMS by Instructure (www.canvaslms.com). Capito also 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. Canvas is required for every class; as a result, every course has a classroom on Canvas (and Zoom, in the case of Capitol). All syllabi, grades, and assignments must be entered into Canvas on time throughout the semester. IWP also uses Canvas as its learning management system.

Canvas provides the world's most robust LMS. It is a 21st-century LMS; Canvas is a native cloud hosted by Amazon Web Service. The system is adaptable, reliable, and customizable. Canvas is easy for students and faculty to use. 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, while the Institute of World Politics recently switched from Moodle to Canvas as of January 2023. 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)	$413,208	$722,952	$916,776	$1,170,864	$1,486,224
a. Number of F/T Students	8	12	16	20	24

b. Annual tuition/Fee rate	$26,460	$26,460	$26,460	$26,460	$26,460
c. Total F/T Revenue (a x b)	$211,680	$317,520	$423,360	$529,200	$635,040
d. Number of P/T Students	12	18	28	36	46
e. Credit Hour Rate	$933	$956	$979	$1,003	$1,028
f. Annual Credit Hour	30	30	30	30	30
g. Total P/T Revenue (d x e x f)	$335,880	$516,240	$822,360	$1,083,240	$1,418,640
3. Grants, Contracts and Other External Sources	$0	$0	$0	$0	$0
4. Other Sources	$0	$0	$0	$0	$0
TOTAL (Add 1 – 4)	$413,208	$722,952	$916,776	$1,170,864	$1,486,224

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)	$340,000	$340,000	$340,000	$340,000	$340,000
a. #FTE	4	4	4	4	4
b. Total Salary	$408,000	$408,000	$408,000	$408,000	$408,000

c. Total Benefits (20% of salaries)	$68,000	$68,000	$68,000	$68,000	$68,000
2. Admin Staff (b + c below)	$48,000	$48,000	$48,000	$48,000	$48,000
a. #FTE	1	1	1	1	1
b. Total Salary	$40,000	$40,000	$40,000	$40,000	$40,000
c. Total Benefits	$8,000	$8,000	$8,000	$8,000	$8,000
3. Support Staff (b + c below)	$54,000	$54,000	$54,000	$54,000	$54,000
a. #FTE	1	1	1	1	1
b. Total Salary	$45,000	$45,000	$45,000	$45,000	$45,000
c. Total Benefits	$9,000	$9,000	$9,000	$9,000	$9,000
4. Technical Support and Equipment	$840	$1,425	$2,320	$3,145	$4,140
5. Library	$0	$0	$0	$0	$0
6. New or Renovated Space	$0	$0	$0	$0	$0
7.Other Expenses	$5,850	$14,210	$25,370	$39,330	$56,090
TOTAL (ADD 1-7)	$448,690	$457,635	$469,690	$484,475	$502,230

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.

Capitol Technology University

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 Dean 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 Dean.
- Department Chairs and Academic Dean review the Graduating Student Survey data.
- Department Chairs and Academic Dean review student internship evaluations.
- Department Chairs and Academic Dean review grade distribution reports from the spring and summer semesters.
- Department Chairs and Academic Dean 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 Dean, 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 Dean 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 Dean attends the Student Town Hall and reviews student feedback with Department Chairs.
- Department Chairs conduct interviews with potential employers at our Career Fair.
- Post-residency, the Academic Dean meets with the faculty to review the student learning progress and discuss needed changes.

Spring Semester:

- Faculty Performance Plans are reviewed with faculty to identify divergence issues and adjust the plan as needed.
- Department Chairs and Academic Dean review grade distribution reports from the Fall Semester.
- Department Chairs and the Academic Dean review the Graduating Student Survey data.
- Department Chairs and Academic Dean review student course evaluations from the Fall Semester and the Spring Semester (in May before the Summer Semester begins).
- Department Chairs and Academic Dean 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 Dean. 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 Dean meets 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 Dean. The report may include a recommendation or a request to proceed with a committee to examine the issue further. In most cases, the changes only require the Academic Dean to inform the Vice President of Academic Affairs and University President and provide a report that includes a justification and the impact of changes and a strategic plan. Significant changes typically require the approval of the Executive Council.

Institute of World Politics

Evaluating Courses and Student (Course) Learning Outcomes

The IWP faculty conducts course assessments at the end of every semester, directly measuring student achievement of learning outcomes. Each Course Learning Outcome (CLO) for a course connects to specific student learning deliverables (e.g., quizzes, research paper, etc.) and processes (e.g., professor lecturing, crisis simulation exercise, etc.) and is graded based on rubrics. These assessments also allow professors to utilize results and reflect on their methods and approaches for successful student learning. CLOs are aligned with relevant Program Learning Outcomes (PLOs) and Institutional Learning Outcomes (ILOs) based on IWP's curriculum mapping. The annual Educational Effectiveness Assessment (EEA)

described above (section G.3.a.) includes a review of student CLO achievement based on these course assessments. It serves as a confirmation of whether our students have a sufficient command of course content.

Evaluating Faculty

The Dean of Academics uses the faculty evaluation process to confirm the appropriateness of a faculty member's expertise and performance, determining eligibility for re-hire. Each faculty member is evaluated once every two years by the Dean of Academics. The process includes four elements:

- Faculty self-evaluation
- Student evaluations of courses
- Evaluation and interview by the Dean of Academics
- Review by the Institute's President

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.**

   Capitol Technology University

   Student Learning Outcomes:

   Student learning outcomes for the proposed Joint **MS in Cyber Intelligence and Security** 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 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 retention-related issues. 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 semester, each student also meets with their Academic Advisor to evaluate their progress toward degree completion. An updated action plan 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 regularly meets with the Vice President of Academic Affairs and Academic Dean to review student retention within each degree program and address any issues that impede 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 must 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 Dean review the student evaluations for every course offered at the University. The Department Chairs and Academic Dean 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 Dean. If changes are required at the faculty level, the Department Chairs will make the changes. At the end of the following semester, appropriate stakeholders will analyze the follow-up evaluation results to determine the changes' effectiveness. 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 Dean 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 Vice President of Finance and Administration also monitors each academic program for its cost-effectiveness throughout every semester and term. 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.

IWP's annual Educational Effectiveness Assessment (EEA) and its Curriculum and Program Review Process (CPRP) described above (section G.3.a.) address the evaluation of this degree's educational effectiveness. Meanwhile, it should be noted that the U.S. Department of Education does not require retention data (nor transfer rate data) for IWP because it is a graduate school; however, the District of Columbia Higher Education Licensure Commission (DC HELC) does require retention rate data from IWP, which is included as part of its EEA.

Institute of World Politics

IWP's annual Educational Effectiveness Assessment (EEA) and its Curriculum and Program Review Process (CPRP) described above (section G.3.a.) address the evaluation of this degree's

educational effectiveness. Meanwhile, it should be noted that the U.S. Department of Education does not require retention data (nor transfer rate data) for IWP because it is a graduate school; however, the District of Columbia Higher Education Licensure Commission (DC HELC) does require retention rate data from IWP, which is included as part of its EEA.

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 **MS in Cyber Intelligence and Security.**

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

   The Institute of World Politics is accredited as a degree-granting institution by the Middle States Commission on Higher Education (MSCHE). It is licensed to operate in the District of Columbia by its Higher Education Licensure Commission (HELC). IWP is also certified by the State Council of Higher Education for Virginia (SCHEV) to operate in the Commonwealth of Virginia. Furthermore, IWP is approved to participate in the National Council for State Authorization Reciprocity Agreements (NC-SARA) for distance education.

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 Evaluating Distance Education. Capitol and IWP will continue to abide by the C-RAC guidelines with the proposed Joint **MS in Cyber Intelligence and Security.**

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 Dean, chairs, and faculty review the 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 monitoring 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

Dean monitors 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 other faculty experienced with research and publishing. The faculty teaching and chairing are the degree overlaps and will be administered in this program, although it is a Master's degree. Other appropriately credentialed faculty with multi-disciplinary 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 the use of 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 a 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 program changes, including course and program development. All faculty are selected based on domain expertise and program-related teaching experience.

When new faculty or outside consults are necessary to design 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 based on domain expertise and program-related teaching experience.

The University's online platforms offer several avenues to support instructors engaged in online learning. The Director of the 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 Dean, 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 Dean and Department Chairs. On an annual basis, the information is reported to the University's accreditation authorities, such as MSCHE and NSA/DHS.

This agreement will be administered jointly through the following Program directors' offices:

The Institute of World Politics

Jim Robbins
Dean of Academics
152 t 16th Street NW Washington, DC 20036

Capitol Technology University

William Butler
Vice President of Cyber Science Outreach and Partnerships
11301 Springfield Road
Laurel, MD 20708

CAPITOL Technology University

MEMORANDUM OF AGREEME 'T (MOU)
between
Capitol Technology University
and
The Institute of \World Politics,
A Graduate School of National Security and International Affairs
Washington, DC

THE INSTITUTE
WORLDPOLITICS

PURPOSE

To accomplish a variety of professional education goals, The Institute of World Politics (IWP) and Capitol Technology University (CTU) have agreed to create a program in Cyber Intelligence and Security. This program will provide both high-level expertise in Cyber Intelligence and Security and the technical skills required to understand cybersecurity. Students will take classes from both TWP and CTU and will, upon successful completion, earn one Master's Degree, containing the name of each Institution. Degrees of this sort are called Cooperative Degrees by the Maryland Higher Education Commission.

Given the unique academic mission of both institutions, significant gains can be realized by both parties offering their students' opportunities to develop skills and experience to work and lead in the interagency environment both domestically and overseas. The purpose of this memorandum is to describe those benefits and other specific administrative details.

To that end, Capitol Technology University (CTU) and The Institute of World Politics (!WP), both regionally accredited graduate schools, hereby enter the arrangement herein described:

ARTICULATION AGREEMENT

This memorandum will apply only to the following specified MA offered jointly by IWP and CTU, conferred by CTU, and ranges between 42 to 48 credits. Two CTU courses may be waived, per CTU's policy, to complete the joint degree in as little as 42 hours. The degree will be an MA in Cyber Intelligence and Security. All courses for the degree will be conducted online. A complete summary of qualifying criteria for the MA degree offered under this MOU is on the addendum sheet at the end of this document.

Benefits

Potential benefits for each party to this agreement are highlighted below.

1. Benefits to Capitol Technology University (CTU):
    a. Immersion into the study of Cyber Intelligence and Security and national security, statecraft, and international affairs with highest quality and experienced civilian and military educators as well as graduate students who are both recent college graduates and senior /mid-career personnel from U.S. government agencies, the Armed Forces, non-governmental organizations, private sector companies, and foreign embassies;

b. Preferred Tuition rate reductions which meet the parameters of IWP's scholarship and tuition assistance protocols.

c. Cooperative interaction between CTU and IWP in customizing the curriculum to meet the needs of individual students focused on a Cyber Intelligence and Security track;
d. Access to unique courses which fall outside the realm of traditional training, yet which hold high relevance to current and future Cyber Intelligence and Security, national security strategy leadership and management;
e. Engagement with a faculty of scholar-practitioners who are masters of a variety of critical instruments of national power;
f. An MA program in a congenial, mission-compatible, and welcoming environment for CTU students that provides knowledge, skills, and moral formation necessary for success in subsequent assignments as Cyber professionals.

2. Benefits to The Institute of World Politics:
   a. Immersion into the study of cyber security with highest quality and experienced civilian Information Technology educators and students who are both recent college graduates and senior /mid-career personnel from U.S. government agencies, the Armed Forces, non-governmental organizations, and private sector compa111es;
   b. Preferred Tuition rate reductions which meet the parameters of CTU's scholarship and tuition assistance protocols.
   c. Cooperative interaction between CTU and IWP in customizing the curriculum to meet the needs of individual students focused on a Cyber Security technical track;
   d. Access to unique courses which fall outside the realm of traditional training, yet which hold high relevance to current and future cyber security, national security strategy and Information Technology leadership, and management;
   e. Engagement with a faculty of scholar-practitioners who are masters of a variety of critical Information Technology industrial advances;
   f. An MA program in a congenial, mission-compatible, and welcoming environment for IWP students that provides knowledge and technical skills for success in subsequent assignments as Cyber professionals.

CAPITOL Technology University

THE INSTITUTE WORLDPOLITICS

MEMORANDUM OF AGREEMENT (MOU)
between
Capitol Technology University
and
The Institute of World Politics,
A Graduate School of National Security and International Affairs
\\lashington, DC

Process and Scope

1. Each semester, an acceptance committee consisting of the Chair of Cyber Security at CTU and the Chair oflntelligence at IWP will review applications and accept new students to the MA in Cyber Intelligence and Security.

2. Students are fully responsible for all fees and other requirements within the application process including application, transcripts, registration, parking, student ID orientation, or reservation fees. Both IWP and CTU agree to make timely admissions decisions that usually occur during the January-March period for fall admission and October-December time period for spring admission. Capitol as the home institution will process all students' financial aid, VA and TA. Students that enroll at IWP vvill not be invoiced directly for courses and fees. Those student invoices will be forwarded to Capitol for payment by IWP each semester. Capitol will pay those invoices directly to IWP at the end of each semester's add/drop period.

3. The period of attendance will normally enable IWP and CTU students to complete the program within a 24-month uninterrupted cycle. Students are expected to enroll in a course load that allows them to concentrate on studies to complete the program on time. Both institutions will enroll currently admitted students into the fall, spring, and summer terms.

4. The first students admitted under this memorandum are anticipated to begin the MA program in the Spring 2024 (Academic year 2024). Students are expected to meet published admissions standards, as outlined by the acceptance committee, in effect at the time of matriculation unless an exception is requested and warranted due to individual circumstances. Each Institution shall also manage its own marketing and advertising efforts for this program. However, the partner institution will review and approve all marketing materials and advertising.

5. Candidates must maintain acceptable academic performance throughout the MA program, in accordance with published policy in effect at the time of initial matriculation. Students shall be bound by the academic rules (such as grading scale and academic integrity) of the Institution whose course they are taking. In case of student misbehavior outside the classroom, IWP and CTU will coordinate their investigations and jointly determine any disciplinary action required. IWP and CTU agree to inform the other of any disciplinary action taken against dual-degree students.

6. Admitted students will have access to both Institution's student services, to include library resources, career counseling, and academic advising.

7. IWP and CTU will grant credit and confer degrees in accordance with established and published requirements for course and degree completion. A total of 42 to 48 credit hours are

required for the MA in Cyber Intelligence and Security. Each Jnstitution agrees to apply all credits earned through the successful completion of the courses specified in the addendum at the end of the document towards their respective degrees.

8. Each Institution will have the authority to grant course substitutions for its respective course components of the program. This agreement does not prevent either school from awarding its respective degree for its own coursework. (i.e. a certificate or degree)Nothing in this agreement prevents either school from awarding its respective degree for only its own coursework.

Costs

Under this MOU, IWP and CTU agree to align their tuition so the difference between tuition rates does not equal more than $50 per credit hour. At the writing of this MOU, the tuition at each Institution is nearly equal with CTU charging $630 per credit plus fees, and !WP charging $650 per credit hour plus fees. Cost adjustments not covered by this document will be negotiated at the request of either partner.

Payment Process

Students will abide by the tuition deadlines and refund policies of CTU for all courses taken in the MA in Cyber Jntelligence and Security program. As the home institution, CTU will collect fees for classes taken at CTU and IWP and will remit payment to IWP for courses taken at IWP.

Duration of Agreement

This memorandum will be in effect for twelve months, with two option years beyond initial date of signature. After successful year one "pilot," the parties may exercise option years or re-negotiate the terms of this agreement.

Program Administration

This agreement will be administered jointly through the following Program directors' offices:

The Institute of World Politics
Jim Robbins
Dean of Academics
152 t 16th Street NW
Washington, DC 20036

Capitol Technology University
William Butler
Vice President for Academic Affairs
11301 Springfield Road
Laurel, MD 20708

MEMORANDUM OF AGREEMENT (MOU)
between
Capitol Technology University
and
The Institute of World Politics,
A Graduate School of National Security and International Affairs
Washington, DC

Governing Law: This Agreement shall be construed according to and governed by the laws of District of Columbia.

Independent Status: The IWP and the CTU acknowledge and agree that each is an independent legal entity from the other with no relationship to the other outside of those obligations and commitments established in and under this Agreement. The parties agree that neither shall hold out the other as liable for any of the other's contracts, obligations, torts, or other acts or omissions, or those of the other's trustees, directors, officials, employees, agents, or

representatives. IWP and CTU acknowledge and agree that this Agreement does not create a joint venture, partnership, or any other similar legal relationship among the parties.

Agreement Initiation/Termination: This agreement becomes effective upon signature of responsible parties of both institutions Either Institution, upon written notification six months in advance of such action, may terminate the agreement. However, any student enrolled at either Institution at the time of such notice must be allowed to complete the program. Revisions, by mutual consent, may occur at any time.

SIGNATURES

CAPITOL TECHNOLOGY UNIVERSITY
BRADFORD SIMS
President
Date: 1/6/24

THE INSTITUTE OF WORLD POLITICS
CHRIS GLASS
Executive Vice President
Date: 01/21/2023

MEMORANDUM OF AGREEMENT (MOU)
between
Capitol Technology University
and
The Institute of World Politics,
A Graduate School of National Security and International Affairs
Washington, DC

THE INSTITUTE
WORLDPOLITICS

MA in Cybcr Intclligcncc and Security

Capitol Technology University and the Institute of World Politics have developed a program that will provide high-level expertise in Cyber Intelligence and Security and the technical skills required to understand cybersecurity. Under this program, students will take classes from both Capitol Technology University and the Institute of World Politics and will, upon successful completion, earn the MA in Cyber Intelligence and Security and upon the CTU conferred diploma will sit the seal and signatures of both institutions.

The curriculum consists of between 42 to 48 credits. All courses will be conducted online.
To earn these degrees, students will take the following courses:

IWPO 605 Intelligence and Policy-4 credits (online)
IWPO 610 Counterintelligence in a Democratic Society - 4 credits (online)
IWPO 627 International Relations, Statecraft, and Integrated Strategy- 4 credits (online)
IWPO 608 Sources of American Political Thought- 2 credits (online)
IWPO 699 Fundamentals of Cyber Intelligence and Security -4 credits (online)
IAE 685 Principles of Cyber Security- 3 credits (online)
IAE 671 Legal Aspects of Computer Security and Information Privacy-3 credits (online)
IAE-675 Computer Forensics and Incident Handling - 3 credits (online)
IAE-677 Malicious Software - 3 credits (online)
IAE-682 Internal Protection - 3 credits (online)
IAE-680 Perimeter Protection - 3 credits (online)
IAE-674 Security Risk Management (capstone course)- 3 credits (online)
IAE-679 Vulnerability Mitigation - 3 credits (online)

IAE 500 Introduction to Information Assurance* - 3 credits (online) (leveling course)
CS 620 Operating System Principles for Information Assurance** - 3 credits (online) (leveling course)

*Students who can demonstrate knowledge of information assurance topics at an undergraduate level through undergraduate transcripts, certifications, or work experience may have IAE500 waived with appropriate documentation evaluated at the time of admission.

**Students who can demonstrate knowledge of the UNIX operating system and C programming language may have CS620 waived with appropriate documentation which is evaluated at the time of admission.

MEMORANDUM OF AGREEMENT (MOU)
between
Capitol Technology University
and
The Institute of World Politics,
A Graduate School of National Security and International Affairs
Washington, DC

THE INSTITUTE WORLDPOLITICS

Course Transfer Table Articulation of IWP courses to CTU for completion of requirements for MA in Cyber Intelligence and Security	
Capitol Technology University (27 to 30 Credits)	Institute of World Politics (18 Credits)
For Completion of MA in C ber Intelligence and Security	
18 Credits transfer from IWP to CTU to complete the required coursework for the MA Cyber Intelligence and Security degree conferred by CTU.	IWPO 605 Intelligence and Policy - 4 credits (online) IWPO 601 National Security Policy Process -4 credits (online) IWPO 627 International Relations, Statecraft, and Integrated Strategy - 4 credits (online) IWPO 608 Sources of American Political Thought - 2 credits (online) IWPO 699 Cyber Intelligence Overview - 4 credits (online)
IAE 685 Principles of Cyber Security - 3 credits (online) IAE 671 Legal Aspects of Computer Security and Information Privacy - 3 credits (online) IAE-675 Computer Forensics and Incident Handling- 3 credits (online) IAE-677 Malicious Software - 3 credits (online) IAE-682 Internal Protection - 3 credits (online) IAE-680 Perimeter Protection - 3 credits (online) IAE-674 Security Risk Management (capstone course)- 3 credits (online) IAE-679 Vulnerability Mitigation - 3 credits (online) IAE 500 Introduction to Information Assurance* - 3 credits (online) (leveling course) CS 620 Operating System Principles for Information Assurance** - 3 credits (online) (leveling course)	

*Students who can demonstrate knowledge of information assurance topics at an undergraduate level either through undergraduate transcripts, certifications, or work experience may have IAES00 waived with appropriate documentation which is evaluated at the time of admission. **Students who can demonstrate knowledge of the UNIX operating system and C programming language may have CS620 waived with appropriate documentation which is evaluated at the time of admission.	

TRANSFER SCHOLARSHIPS

Students are eligible for additional scholarships for which they qualify as well as federal grants and loans located at https://dodstem.us/stem-programs/scholarships

DoD Cyber Scholarship Program (DoD CySP)

Given our increasing reliance on cybersecurity, information technology (IT), the growing threats to information, and information systems and infrastructures, it is critical that the Department of Defense (DoD) protect itself. To do so, the DoD must be staffed with technically savvy personnel. To help achieve this task, the DoD Cyber Scholarship Program (DoD CySP) was established. The DoD CySP is sponsored by the DoD Chief Information Office and administered by the National Security Agency (NSA). The objectives of the program are to promote higher education in all disciplines of cybersecurity, to enhance the Department's ability to recruit and retain cyber and IT specialists, to increase the number of military and civilian personnel in the DoD with this expertise, and ultimately, to enhance the nation's cyber posture.

Recruitment Scholarships (Non-DoD Employees):

As a recruitment tool, the DoD CySP sponsors students who currently are not DoD or government employees who are enrolled in or applying to universities designated as a National Center of Academic Excellence in Cybersecurity. Following graduation, students are eligible for full-time employment with various components and agencies across the DoD. Students are required to work for the DoD a minimum of one year for each year of scholarship support they receive.

Retention Scholarships (DoD Employees, Civilian and Military):

The DoD CySP supports DoD civilians, military officers, and enlisted personnel who pursue Master's and Doctoral degrees in cyber-related fields of study. Typically, these retention students attend a DoD school designated as a CAE and, depending on the program, may finish their graduate degree at a partnering university. For DoD civilian and military personnel, their sponsoring component organization determines the service commitment following graduation. Retention student also have an opportunity to pursue a two-year community college degree or certificate.

https://public.cyber.mil/wid/cdp/dcysp/

DoD SMART Scholarship-for-Service Program

The Science, Mathematics and Research for Transformation (SMART) Scholarship for Service Program has been established by the Department of Defense (DOD) to support undergraduate and graduate students pursuing technical degrees in Science, Technology, Engineering and Mathematics (STEM) disciplines. The program aims to increase the number of civilian scientists and engineers working at DOD facilities. Military Branch or Component: All Services.
https://www.smartscholarship.org/smart

97219 **VENDOR** NO. 17911 DATE 9/19/2024 CHECK NO. 97219

CAPITOL TECHNOLOGY UNIVERSITY

INVOICE NUMBER	INVOICE DATE	DESCRIPTION	GROSS AMOUNT	DISCOUNT/ADJUSTMENTS	PAYMENT AMOUNT
9/16/2024	09/16/2024	Degree Propoaal Cyber Intelligerl e	850.00	0.00	850.00
			850,00	0,00	850.00

ORIGINAL CHECK HAS A COLORED BACKGROUND PRINTED ON CHEMICAL REACTIVE PAPER SEE BACK FOR DETAILS

97219

HOWARD BANK

,1P,!!9,1

ELLICOTT CITY, MD 21043
65-3431550

DATE 9/19/2024

CHECK AMOUNT

$ *********850.00

11301 SPRINGFIELD ROAD, LAUREL, MD 20708
PH: 301--369,-2800

PAV EIGHT HUNDRED FIFTY AND N0/100 DOLLARS

TO THE **ORDER** *OF*
Maryland Higher Education Comission
6 N. Liberty St
Baltimore, MD 21201

CAPITOL TECHNOLOGY UNIVERSITY

£4...;., a dAl

u•oCJ? 21,CJu• 1:0 5 500 ll, **31,1:** 0 10 **lo lo** 21::,i;u•