New Program Proposal

Bachelor of Arts in Cyber Threat Intelligence [CIP Code: 43.0404]

Coastal Carolina University [Site Code: 51001]

A. SUMMARY

Coastal Carolina University proposes a new Cyber Threat Intelligence Bachelor of Arts (BA) program to prepare students for careers and further study in the cyber domain that involve the analysis and evaluation of system vulnerabilities and the malicious actors that seek to exploit these vulnerabilities. Using an interdisciplinary approach, this innovative major synthesizes the technical and non-technical concepts in the field of cybersecurity and applies knowledge and skills from the fields of intelligence analysis and security studies.

Students will have career opportunities in a career field that has a growing workforce need which continues to outstrip supply. The U.S. Bureau of Labor Statistics (BLS) projects that employment in information security will grow 35 percent from 2021 to 2031, much faster than the average for all occupations. Another source indicated that the job vacancies in cybersecurity grew by 350 percent between 2013 and 2021 and that the year-over-year disparity between demand and supply will continue to grow through at least 2025.[1] As cyber threats grow in frequency and complexity, the need for programs that integrate cybersecurity and intelligence capabilities is both critical and inevitable.

The proposed BA Cyber Threat Intelligence degree requires 120 credit hours. Core curriculum requirements are 36-40 credit hours. Program requirements are 44-56 credit hours. Cognate is 9 credit hours; electives are 9-28 credit hours. The program will be offered face to face to begin Fall 2024.

New courses:

INTEL 318 (3 Credits) (Prereq: INTEL 200 or permission of the instructor) – Open-Source Intelligence Collection. This course explores the topic of open-source intelligence (OSINT) in a social, cultural, political, and legal context. It introduces students to the history of OSINT as a field, its development and relevance to intelligence. Essential components of the course include what sources of intelligence collection exist, and how to identify, understand, use, and analyze the intelligence collected from them. Special attention is given to various specific sources of OSINT and the preparation of students to build logical, concise, and informative OSINT briefs, reports, and scholarly materials.

INTEL 345 (3 Credits) – Cybersecurity Strategy and Governance. This course explores cybersecurity strategy and governance. It introduces students to the essential elements of strategy development and governance issues in cybersecurity. The second part of the course explores various topics important for the development of cybersecurity strategy and governance. Special attention is paid to the connections between cybersecurity policies, businesses, and governmental institutions, the social, political, and ethical implications that arise in cybersecurity policies, strategies to assess cybersecurity policy, and the interaction between national security and cybersecurity policy.

INTEL 350 (3 Credits) (Prereq: INTEL 200 and CSCI 101 or permission of the instructor) – Understanding Cyber Threat Actors. This course provides an in-depth exploration of cyber threat actors, their motivations, techniques, and impact on cybersecurity. Through a multidisciplinary approach, students will analyze real-world case studies, engage with the writings of industry experts, and develop a comprehensive understanding of the evolving landscape of cyber threats. The course will cover various threat actor profiles, their tactics, techniques, and procedures, and strategies for defending against them.

INTEL 351 (3 Credits) (Prereq: INTEL 200 or permission of the instructor) – Emerging Technologies in Intelligence and Security. This class examines the role of new technological innovation on the processes and policies of intelligence and security. Beyond an in-depth exploration of several contemporary emerging technologies, the course will also consider the

theories of technological change and historical case studies relating to the integration of new technologies in intelligence and security affairs.

REACH Act Compliance:

As part of their graduation requirements, all students at CCU must complete either *HIST 201 - History of the United States from Discovery to the Present: Discovery through Reconstruction*, or *POLI 201 - Introduction to American Government*, which are both REACH Act compliant.

B. UNIVERSITY STUDENT AND PROGRAM DATA, Semester Year

Undergraduate: in-state (45%) /out-of-State (55%) Enrollment, Fall 2023

*Source Provisional Fall 2023 Enrollment Data

C. INSTITUTIONAL APPROVALS AND DATES OF APPROVAL (include department through Provost/Chief Academic Officer, President, and Board of Trustees approval):

Internal Institutional Unit	Approval Date	Internal Institutional Unit	Approval Date
Department of Intelligence and Security Studies:	09/12/2023	Faculty Senate:	11/03/2023
Board of Trustees:	10/27/2023	Provost:	11/14/2023
College Curriculum Comm.:	9/26/2023	President:	11/14/2023
Academic Affairs:	10/10/2023		

D. SIMILAR PROGRAMS IN SOUTH CAROLINA – PUBLIC AND PRIVATE INSTITUTIONS

Program Name and Designation	Total Credit Hours	Institution	Similarities	Differences
BS, Cyber Intelligence	120	University of South Carolina	Interdisciplinary approach that blends technical and non-technical aspects of cyber.	Less extensive coverage of intelligence process to cyber-related threats.
BS, Cyber Policy and Ethics	121	University of South Carolina	Interdisciplinary approach that blends technical and non-technical aspects of cyber.	No coverage of intelligence process to cyber-related threats.
BA, Intelligence and Security Studies	120	The Citadel	Coverage of intelligence process in the security domain.	Cyber is not the focus of the program. Minimal coverage of cybersecurity issues.
BS, Cyber Operations	123	The Citadel	Coverage on technical elements of cybersecurity.	No coverage of social elements of cybersecurity or intelligence threat assessment.
BS, Cybersecurity	120	USC-Upstate	Coverage on technical elements of cybersecurity	No coverage of social elements of cybersecurity or intelligence threat assessment.
B.S., Applied Computer Science with concentration in Cybersecurity	120	USC-Aiken	Coverage on technical elements of cybersecurity	No coverage of social elements of cybersecurity or intelligence threat assessment.

BS, Cybersecurity	120	Lander University	Coverage on technical elements of cybersecurity	No coverage of social elements of cybersecurity or intelligence threat assessment.
BS, Cybersecurity and Criminal Justice	123	Anderson University	Coverage on technical and social elements of cybersecurity	Coverage confined to criminal justice area with no coverage of intelligence threat assessment.
BS, Cybersecurity	128	Benedict College	Coverage on technical elements of cybersecurity	No coverage of social elements of cybersecurity or intelligence threat assessment.
BS, Computer Science with concentration in Cybersecurity	120	South Carolina State University	Coverage on technical elements of cybersecurity	No coverage of social elements of cybersecurity or intelligence threat assessment.

E. ENROLLMENT PROJECTIONS

Projected Enrollment			
Year	Fall Headcount	Spring Headcount	Summer Headcount
	Total	Total	Total
2024-2025	10	19	0
2025-2026	27	34	0
2026-2027	40	46	0
2027-2028	51	55	0
2028-2029	55	55	0

The table is based on enrollment of 10 new students each fall and 10 new students each spring. Years one through four total headcounts based on 90% returning fall to spring and 90% returning spring to fall. Year five headcount additionally based on 40% graduation rate of returning students.

F. INDUSTRY-RELATED OCCUPATIONAL WAGES AND PROJECTIONS IN SOUTH CAROLINA

Occupation	State		National		Data Type and Source
	Expected Number of Jobs	Employment Projection	Expected Number of Jobs	Employment Projection	
Information Security Analysts	195	31% (Annually)	168,900	32% (2022-32)	SC Works; US Bureau of Labor Statistics
Intelligence Analysts	127	13% (Annually)	808,200	3% (2022-32)	SC Works; US Bureau of Labor Statistics
Network and Computer Systems Administrators	461	14% (Annually)	339,900	2% (2022-32)	SC Works; US Bureau of Labor Statistics
Computer Systems Analyst	752	14% (Annually)	531,400	10% (2022-32)	SC Works; US Bureau of Labor Statistics
Security Management Specialist	10,370	13% (Annually)	NA	NA	SC Works
Security Manager	10,568	14% (Annually)	NA	NA	SC Works

The demand for cyber-related personnel outstrips the available supply on multiple levels. The website Cyberseek indicates that currently South Carolina is only filling 73 percent of its available cyber-related job positions. There are nearly 7,000 unfilled cyber positions in the state and the ratio of unfilled positions to filled positions has been consistently growing since 2011. What is more, this gap in cyber-related talent exists across the country with 663,434 positions unfilled. This equates to nearly a third of all cybersecurity-related positions that exist in the United States.[29]

The regional need for cyber-related professionals is also significant. The Community Profile for Horry County projects a growth for information-related positions of nearly 26 percent between 2020 and 2030.[30] The recent establishment of DC Blox makes Myrtle Beach one of the few areas on the east coast with a subsea cable landing station and suggests that cyber-related occupations are likely to grow in the grand strand area.[31] Additionally, there are a range of companies in manufacturing, healthcare, and finance that will benefit from the graduates and potential collaborations from this program. Median salaries for personnel in these roles in South Carolina (for 2022) range from $52,470 to $112,000 annually, well above the average for Horry County.[32]

G. CHE STAFF STAGES OF CONSIDERATION

Considerations	Date	Comments
Program proposal received	1.11.2024	Original Proposal received via email. Assigned lead reviewer and second reader
Summary of staff comments, responses, and versions	1.30.2024	One revision request included: • Need for a new degree/duplication. • Workforce Demand • Student Demand

		• Internships • Institutional Assessment
ACAP Considerations	3/28/2024	ACAP questions: None Responses: None Vote: Approved
CAAL Considerations (See attached commissioner questions and responses)		CAAL questions Responses Vote
CHE Considerations		CHE questions Responses Vote
Submission to IT for addition to inventory		Date completed

H. STAFF, ACAP, CAAL AND CHE RECOMMENDATIONS

a. STAFF RECOMMENDED ACTION

Recommended

b. ACAP RECOMMENDATION

Approved

c. CAAL RECOMMENDATION

Choose an item.

d. CHE RECOMMENDATION

Choose an item.

Additional Comments:

Meeting: CAAL Meeting
Meeting Date: May 9, 2024
Agenda Item: 5F

NEW PROGRAM PROPOSAL FORM

Name of Institution: Coastal Carolina University

Name of Program (include degree designation and all concentrations, options, or tracks):

Bachelor of Arts in Cyber Threat Intelligence

Program Designation:

- ☐ Associate's Degree
- ☐ Master's Degree
- ☒ Bachelor's Degree: 4 Year
- ☐ Specialist
- ☐ Bachelor's Degree: 5 Year
- ☐ Doctoral Degree: Research/Scholarship (e.g., Ph.D. and DMA)
- ☐ Doctoral Degree: Professional Practice (e.g., Ed.D., D.N.P., J.D., Pharm.D., and M.D.)

Consider the program for supplemental Palmetto Fellows and LIFE Scholarship awards?

- ☐ Yes
- ☒ No

Proposed Date of Implementation: Fall 2024

CIP Code: 43.0404 [Cybersecurity Defense Strategy/Policy]

Delivery Site(s): 51001

Delivery Mode:

- ☒ Traditional/face-to-face
  *select if less than 25% online
- ☐ Distance Education
  - ☐ 100% online
  - ☐ Blended/hybrid (50% or more online)
  - ☐ Blended/hybrid (25-49% online)
  - ☐ Other distance education (explain if selected)

REACH Act Compliance: As part of their graduation requirements, all students must complete either *HIST 201* or *POLI 201*, which are both REACH Act compliant. Sample syllabi are available upon request.

Program Contact Information (name, title, telephone number, and email address):

Dr. Jonathan Smith, Chairman, Department of Intelligence and Security Studies
Office Phone: (843) 349-6573
E-Mail: jonsmith@coastal.edu

Meeting: CAAL Meeting
Meeting Date: May 9, 2024
Agenda Item: 5F

Institutional Approvals and Dates of Approval (include department through Provost/Chief Academic Officer, President, and Board of Trustees approval):

Internal Institutional Unit	Approval Date	Internal Institutional Unit	Approval Date
Department of Intelligence and Security Studies:	09/12/2023	Faculty Senate:	11/03/2023
Board of Trustees:	10/27/2023	Provost:	11/14/2023
College Curriculum Comm.:	9/26/2023	President:	11/14/2023
Academic Affairs:	10/10/2023		

Background Information

State the nature and purpose of the proposed program, including target audience, centrality to institutional mission, and relation to the strategic plan.

The Cyber Threat Intelligence degree will prepare students for careers and further study in the cyber domain that involve the analysis and evaluation of system vulnerabilities and the malicious actors that seek to exploit these vulnerabilities. Using an interdisciplinary approach, this innovative major synthesizes the technical and non-technical concepts in the field of cybersecurity and applies knowledge and skills from the fields of intelligence analysis and security studies.

The need for such a program, both in South Carolina and nationally, is uncontestable. The number of people and devices that rely on the internet continues to grow exponentially. For instance, from 2022 to 2027 the number of Internet of Things (IoT) devices will double to more than 29 billion devices. [1] As computer networked technologies continue to penetrate nearly all facets of human interaction, the vulnerability of these networks poses an increasingly grave security threat for the activities of the private-sector, government, and society. Indeed, the rising threat in conjunction with the challenges of recruiting cyber workers is so dire that the White House recently established the National Cyber Workforce and Education Strategy (NCWES) to address both the immediate and long-term needs in this area.[2]

As this attack surface grows, the threat of malevolent cyber threat actors continues to be a pervasive and significant challenge. The United States Office of the Director of National Intelligence notes that "State and non-state actors use digital technologies to achieve economic and military advantage, foment instability, increase control over content in cyberspace and achieve other strategic goals — often faster than our ability to understand the security implications and neutralize the threat."[3] Indeed, in 2019, the National Intelligence Strategy for the United States identified Cyber Threat Intelligence as one of seven mission objectives for the U.S. Intelligence Community. It is a security challenge that cuts across all levels of government, industry, and civil society.

Now, with the growing role of emerging technologies such as artificial intelligence, the need for security professionals who are knowledgeable regarding this domain has never been stronger. That said, defense against threats to the cyber-domain is far from a purely technical concept. According to the Gartner consulting firm, by 2025

[1] IOT Analytics. "State of IoT 2023: Number of Connected IoT devices growing 16% to 16.7 billion globally." https://iot-analytics.com/number-connected-iot-devices/#IoT%20Connections%20Forecast.
[2] https://www.forbes.com/sites/forbeshumanresourcescouncil/2023/10/16/the-quest-to-close-the-cybersecurity-talent-gap/?sh=703fc702349e
[3] Office of the Director of National Intelligence, Cyber Security. https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-cyber-security. Accessed on 25 July 2023.

approximately half of all significant cyber breaches will be caused by human factors.[4] Embracing a holistic concept of cyber-space, which denotes the convergence of networked computer hardware, digital data, and the 'end point users' (humans) that manage or utilize them, is essential for the workforce of the future. In order for security entities to meet this challenge and not be merely reactive, they must integrate knowledge and skillsets from cyber security with the field of intelligence to effectively mitigate, prevent, or quickly respond to these threats.

To that end, Cyber Threat Intelligence is defined as the collection, processing, analysis, and dissemination of information from all sources of intelligence on foreign actors' cyber programs, intentions, capabilities, research and development, tactics, targets, operational activities and indicators, and their impact or potential effects on [the vital interests and functions of an organization]. Cyber threat intelligence also includes information on cyber threat actor information systems, infrastructure, and data; and network characterization, or insight into the components, structures, use, and vulnerabilities of foreign cyber program information systems.[5] Its primary purpose is to enhance cybersecurity efforts by developing a knowledge advantage over cyber threat actors. This skillset has wide applicability in the cyber domain according to the Center for Internet Security. They note that cyber threat intelligence has proved beneficial at every level of government, from senior executives and Chief Information Security Officers to information technology specialists and law enforcement.[6]

The synthetization of cybersecurity and intelligence provides a critical benefit. As a senior official at Horizon3 AI noted, "the technical/soft skills combination is often what companies need to foster continuous strengthening of their cybersecurity posture."[7] Since one of the primary functions of intelligence professionals is to support decision advantage by leaders of organizations, the blended focus on cybersecurity and intelligence allows these new professionals to serve as effective translators for the technical language of IT professionals to policymakers and the boardroom. This function can also be of service in the opposite direction in communicating conceptual and policy information to the technical experts who manage the systems and infrastructure. In this way, cyber threat intelligence professionals serve as conceptual mediators across the security enterprise.[8]

The addition of a Cyber Threat Intelligence major at Coastal Carolina University is highly consistent with the mission of the institution. It clearly supports the university's goal of being a "public comprehensive liberal arts institution that seeks to develop students who are both knowledgeable in their chosen fields and prepared to be productive, responsible, healthy citizens with a global perspective". Also, the addition of such a specialized program can only assist with the strategic planning objectives to provide innovative curricular and co-curricular pathways to improve graduation outcomes and post-college success and ensure contemporary academic offerings grounded in liberal arts.[9]

Assessment of Need

Provide an assessment of the need for the program for the institution, the state, the region, and beyond, if applicable.

---

[4] https://www.gartner.com/en/newsroom/press-releases/2023-02-22-gartner-predicts-nearly-half-of-cybersecurity-leaders-will-change-jobs-by-2025

[5] Office of the Director of National Intelligence. National Intelligence Strategy, 2019: 11. https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf

[6] Intel & Analysis Working Group. "What is Cyber Theat Intelligence?", Center for Internet Security. https://www.cisecurity.org/insights/blog/what-is-cyber-threat-intelligence. Accessed on 15 September 2023.

[7] Sue Porema, "The cybersecurity talent shortage: The outlook for 2023," Cybersecurity Drive (5 January 2023). https://www.cybersecuritydive.com/news/cybersecurity-talent-gap-worker-shortage/639724/

[8] Stephen McCombie, et. al. "The Elusive Field of Cyber Intelligence: Notes from the Educational Front", *Journal of the AIPIO*, Vol. 27 (No. 2), 2019, 31.

[9] https://www.coastal.edu/aboutccu/leadership/strategicplan/

Overall Need

The need for more cybersecurity professionals – and cybersecurity professionals who can analyze both sides of the technical and behavioral divide – has never been more acute. This is due to both an increased need from industry and government, but also the challenges in developing the workforce. The demand for professionals in this field continues to outstrip supply. The U.S. Bureau of Labor Statistics (BLS) projects that employment in information security will grow 35 percent from 2021 to 2031, much faster than the average for all occupations. Another source indicated that the job vacancies in cybersecurity grew by 350 percent between 2013 and 2021 and that the year-over-year disparity between demand and supply will continue to grow through at least 2025.[10] A study by (ISC)² found that 56 percent of businesses say the cybersecurity talent shortage is putting them at risk.[11] This program will attract more qualified professionals into the field, but also equip them to address these concerns from a larger perspective. As cyber threats grow in frequency and complexity, the need for programs that integrate cybersecurity and intelligence capabilities is both critical and inevitable.[12]

Government Demand

The unparallelled growth of the cyber threat intelligence in our time has been fueled by the proliferation of increasingly sophisticated attacks by malicious cyber actors[13], coupled with the expansion of the attack surface through the rise of cloud computing and the hybrid work environment.[14] The growing demand for cyber threat intelligence professionals in the national security space became evident in February 2015, when the White House established the Cyber Threat Intelligence Integration Center (CTIIC).[15] Aside from marking a significant step toward fortifying the nation's cybersecurity defenses, the establishment of the CTIIC helped spur the unparalleled growth of CTI professionalization across the U.S. government sector. As a national intelligence center dedicated to "connecting the dots"[16] on malicious foreign cyber threats and incidents affecting U.S. national interests, the CTIIC's culture of combining intelligence processes with deep knowledge about cyber threats became infused across the U.S. government.[17]

Today, the leading cyber security agencies of the United States government are undergoing a hiring boom that is unprecedented in the post-9/11 era. In FY2023 alone, the National Security Agency (NSA) advertised for 3,000 new employees in the field of cyber security —something that, in the past, would have satisfied its hiring needs for several years. Yet the NSA is advertising for another 3,000 positions in FY2024, which has never happened before.[18] For the past decade, demand for cyber threat intelligence jobs in the government sector has paralleled, and at times

---

[10] Steven Morgan, "Cybersecurity Jobs Report: 3.5 Million Unfilled Positions in 2025". *Cybersecurity Magazine* (14 April 2023). Https://cybersecurityventures.com/jobs/. Accessed on 5 September 2023.

[11] Security Intelligence. "The Uncertainty of Cybersecurity Hiring'> https://securityintelligence.com/articles/whats-going-on-with-cybersecurity-hiring/.

[12] McCombie, et. al., 22.

[13] Kevin Popireault (2023) "Cyber-Attacks Targeting Government Agencies Increase 40%", *InfoSecuity Magazine*, 03 August. https://www.infosecurity-magazine.com/news/cyberattacks-government-agencies/.

[14] Alexandra Borgeaud (2024) "Cyber Threat Intelligence (CTI) Statistics and Facts", *Statista*, 10 January https://www.statista.com/topics/10666/cyber-threat-intelligence-cti/.

[15] Barack Obama (2015) "Memorandum on Establishment of the Cyber Threat Intelligence Integration Center", United States Federal Register, Washington, DC, 02 March.

[16] Office of the Press Secretary (2015) "Fact Sheet: Cyber Threat Intelligence Integration Center", The White House, Washington, DC, 25 February.

[17] Jon Lindsay and Erik Gartzke (2019) "Cybersecurity and Cross-Domain Deterrence: The Consequences of Complexity", in Damiel Van Puyvelde and Aaron F. Brantly (eds.) *US National Cybersecurity: International Politics, Concepts and Organization*, Routledge, New York, NY.

[18] Jillian Hamilton (2023) "NSA Hiring Goals for 2024 Continue Agency's Aggressive Talent Push", ClearanceJobs, 25 August.

exceeded, demand in the private sector.[19] Should that trend continue, then demand for cyber threat intelligence professionals in the government sector should be expected to double between 2024 and 2028.[20]

Private Sector Demand

The market for private sector demand for cyber threat intelligence services was valued at $11.6 billion in 2023 and is expected to grow at a compound annual growth rate of 20.4 percent to reach $18.11 billion by 2030.[21] This growth is reflected in a diverse array of businesses including banks, insurance companies, consulting agencies, health care organizations, software companies, and internet providers.[22]

Some of the specific companies hiring cyber threat analysts include Microsoft, CACI, Deloitte, M&T Bank, Citi, Blue Cross and Blue Shield, Bank of America, JPMorgan Chase & Co., PayPal, and others (Indeed.com, 2024). The majority of these positions, approximately 82 percent, offer starting salaries of $90,000. These positions can be particularly appealing, as the average annual salary is $104,031 – 20 percent more than the average annual salary of a general intelligence analyst ($83,640 per year), which itself has a growth rate of 5 percent itself, according to CareerExplorer. A similar career path of graduates form the Cyber Threat Intelligence major is becoming an open-source intelligence analyst with salaries averaging $73,261/year and with potential employers including Leyden Solutions Inc, Booz Allen Hamilton, TEKsystems, BTS, BAE Systems, CACI and others (ZipRecruiter, 2024).

At a state and local level, the value of this program is manifest. The South Carolina Chapter of Infragard, a public private partnership with the Federal Bureau of Investigation (FBI) that represents most of the critical infrastructure elements in the state, has drafted a letter of support for this initiative. Letters of support from Conway Medical Center, HTC, Inc., and Santee Cooper are also attached; see Appendix A.

Program Availability

Programs in Cyber Threat Intelligence are both markedly rare and highly sought after. As of 2024, there are fewer than ten undergraduate programs in this area across the United States. However, the need to integrate these areas has been recognized for some time. Carnegie Mellon University found that, "The cyber intelligence workforce is a heterogeneous mix of technical and non-technical intelligence analysts, neither completely familiar with the nuances and complexities of the other half."[23] The need for developing these skills is pervasive. A 2020 study by the Enterprise Strategy Group found that 71 percent of organizations that use cyber threat intelligence (CTI) experienced improved incident response.[24]

---

[19] Sasha Romanosky, Karen Schwindt and Ryan Johnson (2003) Comparison of Public and Private Sector Cybersecurity and IT Workforces, RAND, National Security Research Division, Santa Monica, CA.

[20] Alexandra Borgeaud (2024) "Global Cyber Threat Intelligence (CTI) Market Size 2023-2033", *Statista*, 12 February. https://www.statista.com/statistics/1230328/cyber-threat-intelligence-market-size-global/.

[21] Cyber threat intelligence (CTI) market size worldwide from 2023 to 2033 (in billion U.S. dollars), *Statista*. https://www.statista.com/statistics/1230328/cyber-threat-intelligence-market-size-global/#:~:text=Global%20cyber%20threat%20intelligence%20(CTI)%20market%20size%202023%2D2033&text=In%202023%2C%20the%20global%20cyber,to%20the%20evolving%20threat%20landscape. Accessed on 13 September 2023.

[22] Michelle Moore, "Cyber Threat Intelligence Analyst: Salary and Career Guide", University of San Diego. https://onlinedegrees.sandiego.edu/cyber-threat-intelligence-analyst/. Accessed on 12 September 2023.

[23] M. Ludwick, et. al. Cyber Intelligence Tradecraft Project. Software Engineering Institute, Carnegie Mellon University, 2013.

[24] Ed Cabrera, "Cyber Threat Intelligence: The Power of Data", *Trend Micro* (20 April 2023). https://www.trendmicro.com/en_us/ciso/23/d/cyber-threat-intelligence.html#:~:text=A%202020%20study%20by%20the,intelligence%20experienced%20improved%20incident%20response.&text=Many%20organizations%20rely%20on%20third,can%20introduce%20additional%20cyber%20risks.

Coastal Carolina University is uniquely positioned because, in addition to having an ABET-accredited Computing Sciences department, it also has one of the strongest intelligence studies programs in the country. These two departments reflect both the technical and social/behavioral aspects of cybersecurity, as well as a strong emphasis on intelligence threat analysis. The development of this program was recognized in February 2024 with the Dr. Charles Wyatt Award for Excellence in Academics by CyberSC and the South Carolina Cyber Foundation professional associations.

Currently, there are no cyber-related undergraduate majors at CCU. The only curricular program at the undergraduate level is a minor in cybersecurity offered by the Department of Computing Sciences. Given the growing need for cyber threat intelligence professionals, in conjunction with the limited number of academic programs that focus on this area of expertise, the program will likely attract new students to Coastal Carolina University to pursue this course of study. The U.S. Bureau of Labor Statistics projects that 'information security analysts' will be one of the 20 most in-demand jobs over the next decade (2018-2028).[25] Indeed, in the *South Carolina Cyber Ecosystem Coordination Initiative* presentation that was delivered by Simon Everet Consulting to the SC Commission on Higher Education in June 2023, identified this as the largest area of growth in South Carolina.[26]

There are also currently no other Cyber Threat Intelligence programs in the state of South Carolina. The closest curriculum would be the Cyber Intelligence B.S. degree at the University of South Carolina. This program is similar in as much as it also attempts to fuse the technical and non-technical factors in the cyber domain. That said, the proposed program at Coastal Carolina University has a much more substantial focus on the role of intelligence processes that can be leveraged to improve the security of organizations within the cyber domain. The program at USC is also being phased out in lieu of a new undergraduate program in Cyber Policy and Ethics.[27]

Student Demand

Student interest for this program is already quite strong at Coastal Carolina University and expected to grow. In a Fall 2023 survey of students, more than 80 percent of the respondents (n=115) indicated that they would definitely or probably enroll in the Cyber Threat Intelligence major if it was offered at Coastal Carolina University. A further 10 percent would consider enrolling in the new major if they had additional information.[28]

Transfer and Articulation

Coastal Carolina University has an ongoing effort to build a pipeline of students from Horry Georgetown Technical College (HGTC). Because there are no specialized requirements for entry into this new major program, it is assumed some students will come to the program from HGTC, as well as other technical colleges. Given the role of the core curriculum requirement for Coastal Carolina University, students pursuing associate of arts or associate of science programs at 2-year institutions should not be delayed in completing the program on a 4-year schedule.

In 2022, the Intelligence and Security Studies department created a 2+2 pipeline with the associate of applied science degree program for cybersecurity at HGTC. An attempt to develop a similar agreement for the cyber threat

[25] The 20 Most In-demand Jobs Over the Next Decade, Affordable Schools. https://affordableschools.net/faq/in-demand- jobs-over-next-decade/. Accessed on 9 September 2023.
[26] Simon Everet Consulting. *South Carolina Cyber Ecosystem Coordination Initiative.* Presentation delivered to the South Carolina Commission on Higher Education, 8 June 2023, Slide 9.
[27] University of South Carolina. New Program Proposal: Bachelor of Science in Cyber Policy and Ethics. Submission to Committee on Academic Affairs and Licensing, South Carolina Commission of Higher Education (11 May 2023), p. 3. https://che.sc.gov/sites/che/files/Documents/Meetings/Meetings%202023/CAAL/CAAL%20May%2011/7W_USCC%20BS%20Cyber%20Policy%20and%20Ethics.pdf
[28] CCU Cyber Threat Intelligence Interest Survey Fall 2023.

intelligence major will be initiated, both with HGTC and other technical colleges in the state, after the start of the new major. See page 13 for a curriculum map for a transfer student with a 2-year degree. Additionally, recent initiatives developed between HGTC and local high schools to create a new pathways program, combined with our relationship with HGTC, will foster a growing cybersecurity education ecosystem in Horry County.

Employment Opportunities

Provide supporting evidence of anticipated employment opportunities for graduates.

Occupation	State		National		Data Type and Source
	Expected Number of Jobs	Employment Projection	Expected Number of Jobs	Employment Projection	
Information Security Analysts	195	31% (Annually)	168,900	32% (2022-32)	SC Works; US Bureau of Labor Statistics
Intelligence Analysts	127	13% (Annually)	808,200	3% (2022-32)	SC Works; US Bureau of Labor Statistics
Network and Computer Systems Administrators	461	14% (Annually)	339,900	2% (2022-32)	SC Works; US Bureau of Labor Statistics
Computer Systems Analyst	752	14% (Annually)	531,400	10% (2022-32)	SC Works; US Bureau of Labor Statistics
Security Management Specialist	10,370	13% (Annually)	NA	NA	SC Works
Security Manager	10,568	14% (Annually)	NA	NA	SC Works

The demand for cyber-related personnel outstrips the available supply on multiple levels. The website Cyberseek indicates that currently South Carolina is only filling 73 percent of its available cyber-related job positions. There are nearly 7,000 unfilled cyber positions in the state and the ratio of unfilled positions to filled positions has been consistently growing since 2011. What is more, this gap in cyber-related talent exists across the country with 663,434 positions unfilled. This equates to nearly a third of all cybersecurity-related positions that exist in the United States. [29]

[29] Cyber Seek. Cybersecurity Supply/Demand Heat Map. Https://www.cyberseek.org/heatmap.html. Accessed on 14 September 2023.

The regional need for cyber-related professionals is also significant. The Community Profile for Horry County projects a growth for information-related positions of nearly 26 percent between 2020 and 2030.[30] The recent establishment of DC Blox makes Myrtle Beach one of the few areas on the east coast with a subsea cable landing station and suggests that cyber-related occupations are likely to grow in the grand strand area.[31] Additionally, there are a range of companies in manufacturing, healthcare, and finance that will benefit from the graduates and potential collaborations from this program. Median salaries for personnel in these roles in South Carolina (for 2022) range from $52,470 to $112,000 annually, well above the average for Horry County.[32]

Description of the Program

Projected Enrollment			
	Fall Headcount	Spring Headcount	Summer Headcount
Year	Total	Total	Total
2024-2025	10	19	0
2025-2026	27	34	0
2026-2027	40	46	0
2027-2028	51	55	0
2028-2029	55	55	0

The table is based on enrollment of 10 new students each fall and 10 new students each spring. Years one through four total headcounts based on 90% returning fall to spring and 90% returning spring to fall. Year five headcount additionally based on 40% graduation rate of returning students.

Besides the general institutional admission requirements, are there any separate or additional admission requirements for the proposed program? If yes, explain.

☐ Yes

☒ No

Curriculum

In order to ensure that this curriculum is consistent with current standards in the field, it was developed utilizing the whitepaper "Cyber Threat Intelligence Analysts Core Competencies Framework" produced by Mandiant Corporation, as well as the Office of the Director of National Intelligence whitepaper "Key Challenges in Cyber Threat Intelligence".[33] See Appendix B for full catalog description.

Cyber Threat Intelligence, B.A. (120 credits)	

[30] Community Profile: Horry County, S.C. Department of Employment and Workforce, Business Intelligence Department. https://lmi.dew.sc.gov/lmi%20site/Documents/CommunityProfiles/04000051.pdf. Accessed on 10 September 2023.
[31] Richard Caines, "How the Myrtle Beach Area could become an internet hub both globally and in SC", *The Post and Courier* 14 June 2023.
[32] https://www.onetonline.org/
[33] See "Cyber Threat Intelligence Analysts Core Competencies Framework", Mandiant Corporation (2022). https://www.mandiant.com/sites/default/files/2022-05/cti-analyst-core-competencies-framework-v1.pdf. Accessed on 3 August 2023.

I. CORE CURRICULUM (36-40 credits)	**36-40**
II. GRADUATION REQUIREMENT (3-6+ credits)	**3-6**
UNIV 110 The First-Year Experience	3
HIST 201 or POLI 201†	3
III. PROGRAM REQUIREMENTS (44/56 credits)	
A) Foundation Courses	**6-17**
• Complete the following courses:	9
• INTEL 200 Introduction to Intelligence and National Security Studies	3
• INTEL 250 Introduction to Security Studies	3
• CSCI 101 Introduction to the Internet and the World Wide Web*	0-3
• Select one of the following courses:	0-4
• PHYS 104/L Science for Security* or SCIE 101/L Introduction to Science*	0-4
• Select one of the following courses:	0-3/4
• STAT 201/L Elementary Statistics* or POLI 205 Introductory Statistics for the Political and Social Sciences*	0-3/4
B) Computing Sciences Core Courses	
• Complete the following courses:	**9**
• CSCI 216 Linux Fundamentals 1	3
• CSCI 270 Data Communications Systems and Networks	3
• CSCI 385 Introduction to Information Systems Security	3
C) Computing Sciences Elective Courses	
• Choose two upper-division courses from a rotation of current offerings.	**6**
• CSCI 316 Linux Fundamentals II	3
• CSCI 386 Offensive Security	3
• CSCI 416 Linux Systems Administration	3
• CSCI 434 Digital Forensics	3
• CSCI 435 Anti-Forensics and Digital Privacy	3
D) Intelligence and Security Studies Core Courses	
• Complete the following courses:	**18**
• INTEL 309 Data Analytics in Intelligence and Security	3
• INTEL 310 Intelligence Analysis	3
• INTEL 345 Cybersecurity Strategy and Governance**	3
• INTEL 350 Understanding Cyber Threat Actors**	3
• INTEL 351 Emerging Technologies in Intelligence and Security**	3
• INTEL 410 Cyber Threat Intelligence	3

E) Intelligence and Security Studies Major Elective Courses	
• Choose two upper-division courses from a rotation of current offerings.	**6**
• INTEL 311 Intelligence Communications	3
• INTEL 312 Intelligence Operations	3
• INTEL 313 Covert Action and Grey Zone Conflict	3
• INTEL 315 Human Intelligence	3
• INTEL 318 Open-Source Intelligence Collection**	3
• INTEL 335 Homeland Security	3
• INTEL 340 National Security Strategy	3
• INTEL 341 Intelligence and War	3
• INTEL 343 Terrorism and Political Violence	3
• INTEL 344 Weapons of Mass Destruction	3
• INTEL 360 Foreign Intelligence Services	3
• INTEL 375 Security and the Economy	3
• COMM 308 Disinformation and Propaganda	3
• DCD 312 Social Media	3
IV. Additional Requirements	
A) Cognate	**9**
V. Electives	**9-28**

†**REACH Act Compliance:** As part of their graduation requirements, all students at CCU must complete either *HIST 201 - History of the United States from Discovery to the Present: Discovery through Reconstruction*, or *POLI 201 - Introduction to American Government*, which are both REACH Act compliant. Sample syllabi are available upon request.
* Course credit hours only count once toward the total university graduation credit hour requirements.
**Denotes a new course that is proposed concurrently with the major program.

New Courses

INTEL 318 (3 Credits) (Prereq: INTEL 200 or permission of the instructor) – Open-Source Intelligence Collection. This course explores the topic of open-source intelligence (OSINT) in a social, cultural, political, and legal context. It introduces students to the history of OSINT as a field, its development and relevance to intelligence. Essential components of the course include what sources of intelligence collection exist, and how to identify, understand, use, and analyze the intelligence collected from them. Special attention is given to various specific sources of OSINT and the preparation of students to build logical, concise, and informative OSINT briefs, reports, and scholarly materials. NOTE: Located in Section 3E (Intelligence and Security Studies Major Elective Courses) of the proposed curriculum.

INTEL 345 (3 Credits) – Cybersecurity Strategy and Governance. This course explores cybersecurity strategy and governance. It introduces students to the essential elements of strategy development and governance issues in cybersecurity. The second part of the course explores various topics important for the development of cybersecurity strategy and governance. Special attention is paid to the connections between cybersecurity policies, businesses, and governmental institutions, the social, political, and ethical implications that arise in cybersecurity policies, strategies to assess cybersecurity policy, and the interaction between national security and cybersecurity policy. NOTE: Located in Section 3D (Intelligence and Security Studies Core Courses) of the proposed curriculum.

INTEL 350 (3 Credits) (Prereq: INTEL 200 and CSCI 101 or permission of the instructor) – Understanding Cyber Threat Actors. This course provides an in-depth exploration of cyber threat actors, their motivations, techniques, and impact on cybersecurity. Through a multidisciplinary approach, students will analyze real-world case studies, engage with the writings of industry experts, and develop a comprehensive understanding of the evolving landscape of cyber threats. The course will cover various threat actor profiles, their tactics, techniques, and procedures, and strategies for defending against them.
NOTE: Located in Section 3D (Intelligence and Security Studies Core Courses) of the proposed curriculum.

INTEL 351 (3 Credits) (Prereq: INTEL 200 or permission of the instructor) – Emerging Technologies in Intelligence and Security. This class examines the role of new technological innovation on the processes and policies of intelligence and security. Beyond an in-depth exploration of several contemporary emerging technologies, the course will also consider the theories of technological change and historical case studies relating to the integration of new technologies in intelligence and security affairs.
NOTE: Located in Section 3D (Intelligence and Security Studies Core Courses) of the proposed curriculum.

Total Credit Hours Required: 120

Curriculum by Year					
Course Name	**Credit Hours**	**Course Name**	**Credit Hours**	**Course Name**	**Credit Hours**
Year 1					
Fall		**Spring**		**Summer**	
UNIV 110	3	ENGL 102	4		
ENGL 101	4	Core Curr. – 2B Course	3		
PHYS 104/L	4	INTEL 200	3		
HIST/POLI 201*	3	Core Curr. – 2C Course	3		
INTEL 250	3	CSCI 101	3		
Total Semester Hours	17	Total Semester Hours	16	Total Semester Hours	0
Year 2					
Fall		**Spring**		**Summer**	
Core Curr. 1C Course	5	INTEL 309	4		
STAT 201/Lab	4	Core Curr. – 2B Course	3		
Core Curr. – 2C Course	3	Core Curr. – 2D Course	3		
CSCI 216	3	CSCI 270	3		
		CSCI 385	3		
Total Semester Hours	15	Total Semester Hours	16	Total Semester Hours	0

*__REACH Act Compliance:__ As part of their graduation requirements, all students at CCU must complete either *HIST 201 - History of the United States from Discovery to the Present: Discovery through Reconstruction*, or *POLI 201 - Introduction to American Government*, which are both REACH Act compliant. Sample syllabi are available upon request.

(Continued next page.)

Course Name	Credit Hours	Course Name	Credit Hours	Course Name	Credit Hours
Year 3					
Fall		**Spring**		**Summer**	
INTEL 310	3	INTEL 350	3		
INTEL 345	3	INTEL Major Elective	3		
CSCI Major Elective	3	Major Elective CSCI	3		
Cognate Course	3	Cognate Course	3		
Core Curr. – 1A Course	3	Elective	3		
Total Semester Hours	15	Total Semester Hours	15	Total Semester Hours	0
Year 4					
Fall		**Spring**		**Summer**	
INTEL 351	3	INTEL 410	3		
INTEL Major Elective	3	Elective	3		
Cognate Course	3	Elective	3		
Elective	3	Elective	3		
Elective	1	Elective	1		
Total Semester Hours	13	Total Semester Hours	13	Total Semester Hours	

2 Year Plan (Assuming completion of Associate of Arts or Associate of Science degree at a different institution):

Course Name	Credit Hours	Course Name	Credit Hours	Course Name	Credit Hours
Year 3					
Fall		**Spring**		**Summer**	
INTEL 200	3	INTEL 250	3		
CSCI 101	3	STAT 201/L or POLI 205	3/4		
PHYS 104/L or SCI 101/L	4	CSCI Elective	3		
CSCI 216	3	INTEL 310	3		
INTEL 345	3	INTEL 350	3		
Total Semester Hours	16	Total Semester Hours	15/16	Total Semester Hours	0
Year 4					
Fall		**Spring**		**Summer**	
CSCI 270	3	INTEL 410	3		
INTEL 309	3	CSCI 385	3		
CSCI Elective	3	INTEL 351	3		
INTEL Elective	3	Cognate	3		
INTEL Elective	3	Cognate	3		
Cognate	3				
Total Semester Hours	18	Total Semester Hours	15	Total Semester Hours	

Similar Programs in South Carolina offered by Public and Independent Institutions
Identify the similar programs offered and describe the similarities and differences for each program.

Program Name and Designation	Total Credit Hours	Institution	Similarities	Differences
BS, Cyber Intelligence	120	University of South Carolina	Interdisciplinary approach that blends technical and non-technical aspects of cyber.	Less extensive coverage of intelligence process to cyber-related threats.
BS, Cyber Policy and Ethics	121	University of South Carolina	Interdisciplinary approach that blends technical and non-technical aspects of cyber.	No coverage of intelligence process to cyber-related threats.
BA, Intelligence and Security Studies	120	The Citadel	Coverage of intelligence process in the security domain.	Cyber is not the focus of the program. Minimal coverage of cybersecurity issues.
BS, Cyber Operations	123	The Citadel	Coverage on technical elements of cybersecurity.	No coverage of social elements of cybersecurity or intelligence threat assessment.
BS, Cybersecurity	120	USC-Upstate	Coverage on technical elements of cybersecurity	No coverage of social elements of cybersecurity or intelligence threat assessment.
B.S., Applied Computer Science with concentration in Cybersecurity	120	USC-Aiken	Coverage on technical elements of cybersecurity	No coverage of social elements of cybersecurity or intelligence threat assessment.
BS, Cybersecurity	120	Lander University	Coverage on technical elements of cybersecurity	No coverage of social elements of cybersecurity or intelligence threat assessment.
BS, Cybersecurity and Criminal Justice	123	Anderson University	Coverage on technical and social elements of cybersecurity	Coverage confined to criminal justice area with no coverage of intelligence threat assessment.
BS, Cybersecurity	128	Benedict College	Coverage on technical elements of cybersecurity	No coverage of social elements of cybersecurity or intelligence threat assessment.

BS, Computer Science with concentration in Cybersecurity	120	South Carolina State University	Coverage on technical elements of cybersecurity	No coverage of social elements of cybersecurity or intelligence threat assessment.

Nationally, there are fewer than ten comparable programs at the undergraduate level. There are comparable programs at UT-San Antonio, University of Southern California, Ferris State University (Michigan), and Johnson and Wales University (Rhode Island). Available data suggests that graduates from such programs are very successful. For instance, the Cyber Intelligence and Security B.S. program at Embry Riddle Aeronautical University in Prescott, Arizona boasts a 100 percent placement rate with an average salary of $74,800 within one year of graduation.[34]

Faculty

Rank and Full- or Part-time	**Courses Taught for the Program**	**Academic Degrees and Coursework Relevant to Courses Taught, Including Institution and Major**	**Other Qualifications and Relevant Professional Experience (e.g., licensures, certifications, years in industry, etc.)**
Professor; Full-Time	INTEL Courses	Ph.D., Political Science, University of South Carolina	Created/Directed BA in Intelligence and National Security Studies at CCU; Retired Naval Intelligence Officer (23yrs); Existing faculty teaching in courses currently offered/applicable to the degree.
Professor; Full-Time	INTEL Courses	Ph.D., Political Science, Glasgow University	Created/Directed BA in Intelligence and Security Studies at King University; Existing faculty teaching in courses currently offered/applicable to the degree.
Asst. Professor; Full-Time	INTEL Courses	Ph.D., International Studies, Old Dominion University	Visiting Research Professor, School of Cybersecurity, Old Dominion University (2yrs); Existing faculty teaching in courses currently offered/applicable to the degree.
Asst. Professor; Full-Time	INTEL Courses	Ph.D., Political Science, Duke University	Existing faculty teaching in courses currently offered/applicable to the degree.
Asst. Professor; Full-Time	INTEL Courses	Ph.D., Political Science, University of Arizona	Existing faculty teaching in courses currently offered/applicable to the degree.
(NEW) Asst. Professor; Full-Time	INTEL and CSCI Courses	Joint Appointment (to be hired)	
Lecturer; Full-Time	INTEL Courses	M.A., International Relations, Troy University	Retired Defense Senior Intelligence Service-2 Officer (2-Star Flag Officer Equivalent) (37yrs); Existing faculty

[34] "Bachelor of Science in Cyber Intelligence and Security", Embry Riddle Aeronautical University (Prescott Campus). https://erau.edu/degrees/bachelor/cyber-intelligence-security.

			teaching in courses currently offered/applicable to the degree.
Associate Professor; Full-Time	CSCI Courses	Ph.D. in Computer Science, Clemson University	Existing faculty teaching in courses currently offered/applicable to the degree.
Senior Lecturer; Full-Time	CSCI Courses	M.S. in Computer Science, University of South Carolina	Existing faculty teaching in courses currently offered/applicable to the degree.
Lecturer; Full-Time	CSCI Courses	M.A. in Computer Resource and Information Management, Webster University	Retired U.S. Airforce (NCOIC), computer programmer, project manager; Existing faculty teaching in courses currently offered/applicable to the degree.
Teaching Associate; Part-Time	CSCI Courses	M.S. in Information Technology, East Carolina University	Linux Systems Engineer; Existing faculty teaching in courses currently offered/applicable to the degree.
Teaching Associate; Part-Time	CSCI Courses	Ph.D. in Cyber Operations, Dakota State University Master of Information Technology, Virginia Tech	Information Security Manager; Solutions Engineer; Existing faculty teaching in courses currently offered/applicable to the degree.
Professor; Full-Time	PHYS Course	Ph.D. in Physics, Michigan State University	Existing faculty teaching in courses currently offered/applicable to the degree.
Lecturer; Full-Time	STAT Course		Existing faculty teaching in courses currently offered/applicable to the degree.

Total FTE needed to support the proposed program:
Faculty: 3.0 FTE
Staff: 0.33 FTE
Administration: 0.16 FTE

Faculty, Staff, and Administrative Personnel
The program can begin with existing faculty levels to meet the projected demand in year 1 of the program. However, an assistant professor tenure-track line will be needed in the Intelligence and Security Studies and Computing Sciences departments by the end of year 1 to meet the projected demand for this new program.

Resources

Library and Learning Resources
Explain how current library/learning collections, databases, resources, and services specific to the discipline, including those provided by PASCAL, can support the proposed program. Identify additional library resources needed.

Kimbel Library holds about 1.1 million items in all formats, including over 375,000 eBooks provided by PASCAL, a statewide consortium. The library subscribes to about 230,000 periodicals, including magazines, newspapers, scholarly journals, and proceedings in print and online formats. The library provides access to its print holdings, 175 online citation, full-text, and reference resources, via the library website at www.coastal.edu/library. All electronic resources, including books, articles, and videos, are available to Coastal students, faculty, and staff from off campus.

Course-integrated library instruction sessions are available to all academic departments; the library also offers one-credit information literacy courses. Librarians offer appointments for in-depth research help. Kimbel Library is open 98 hours per week during the fall and spring semesters; during that time, library staff members are available to assist students via phone, chat, or in-person at the help desk.

Teaching faculty provide input regarding selection of library resources, including both print and electronic resources. The physics and education departments have a designated library liaison who takes order requests and communicates with faculty when new resources are available.

Student Support Services
All CCU students have access to university sponsored student support services including Accessibility and Disability Services, Student Computing Services, Kimbel Library, Student Health Services, and the Coastal Student Success Center including the Tutoring and Learning Center.

Majors in this program will receive academic advising from the Edwards College of Fine Arts and Humanities for their freshman and sophomore years. The Department of Intelligence and Security Studies faculty will assume academic advising responsibilities at the start of the junior year.

Physical Resources/Facilities
There are no additional physical resources needed to start this program. The current classroom space is adequate to service the program. Further, the Intelligence Operations Command Center – a 1600 square foot simulated intelligence watch floor – can provide unique pedagogical opportunities for students in this program.

Equipment
The is no additional equipment that is required to start the Cyber Threat Intelligence program.

Impact on Existing Programs
Will the proposed program impact existing degree programs or services at the institution (e.g., course offerings or enrollment)? If yes, explain.

☒Yes

☐No

Given that this program represents a fusion of the technical and non-technical issues in the cyber domain, students completing the B.A. in Cyber Threat Intelligence degree will be taking some of the same classes offered for the B.S. programs in the Department of Computing Sciences, as well as the B.A. in Intelligence and Security Studies – in addition to the unique courses required for this program. However, these new courses for the CTI program will be able to also serve as elective courses in some of these existing programs.

This new program is expected to impact the enrollment levels in some of the offerings for these departments but will not be beyond the current enrollment space for at least the first year. Additional demand in courses will be mitigated by hiring a new faculty member in year 2 to be shared by the Department of Computing Sciences and the Department of Intelligence and Security Studies.

Meeting: CAAL Meeting
Meeting Date: May 9, 2024
Agenda Item: 5F

Financial Support

Sources of Financing for the Program by Year												
	1st		2nd		3rd		4th		5th		Grand Total	
Category	**New**	**Total**	**New**	**Total**	**New**	**Total**	**New**	**Total**	**New**	**Total**	**New**	**Total**
Tuition Funding	$209,514	$306,864	$213,704	$677,270	$217,978	$973,196	$222,338	$1,230,719	$226,785	$1,300,003	$1,090,319	$4,488,052
Program-Specific Fees											$0	$0
Special State Appropriation											$0	$0
Reallocation of Existing Funds											$0	$0
Federal, Grant or Other Funding											$0	$0
Total	**$209,514**	**$306,864**	**$213,704**	**$677,270**	**$217,978**	**$973,196**	**$222,338**	**$1,230,719**	**$226,785**	**$1,300,003**	**$1,090,319**	**$4,488,052**
Estimated Costs Associated with Implementing the Program by Year												
	1st		2nd		3rd		4th		5th		Grand Total	
Category	**New**	**Total**	**New**	**Total**	**New**	**Total**	**New**	**Total**	**New**	**Total**	**New**	**Total**
Program Administration and Faculty/Staff Salaries		$107,163	$91,800	$298,094		$381,343		$452,036		$473,942	$91,800	$1,712,578
Facilities, Equipment, Supplies, and Materials		$0		$0		$0		$0		$0	$0	$0
Library Resources		$0		$0		$0		$0		$0	$0	$0
Other (specify)												
Total	**$0**	**$107,163**	**$91,800**	**$298,094**	**$0**	**$381,343**	**$0**	**$452,036**	**$0**	**$473,942**	**$91,800**	**$1,712,578**

Net Total (Sources of Financing Minus Estimated Costs)	**$209,514**	**$199,701**	**$121,904**	**$379,176**	**$217,978**	**$591,854**	**$222,338**	**$778,683**	**$226,785**	**$826,061**	**$998,519**	**$2,775,474**

Note: New costs - costs incurred solely as a result of implementing this program. Total costs - new costs; program's share of costs of existing resources used to support the program; and any other costs redirected to the program.

Budget Justification

Provide a brief explanation for all of the costs and sources of financing identified in the Financial Support table.

Program cost-effectiveness and return-on-investment are evaluated institutionally using an induced revenue/expense model. As shown in the Financial Support table, tuition revenues are based on a 15-credit course load for each student projected to enroll in the program. These revenues represent course revenues derived from all courses taken by the student, including both departmental-fielded courses and cross-department electives. The expenses shown in the Financial Support table represent only direct expenses necessary for delivering program courses and administration. The beginning program administration and faculty/staff salaries total are determined by using average faculty and administration salaries of faculty and staff supporting the program based on FTEs for the program. The expenses for new faculty or administration salaries are determined by using a proportion of the CUPA salary averages based on FTE for new positions in the year being hired. The university uses a 50% gross academic margin assessment to ensure that new undergraduate and certificate programs will provide sufficient revenues to support their expense impact on institutional operations.

To derive gross academic margin, total induced revenue ($4,488,052 for the period) is calculated minus total direct expenses ($1,615,885 for the period) divided by total induced revenue ($4,488,052 for the period). [(Revenue-Expenses)/Revenue]

For a program to be considered cost-effective, the University looks for undergraduate and certificate programs to produce a gross academic margin of 50% or better. This program's gross academic margin is 64.0% for the period, which indicates that this program has a high likelihood of producing sustainable revenues.

Evaluation and Assessment

Program Objectives	Student Learning Outcomes Aligned to Program Objectives	Methods of Assessment
Develop student abilities to employ intelligence analysis practices to assess the activities, capabilities, and intentions of threat actors in the cyber domain.	Apply various analytical techniques to real-world intelligence challenges.	Program Faculty will assess a sample of student term papers from INTEL 410 Cyber Threat Intelligence using a pre-determined rubric.
Advance student skills related to the assessment and impact of threats of computer information networks and systems from technical and human factors.	Conduct comprehensive threat assessments of contemporary cyber threat actors and their associated tactics, techniques, and procedures.	Program Faculty will assess a sample of student term papers from INTEL 410 Cyber Threat Intelligence using a pre-determined rubric.
Encourage student analytic skills of governance structures and legal frameworks that inform the defense of cyber-related systems and activities.	Identify, discuss and critique core concepts and issues in cybersecurity policy and governance and existing measures to address them.	Program Faculty will assess a sample of student term papers from INTEL 410 Cyber Threat Intelligence using a pre-determined rubric.
Develop student abilities to analyze and evaluate the composition, operation, and evolution of computer systems and their associated network architecture.	Evaluate contemporary computer systems and network architecture to assess critical vulnerabilities.	Program faculty will assess a sample of student projects from the CSCI 385 Introduction to Information Systems Security course using a pre-determined rubric.
Enhance the critical thinking, reasoning, and problem identification/solving skills of student.	Demonstrate the ability to employ critical thinking and problem-solving skills in order to evaluate issues.	Students will be administered a pre/post-test in INTEL 200 Introduction to Intelligence and National Security and INTEL 410 Cyber Threat Intelligence.
Enhance student abilities to effectively communicate their findings that take into account time, audience, and security considerations.	Create and deliver written products that are relevant to the subject area.	Program Faculty will use a pre/post-test approach to assess this area by comparing a sample of papers in INTEL 250 Introduction to Security Studies and INTEL 410 Cyber Threat Intelligence using a pre-determined rubric.

Explain how the proposed program, including all program objectives, will be evaluated, along with plans to track employment. Describe how assessment data will be used.

INTEL 410 Cyber Threat Intelligence will function as an expected endpoint for the major program. The major project from this course will serve as a functional equivalent to a capstone assignment and will be used to assess the first 3 program objectives. Ten student projects will be selected at random and then evaluated by a 3-faculty member panel using pre-determined rubrics for each of these three objectives. Because CSCI 385 Introduction to Information Systems Security has CSCI 270 Data Communications Systems and Networks as a prerequisite, it represents a logical place to assess student learning in program objective 4. As with the first 3 program objectives, a group of 3 faculty will review a sample of 10 randomly-selected projects utilizing a pre-determined rubric. Program faculty will assess

objectives 5 and 6 using a pre/post-test format utilizing INTEL 200 Introduction to Intelligence and Security Studies or INTEL 250 Introduction to Security Studies to compare to similar assignments in INTEL 410 Cyber Threat Intelligence. Data from these assessments will be analyzed and employed to improve the program, as needed. Programmatic student learning outcome assessment is completed yearly, and is reviewed and evaluated at the college level by a college assessment committee. The college assessment committee makes recommendations for improvement to the department concerning both the structure of the assessment plan, and the outcomes of the assessment. At the University level, completion of yearly assessment is monitored by the University-Wide Assessment Committee – Educational Programs (UWAC-EP) Subcommittee. In addition, every three years, each program completes a three-year summary of their assessment outcomes, including an evaluation of the degree to which the program is meeting its student learning outcomes, and plans for improvements based on these outcomes. The three-year summaries are evaluated by the UWAC-EP, who also provides feedback and suggestions for improvement. In this way, the University ensures that yearly program assessment is completed, and also that programs close the loop leading to learning improvements.

Tracking employment rates for graduates will be conducted utilizing an alumni outreach survey.

Accreditation and Licensure/Certification

Will the institution seek program-specific accreditation (e.g., CAEP, ABET, NASM, etc.)? If yes, describe the institution's plans to seek accreditation, including the expected timeline.

☐Yes

☒No

Will the proposed program lead to licensure or certification? If yes, identify the licensure or certification.

☐Yes

☒No

Explain how the program will prepare students for this licensure or certification.

If the program is an Educator Preparation Program, does the proposed certification area require national recognition from a Specialized Professional Association (SPA)? If yes, describe the institution's plans to seek national recognition, including the expected timeline.

☐Yes

☒No

Appendix A: Letters of Support


Letter of Support - CMC Cyber Security


Letter of Support - HTC


Letter of Support - Santee Cooper


Letter of Support - SCIMA

Appendix B: Catalog Description

Cyber Threat Intelligence, B. A.

The Cyber Threat Intelligence major will prepare prepares students for careers and further study in the cyber domain that involve the analysis and evaluation of system vulnerabilities and the malicious actors that seek to exploit these vulnerabilities. Using an interdisciplinary approach, this major the synthesizes the technical and non-technical concepts in the field of cybersecurity and applies knowledge and skills from the field of intelligence analysis and security studies.

Student Learning Outcomes:
Students who complete the requirements for a degree in Cyber Threat Intelligence will be able to:

1. Apply various advanced analytical techniques to real-world intelligence challenges.
2. Demonstrate the ability to employ critical thinking and problem-solving skills in order to evaluate cybersecurity related challenges.
3. Evaluate contemporary computer systems and network architecture in order to assess critical vulnerabilities.
4. Conduct comprehensive threat assessments of contemporary cyber threat actors and their associated tactics, techniques, and procedures.
5. Identify, discuss and critique core concepts and issues in cybersecurity policy and governance and existing measures to address them.
6. Create and deliver oral and written products on cyber threat intelligence issues.

Students who wish to pursue a degree in intelligence and security studies must conform to the following regulations:

To remain a member of the major, a student must earn a grade of 'C' or better in each course used to satisfy requirements for the major, including foundation courses for the intelligence and security studies major. Students who fail to maintain this academic standard may be dropped from the program by the department chair upon unanimous recommendation of the program's faculty.

The curriculum for this program is interdisciplinary with most of the courses being housed in the Department of Intelligence and Security Studies. Students will complete the University core curriculum and a collection of foundation courses to establish a base-line level of knowledge in the relevant subject areas connected to the study of intelligence and security. These early courses also introduce students to core skills that are useful in the analysis, evaluation and communication of intelligence information. From here, students are positioned to expand their knowledge and skills in the realms of intelligence and security, as well as the regional and occupational contexts that inform these issues.

** Only three courses from the major requirements may be applied toward a student's minor requirements or a different major.

Cyber Threat Intelligence, B.A.

Degree Requirements (120 Credits)

Core Curriculum Requirements (36 to 40 credits)
Core Curriculum (36-40 Total Credit Hours)

Graduation Requirements (3 to 6 credits)

- UNIV 110 - The First-Year Experience (3 credits)
- HIST 201 - History of the United States from Discovery to the Present: Discovery through Reconstruction (3 credits) *or* POLI 201 - Introduction to American Government (3 credits)

REACH Act Compliance: As a graduation requirement, all students at CCU must complete either *HIST 201 - History of the United States from Discovery to the Present: Discovery through Reconstruction*, or *POLI 201 - Introduction to American Government* for REACH Act compliance. Sample syllabi are available upon request.

Program Requirements (44-56 Credits)

Foundation Courses
Complete the following courses (9 Credits):
CSCI 101 Introduction to the Internet and World Wide Web 3 credits
INTEL 200 Introduction to Intelligence and National Security 3 credits
INTEL 250 Introduction to Security Studies 3 credits
Complete the following course (4 Credits):
PHYS 104 Science for Security 3 credits and
PHYS 104L Science for Security Laboratory 1 credit
OR
SCIE 101 Introduction to Science 3 credits and
SCIE 101L Introduction to Science Laboratory 1 credit
Select one of the following courses (3-4 Credits):
POLI 205 Introductory Statistics for the Political and Social Sciences 3 credits
OR
STAT 201 Elementary Statistics 3 credits and
STAT 201L Elementary Statistics Computer Laboratory 1 credit

Computing Sciences Core Courses
Complete the following courses (9 Credits):
CSCI 216 Linux Fundamentals I 3 credits
CSCI 270 Data Communication Systems and Networks 3 credits
CSCI 385 Introduction to Information Systems Security 3 credits

Computing Sciences Elective Courses

Choose two upper-division courses from a rotation of current offerings (6 Credits):

CSCI 316 Linux Fundamentals II 3 credits
CSCI 386 Offensive Security 3 credits
CSCI 416 Linux System Administration 3 credits
CSCI 434 Digital Forensics 3 credits
CSCI 435 Anti-Forensics and Digital Privacy 3 credits

Intelligence and Security Studies Core Courses

Complete the following courses (18 Credits)

INTEL 350 Understanding Cyber Threat Actors 3 credits
INTEL 309 Data Analytics for Intel & Security Studies 3 credits
INTEL 310 Intelligence Analysis 3 credits
INTEL 345 Cybersecurity Strategy and Governance 3 credits
INTEL 351 Emerging Technologies in Intelligence and Security 3 credits
INTEL 410 Cyber Threat Intelligence 3 credits

Intelligence and Security Studies Major Elective Courses

Choose two upper-division courses from a rotation of current offerings (6 Credits)

COMM 308 Disinformation and Propaganda 3 credits
DCD 312 Social Media 3 credits
INTEL 318 Open-Source Intelligence Collection 3 credits
INTEL 311 Intelligence Communications 3 credits
INTEL 312 Intelligence Operations 3 credits
INTEL 313 Covert Action & Grey Zone Conflict 3 credits
INTEL 315 Human Intelligence 3 credits
INTEL 335 Homeland Security 3 credits
INTEL 340 National Security Strategy 3 credits
INTEL 341 Intelligence and War 3 credits
INTEL 343 Terrorism and Political Violence 3 credits
INTEL 344 Weapons of Mass Destruction 3 credits
INTEL 360 Foreign Intelligence Services 3 credits
INTEL 375 Security and the Economy 3 credits

Cognate (9 Credits)

Requirements

A minimum of nine credits is required to complete the cognate requirement. Courses taken for cognate credit must be at the 300 level (or above) and not be otherwise required by the major program. Students may also count study abroad courses, experiential learning courses, international study credits, or internship credit towards this cognate requirement.

Electives (9-28 Credits)

Total Credits Required: 120 Credits

From:	Emma Savage-Davis
To:	Dr. Cheng-Yuan "Corey" Lee; Joseph Winslow; Alex Fegely
Cc:	Holley Tankersley
Subject:	FW: Costal Carolina University Computer Science Add-on
Date:	Wednesday, May 19, 2021 3:21:17 PM
Attachments:	image003.png image005.png

Great news Gentlemen. See the e-mail below. Congratulations!!!

Just so that you are aware, for MAT to add the computer science course as a content area, they will need to submit a new program proposal to CHE and the state department for their approval. This document does not provide that approval.

Emma

Dr. Emma Savage-Davis
Coastal Carolina University
Spadoni College of Education
Professor of Education
Coordinator of the Middle Level Education Program
Chair of the Department of Graduate and Specialty Studies
105G Prince Hall
P.O. Box 261954
Conway, SC 29528-6054
Office/Fax 843-349-2738
esavage@coastal.edu

From: Ritter, James <jritter@ed.sc.gov>
Sent: Wednesday, May 19, 2021 2:38 PM
To: Emma Savage-Davis <esavage@coastal.edu>
Cc: Schneider, Sherry <SSchneider@ed.sc.gov>; Strauss, Keri <KStrauss@ed.sc.gov>; Walsh, Jaclyn <jwalsh@ed.sc.gov>
Subject: Costal Carolina University Computer Science Add-on

Dear Dr. Savage-Davis:

The Coastal Carolina University courses submitted for the add-on area certification in Computer

Science have been reviewed and accepted. Please let us know if there are any revisions to this course sequence in the future so that it can be reviewed and revised. As a reminder, the courses are valid only for add-on purposes and not as an approved program for initial certification.

Best,

James

James Ritter, Ph.D., Education Associate
Office of Educator Services
South Carolina Department of Education
8301 Parklane Rd.
Columbia, SC 29223
(803) 896-0223 (phone)
(803) 896-0395 (fax)
jritter@ed.sc.gov
www.ed.sc.gov

The Office of Educator Services Call Center is available at 803-896-0325 to assist current and prospective educators.

Call Center Hours: Monday through Friday except on State Holidays (beginning November 6, 2020)

Monday	12:30 to 4:30 p.m.
Tuesday	9:00 a.m. to 1:00 p.m.
Wednesday	12:30 to 4:30 p.m.
Thursday	9:00 a.m. to 1:00 p.m.
Friday	12:30 to 4:30 p.m.

From: Emma Savage-Davis <esavage@coastal.edu>
Sent: Monday, May 10, 2021 11:15 AM
To: Ritter, James <jritter@ed.sc.gov>
Subject: Computer Science Add-on

Good Morning James,

I hope all is well with you. I would like to submit the attached documents for SCDE review and consideration for meeting the add-on teaching endorsement in Computer Science. The Post-Baccalaureate Certificate was approved by CHE on October 29, 2020. We have reviewed the SC Teacher Certification Manual and, in the attached Memo to SCDOE, have aligned the courses within

the certificate program to the state add-on course requirements. You will also find a copy attached of the CHE proposal.

We understand that licensing decisions are solely the responsibility of the state department. Our efforts for this add-on is with our students in mind. We are trying to accommodate our students interests to expand their license. Please let me know if you have any questions pertaining to this request.

Emma

Dr. Emma Savage-Davis
Coastal Carolina University
Spadoni College of Education
Professor of Education
Coordinator of the Middle Level Education Program
Chair of the Department of Graduate and Specialty Studies
105G Prince Hall
P.O. Box 261954
Conway, SC 29528-6054
Office/Fax 843-349-2738
esavage@coastal.edu

SCDE Add-on or Endorsement Requirement	**CCU Course** (prefix, number, title)	**Credit Hours**	**Course Description**
Computing Systems	CSED 605: Foundations of Computing Systems	3	This course examines the ecology of modern computing through the lens of abstraction, a technical concept that explains how the relationships among hardware and software components impact device functionality. Students are challenged to analyze use cases and identify strategies to design, manage, and troubleshoot computing systems to solve real-world problems.
Network and the Internet	IST 610: Networking and Cybersecurity Fundamentals	3	This course provides students with the fundamentals in networking and cybersecurity. The course discusses the principles of networking including protocols, topologies, circuit and packet switching, routing, and related topics. The course also provides students with a foundation in cybersecurity topics such as security threats, vulnerability analysis, firewalls, intrusion detection, and access control. This course is designed for students with little or no prior networking or security experience.
Data and Analysis	CSED 607: Introduction to Data Science	3	This course explores fundamental tools and methods for collecting, managing, and processing big data using computational models, statistical inferencing, and machine learning to identify trends, support claims, and solve real-world problems in varied disciplines. Data visualization and storytelling techniques are also emphasized. Prior experience in programming or statistical analysis is not required.
Algorithms and Programming	CSED 608: Computational Thinking and Programming	3	This course promotes understanding of computer programming and logic by teaching students to "think like a computer." The course explores skills needed to develop and design language-independent solutions to solve computer-related problems. This course also covers development and design basics, including use of variables, control and data structures, principles of command-line, and object-oriented languages.

Impact of Computing	EDIT 604: Teaching with Technology	3	A standards-based investigation of instructional technologies and their potential to impact teaching practices, professional productivity, and student performance.