Program Proposal for an Undergraduate Certificate

1. Name of the proposed undergraduate certificate.

   Certificate in Cybersecurity
2. Name of the department(s) involved.

   Electrical and Computer Engineering
3. Name of contact person(s).

   Doug Jacobson

   Jeff Franklin
4. General description of the undergraduate certificate.

   The Undergraduate Certificate in Cybersecurity is aimed at graduates with an AAS degree (two-year degree) who are working in a security or IT-related field. The certificate will provide the material needed to upskill students so that they can gain cybersecurity knowledge. The certificate will be offered online as a series of half semester 2 credit courses (the professional communications course is a full semester 3 credit course). The certificate will be 21 credits. The courses in the certificate will map to federal training standards as outlined in the NIST/NICE framework.

   This certificate can be awarded to AAS degreed students who complete the certificate requirements without having earned a bachelor's degree.

5. Need for the proposed undergraduate certificate.

   We have conducted workshops, concluding that employers and organizations are looking for mid to advanced-level cybersecurity employees. The courses that will be part of the certificate were vetted by several employee groups and are designed to meet the needs of the current workforce and employers. While there are not many cybersecurity professionals with four-year degrees, there are many graduates with an AAS degree. The certificate will bridge the knowledge gap between a two- and a four-year degree.
6. Objectives of the proposed undergraduate certificate including the student learning outcomes and how the learning outcomes will be assessed.

   Program Objectives

   - **Upskill Graduates:** To provide graduates with an Associate of Applied Science (AAS) degree in a security or IT-related field with advanced cybersecurity knowledge.
   - **Alignment with Federal Standards:** To offer a curriculum that aligns with federal training standards as outlined in the NIST/NICE framework.
   - **Bridging Knowledge Gaps:** To bridge the knowledge gap between two-year and four-year degrees in cybersecurity, addressing the current needs of the workforce and employers.

Student Outcomes

- **Advanced Cybersecurity Knowledge:** Students will gain in-depth knowledge in various aspects of cybersecurity, including network security, data security, web security, and more.
- **Practical Skills and Competencies:** Students will develop practical skills and competencies required for mid to advanced-level positions in the cybersecurity field.
- **Effective Communication:** Students will be trained to effectively communicate complex cybersecurity concepts to a diverse professional audience.
- **Adversarial Thinking:** Students will learn to anticipate and mitigate cyber threats through an understanding of cybersecurity from an attacker's perspective.
- **Comprehensive Understanding of Cybersecurity Architecture:** Students will be able to develop and apply a comprehensive cybersecurity architecture in real-world scenarios.

Overall Assessment

- **Course-Based Assessments:** Each course will include various forms of assessments like exams, projects, research papers, and case studies to evaluate the students' understanding and application of the concepts.
- **Capstone Project:** A comprehensive capstone project that integrates and applies the knowledge gained throughout the program, requiring students to develop a complete security architecture.
- **Continuous Evaluation:** Ongoing assessments through quizzes, assignments, and interactive sessions to ensure consistent learning and application of skills.
- **Feedback and Improvement:** Regular feedback mechanisms to identify areas of improvement and to align teaching methodologies with student learning outcomes.

7. Relationship of the undergraduate certificate to other programs at Iowa State University.

   There is small overlap with the BS in cybersecurity engineering and the minor in cybersecurity. However, the audience is different. Except for the communications course, the certificate courses are only offered to students enrolled in the program. After the program is established, other programs may allow some certificate courses to serve as electives.

8. Relationship of the undergraduate certificate to the strategic plans of the university, of the college, and of department or program.

   The Professional Certificate in Cybersecurity aligns with Iowa State University's strategic plan by contributing to the university's mission of fostering academic excellence and innovation. The program addresses the growing demand for skilled professionals in the field of cybersecurity, reflecting the university's commitment to addressing current and future societal needs.

   At the college and departmental level, the certificate program complements and enhances the existing curriculum by offering specialized knowledge in cybersecurity, a key area of focus in today's digital world. This initiative supports the department's strategic goals of academic innovation, educational relevance, and preparing students for successful careers in a rapidly evolving technological environment.

9. Comparison of the proposed undergraduate certificate with similar programs at other universities, including the Regent's universities.

Neither UNI nor the University of Iowa have anything similar to this program

10. Program requirements and procedures, including:
    a. prerequisites for prospective students;

       An AAS, AA, AS or BS. There are course prerequisites that require previous coursework in cybersecurity, information technology and/or networking.
    b. application and selection process;

       Using ISU online and ISU admissions processes
    c. language requirements;

       None
    d. courses and seminars presently available for credit toward the program; None
    e. proposed new courses or modifications of existing courses;

       See the list at the end of the document
    f. advising of certificate students;

       ISU Online and electrical and computer engineering advisors
    g. implications for related areas within the university.

       None

11. General description of the resources currently available and future resource needs, in terms of:
    a. faculty members;

       Two FTE Professor of Practice positions were provided by the Provost's office. One Professor of Practice has been hired. A number of part-time faculty likely fill the commitment for the additional FTE Professor of Practice.
    b. computers, laboratories, and other facilities;

       The department maintains a laboratory for cybersecurity
    c. library facilities (journals, documents, etc.) in the proposed area;

       No additional resources
    d. supplies, field work, student recruitment, etc.

       Recruitment will be a combination of the College of Engineering and ISU online

12. Describe the needs for new resources and/or reallocated resources. Attach to the program proposal memos from the department chair(s), the college dean(s), and other appropriate persons, agreeing to the allocation of new resources and/or the reallocation of resources.
    New resources are the two FTE Professors of Practice funded by the Provost.

13. Attach to the program proposal, letters of support, recommendations, and statements when appropriate, from programs and departments at ISU which are associated with the proposed program or have an interest in the proposed program.
    To be provided: from CS, and MIS.

14. If the new program is interdisciplinary, a governance document should be created and submitted to the Associate Provost for Academic Programs. Indicate here that it has been completed.
    N/A

Appendix A. Course list and tentative course descriptions

(note these are working titles and are subject to change)

Required Courses	College / Dept	Credits
Professional Communication for IT & Cyber (Engl 314)	LAS/Engl	3
Fundamentals of Network Security	ENG/ECE	2
Adversarial thinking and cybersecurity architecture	ENG/ECE	2
Fundamentals of Data Security and Privacy	ENG/ECE	2
Fundamentals of Web Security	ENG/ECE	2
Cybersecurity Capstone	ENG/ECE	2
Total required credits		13
Threat hunting and intelligence	ENG/ECE	2
Digital Forensics and Incident Response	ENG/ECE	2
Applications of Cryptography	ENG/ECE	2
Fundamentals of Operating Systems Security	ENG/ECE	2
Fundamentals of Cloud Security	ENG/ECE	2
Fundamentals of Software Security	ENG/ECE	2
Fundamentals of Cybersecurity Scripting	ENG/ECE	2
Fundamentals of Cyber Resilience	ENG/ECE	2
Fundamentals of Cyber-Physical and Critical Infrastructure Security	ENG/ECE	2
Total elective credits		8
Total credits for the certificate		21

Structure of the courses/modules

The proposed technical courses will be 2 credits each and will be offered asynchronously via Canvas. Each course will consist of modules (between 5 and 10) totaling 30 contact hours. Each course will follow the same format as shown below:

- Course introduction/checks for understanding and misconceptions
- Multiple modules
- Posttest / assessment

The structure of a module is shown below:

Delivered content				Post content activities	
Video	Assessment/ Activity/ Checks for understanding	Video	Assessment/ Activity/ Checks for understanding	Lab / Research	Reflection paper

The videos will be 5 to 20 minutes long and will have post-video assessments and/or activities. The post-video assessment will be designed to be auto-graded with feedback. After each module, there will be assigned work which could consist of a lab component, additional research, and/or a reflection paper. The post-module assessment may require an instructor / TA to evaluate.

Student / Faculty Interaction

To facilitate student-to-student and student-to-TA interaction we will use discussion boards. These will be used for general discussions of topics within a course.

Each course will start with "checks for understanding" and "identifying misconceptions." The TA will use this to populate a discussion thread to address the misconceptions and help fill any identified gaps.

The TA and feedback will read each essay/reflection paper will be provided.

The TA will also interact with the students via Canvas messaging to answer specific questions. We could also hold virtual office hours via some type of chat room.

Proposed Certificate Courses

Professional Communication for IT & Cyber— The main objective of this course is to train people with security knowledge to communicate effectively with professionals at various levels. The course aims to convert technical information into simple, meaningful language that non-technical people can understand. Presenting information in the right way can help convey the intricacies of the cyber world and the technical aspects of the dynamic nature of cyber threats and the information environment itself. The course will focus on oral, written, and impromptu communication. English has agreed to create a section of English 314 to meet the requirements.

Adversarial Thinking and Cybersecurity Architecture— This course looks at cybersecurity from an attacker's perspective. This course aims to help develop cybersecurity students' abilities to anticipate the strategic actions of cyber adversaries, including where, when, and how they might attack, the motives behind their attacks, and their tactics for evading detection. The course will introduce multiple cybersecurity architectures and apply adversarial thinking.

Fundamentals of Network Security— Detailed examination of networking standards, protocols, and their implementation. TCP/IP protocol suite, network application protocols. Network security issues across all layers, attack, and mitigation techniques.

Fundamentals of Data Security and Privacy — Introduction and application of basic mechanisms for protecting data. Security issues related to safeguarding sensitive personal and corporate information against inadvertent disclosure. Real-world effects of data breaches on individuals and businesses and the balancing of interests among individuals, government, and enterprises. Emerging technologies that may affect security and privacy concerns. Issues related to developing enterprise data security programs, policies, and procedures that consider the requirements of all relevant constituencies, *e.g.,* technical, business, and legal.

Fundamentals of Web Security— The course covers fundamental concepts of web programming, web vulnerability exploitation, and web browser design flaws. Build secure web applications using HTTP, HTML, and JavaScript - basic syntax, object-oriented programming, the document object model (DOM), and AJAX. Web security issues, such as SQL injection, cross-site scripting, session hijacking, malvertising, and other web vulnerabilities, and how to detect, defend, and protect against such attacks using Open Web Application Security Project (OWASP).

Capstone—Security Architecture— The capstone will extend some of the concepts covered in various security certifications (CompTIA – NET+, ITF+, Cloud+, etc.) and prepare for developing a complete end-to-end security architecture. A scenario that may be sector-based will be provided. The following are the requirements from the students:

- Develop the secure technology
- Provide a response plan or technical report
- Present the plan to both the technical staff and C-suite

Threat Hunting and Intelligence— Threat hunting is a proactive technique that focuses on the pursuit of attacks and the evidence that attackers leave behind when they conduct reconnaissance, information gathering, payload attacks with malware or zero-day attacks, or exfiltrating sensitive data. The threat-hunting process allows attacks to be discovered earlier with the goal of stopping them before any negative impact occurs. The course will establish a proactive defense mentality by identifying threats in systems and networks; guiding a hunt across typical security toolsets—such as SIEM, packet capture, and EDR; using threat intelligence or hypotheses to hunt for known and unknown threats. Some topics include Threat Analysis, Vulnerability Assessment, Penetration Testing, Intrusion Detection, Malware Engineering, Counter Intelligence, Signals Intelligence, Intelligence Operations and Analysis.

Digital Forensics and Incident Response— This course will cover fundamentals of computer and network forensics, forensic duplication and analysis, network surveillance, intrusion detection and response, incident response, anonymity and pseudonymity, privacy-protection techniques, cyber law, computer security policies and guidelines, court testimony and report writing, and case studies. Emphasis on hands-on experiments.
This course will also include incident response. Each computer incident has the potential to cause data loss or service outage. Businesses must be aware of how best to protect themselves through the development of incident response policies and operational procedures to respond to and analyze these incidents. At the top level is the incident response policy, and understanding how to develop and maintain such a policy is critical. Incident response team development and management, evidence handling, and the technical skills necessary to locate appropriate evidence are covered.

Applications of Cryptography— Basic cryptographic underpinnings used in modern cyber security encryption suites. Encryption benefits cyber security and its use in protocols. Topics include cryptographically secure hash functions, pseudorandom numbers, key distribution techniques, secure authentication, and single sign-on. Detection and prevention of security threats such as covert communication, malicious code, and other security threats in protocols are included.

Fundamentals of Operating Systems Security— Focus on securing a Windows and/or Linux OS from an end-user perspective. Topics include OS security concepts and principles, vulnerabilities in ordinary systems, secure capability systems, information flow control, mandatory access control, security kernels, memory protection and management (including shared memory and virtual memory), file system, privileged access, virtual machine systems, compartmentalization, and distributed file systems and security.

Fundamentals of Cloud Security— This course provides ground-up coverage on the high-level concepts of the cloud landscape, architectural principles, techniques, design patterns, and real-world best practices applied to cloud service providers and consumers and delivering secure cloud-based services. The course will describe the cloud security architecture, explore the guiding security design principles, design patterns, industry standards, and applied technologies, and address regulatory compliance requirements critical to the design, implementation, delivery, and management of secure cloud-based services. The course delves deep into the secure cloud architectural aspects with regards to identifying and mitigating risks, protection, and isolation of physical and logical infrastructures—including compute, network and storage, comprehensive data protection at all OSI layers, end-to-end identity management and access control, monitoring and auditing processes and meeting compliance with industry and regulatory mandates. The course will leverage cloud computing security guidelines set forth by ISO, NIST, ENISA and Cloud Security Alliance (CSA).

Fundamentals of Software Security— This course will teach students the theories and tools used for secure software design, threat analysis, secure coding, and vulnerability analysis. The goal is to use these techniques and tools to improve and verify software designs and security. We will consider important software vulnerabilities and attacks that exploit them—such as buffer overflows and viruses—and we will consider defenses that prevent or mitigate these attacks, including advanced testing and program analysis techniques.

Fundamentals of Cybersecurity Scripting — A scripting language is used to automate the execution of tasks that would otherwise be performed individually by a human operator. The course will explain the difference between programming and scripting languages and how to write a script to perform tasks using scripting languages like java, python, PHP, and PowerShell. In the course, students will be provided an overview of how attackers use scripts to inject malicious code, and they will be taught how to detect and mitigate such attacks.

Fundamentals of Cyber Resilience— This course focuses on how to design systems and processes that can withstand a cyber breach. This course builds off the adversarial thinking course to help develop cybersecurity students' abilities to maintain business operations while under a cyber attack.

Fundamentals of Cyber-Physical and Critical Infrastructure Security – This course will provide an overview of the security challenges facing cyber-physical systems and critical infrastructure, including power, transportation, and other systems essential to modern society. Topics will include threat modeling, risk management, incident response, and the design and operation of secure systems. The course will apply adversarial thinking.

IOWA STATE UNIVERSITY
OF SCIENCE AND TECHNOLOGY

College of Engineering
Office of the Dean
4100 Marston Hall
Tel (515) 294-9988
wse@iastate.edu
www.engineering.iastate.edu

9 April 2024

To Whom It May Concern,

I am writing to express the strong support of the College of Engineering for the proposed Professional Certificate in Cybersecurity program, housed within the Department of Electrical and Computer Engineering. This program aligns perfectly with our university's strategic objectives and commitment to providing cutting-edge educational opportunities.

We understand the critical need for advanced cybersecurity education and are committed to supporting this initiative with the necessary resources. We have recently added a full-time Professor of Practice to this area and have plans for future hires, thus demonstrating our dedication to high-quality instruction in the area of Cybersecurity.

The Professional Certificate in Cybersecurity is a vital step towards bridging the knowledge gap in the field and equipping graduates with the skills required for today's demanding cybersecurity roles. We are excited about the potential of this program to contribute significantly to the field and to our students' futures.

Sincerely,

W. Samuel Easterling
James L. and Katherine S. Melsa Dean of Engineering

IOWA STATE UNIVERSITY
OF SCIENCE AND TECHNOLOGY

College of Engineering
Department of Electrical
and Computer Engineering
2215 Coover Hall
2520 Osborn Drive
Ames, IA 50011-1046
Phone: 515 294-2664

April 08, 2024

To whom it may concern

As the Chair of the Department of Electrical and Computer Engineering, I am delighted to extend our department's support for the newly proposed Professional Certificate in Cybersecurity. This program is a testament to our commitment to addressing the evolving needs of the cybersecurity workforce.

Our department is uniquely positioned to contribute significantly to this program. We maintain a state-of-the-art cybersecurity laboratory, which will play a crucial role in providing practical, hands-on experience to our students. Additionally, the curriculum has been carefully developed to align with federal training standards, ensuring our graduates are well-prepared to meet industry demands.

We are excited to work collaboratively with the university administration and other departments to ensure the success of this innovative program. Through this certificate, we aim to empower our students with the knowledge and skills necessary to excel in the rapidly growing field of cybersecurity.

Sincerely,

Ashfaq

Ashfaq Khokhar
Professor and Palmer Department Chair
(ashfaq@iastate.edu)

IOWA STATE UNIVERSITY | Ivy College of Business

Department of Information Systems
and Business Analytics
David and Deb Kingland Supply Chain
and Information Systems Suite
2340 Gerdin Business Building
2167 Union Drive
Ames, Iowa 50011-2027
515 294-3659

February 29, 2024

To: Doug Jacobson, University Professor, Dept. Electrical & Computer Engineering
From: Kevin P. Scheibe, Chair, Department of Information Systems and Business Analytics
RE: Professional Certificate in Cybersecurity

As the Information Systems and Business Analytics (ISBA) Department chair, I am pleased to extend our support for the new Professional Certificate in Cybersecurity. This initiative represents a significant step towards enhancing cybersecurity education and training, which is paramount in our increasingly connected world.

Although the ISBA Department is not providing specific resources to this program, we fully support its mission and goals. The integration of cybersecurity knowledge is vital for the future of information systems and business operations. We anticipate this program will be an excellent resource for students seeking to specialize in this critical area.

Sincerely,

Kevin Scheibe
Union Pacific Professor of Information Systems
Chair, Department of Information Systems and Business Analytics

Jacobson, Doug W [E CPE]

From: Rajan, Hridesh [COM S]
Sent: Saturday, April 6, 2024 12:02 PM
To: Jacobson, Doug W [E CPE]
Cc: Hallam, Arne [LAS]; Chaudhuri, Soma [COM S]
Subject: Proposed Professional Certificate in Cybersecurity program

Dear Dr. Jacobson,

On behalf of the ISU Department of Computer Science, I am writing to express our strong support for the proposed Professional Certificate in Cybersecurity program. We recognize the growing importance of cybersecurity in our digital world and believe this program is a step in the right direction for the field.

While the Computer Science Department is not contributing resources directly to this program, we do support its goals and the detailed curriculum that has been put together. We trust that the program will offer students valuable skills and knowledge, preparing them to meet the challenges of cybersecurity.

As courses in the program are developed, we would be interested in understanding how their similarities with some of the Computer Science courses could be of benefit, both to reduce efforts and to leverage commonalities. We wish you the best in getting this very important program approved and established.

Sincerely,
Hridesh

Dr. Hridesh Rajan
Kingland Professor and Department Chair
Department of Computer Science
Iowa State University
https://www.cs.iastate.edu/hridesh/
Support Computer Science

Academic Program Approval Voting Record

This document is to be appended as the last page of the proposal for any new or revised academic program to record the successive votes of approval as the proposal moves through its required review and approval steps. Consult Faculty Handbook Section 10.8 or the Faculty Senate Curriculum Committee website for information regarding Committee review and voting requirements for each action.

Curricular Action: (check appropriate boxes below)

1. X New Program □ Name Change □ Discontinuation □ Concurrent Degree for:
2. □ Undergraduate Major □ Graduate Major □ Undergraduate Minor □ Graduate Minor

   X Undergraduate Certificate □ Graduate Certificate □ Other: ____________________
3. Name of Proposed Change: Professional Certificate in Cybersecurity
4. Name of Contact Person: Doug Jacobson e-mail address: dougj@iastate.edu
5. Primary College: Engineering Secondary College: ____________________
6. Involved Department(s): Electrical and Computer Engineering

Voting record for this curricular action:

Voting Body	Votes			Date of Vote
	For	Against	Abstain	
ECE Department	30	0	0	3/1/2024
College Curriculum Committee	6	0	0	3/21/2024
College Approval Vote	110	2	8	4/9/2024
Faculty Senate Curriculum Committee	7	0	0	4/18/2024
Faculty Senate Academic Affairs Council	9	0	0	4/22/2024
Faculty Senate				

[FSCC – November 2013]