

**PROPOSED
UNDERGRADUATE CERTIFICATE PROGRAM
in
CYBERSECURITY and PRIVACY**

I. Basic Information

1. Institution: University of Georgia Date: February 09, 2021

2. School/College: Franklin College of Arts and Sciences

3. Department/Division: Department of Computer Science

4. Certificate Title (as it will appear in the *Bulletin*): Cybersecurity and Privacy

5. Level (undergraduate or graduate): undergraduate

6. Proposed starting date for program: Fall 2021

7. Abstract of the Certificate Program (for the University Council's agenda):

Purpose: The Computer Science Department is proposing the following new undergraduate certificate program in Cybersecurity and Privacy. This certificate would be useful primarily for undergraduate students in Computer Science, as well as some students in Mathematical Sciences and Engineering who aim to become experts in the growing field of Computer Security and Privacy.

Eligibility: Admission is open to undergraduate students across the university, but is specifically targeted towards undergraduate students in Computer Science, Data Science as well as related mathematical and engineering disciplines.

8. Letters of support with signatures: See attached letters.

II. Response to the Criteria for All Programs

1. Purpose and educational objectives:

- A) Purpose and objectives: The Computer Science Department is proposing a new undergraduate certificate program in Cybersecurity and Privacy. This certificate program would be useful for students in Computer Science, Data Science as well some students in Mathematical Sciences and Engineering. The certificate program aims to develop expertise in various aspects of computer security and privacy, such as networking, operating systems, network and systems security, and data and communications privacy. The need for expertise in the broad field of Cybersecurity and Privacy has grown tremendously in recent years.

The Forbes Magazine reports “Some estimate that between \$9 and \$21 trillion of global economic value creation could be at risk if companies and governments are unable to successfully combat cyber threats” (<http://www.forbes.com/sites/frontline/2015/07/13/why-cybersecurity-leadership-must-start-at-the-top/>). In addition, the US government has initiatives to expand cybersecurity education and expand the professional workforce, e.g., as part of the Comprehensive National Security Initiative, the executive branch has/will "begin a campaign to promote cybersecurity awareness and digital literacy from our boardrooms to our classrooms and begin to build the digital workforce of the 21st century." The proposed certificate program is intended to help provide a well-trained workforce to meet the increasing demand for cybersecurity experts in the modern economy.

2. There must be a demonstrated and well-documented need for the program:

Why this certificate program is necessary: Students majoring in Computer Science, Data science as well as related Mathematical and Engineering disciplines, would benefit from the proposed certificate program as new courses will be designed and existing courses will be restructured to include material that will support the certificate program. This is very consistent with the USG Cyber Security Initiative that will focus on all the cyber education and training resources across USG in order to meet the needs of the U.S. Army Cyber Command, the National Security Agency, the financial transaction processing industry and the health informatics/electronic medical records industry. The initiative aims to create a cybersecurity workforce of sufficient scale, quality, and capability to meet the needs of Georgia companies, military installations, government agencies and other institutions.

There is a great demand and opportunities for cybersecurity graduates. According to research from Cybersecurity Ventures, an estimated 3.5 million cybersecurity jobs will be unfilled by 2021, and of the candidates who apply, fewer than one in four are even qualified (<https://cybersecurityventures.com/jobs/>).

For more information please refer to: <http://gov.georgia.gov/press-releases/2014-12-10/deal-state-acts-high-demand-career-initiative-report>. Also note the report from Information Systems Audit and Control Association, Inc. (ISACA): “Cybersecurity skills are in high demand, as threats continue to plague enterprises around the world. An overwhelming

majority of students [surveyed](#) by ISACA recognizes this and plans to work in a position that requires cybersecurity knowledge. However, one in five report that their universities do not offer cybersecurity courses and less than half feel they will have the adequate skills and knowledge when they graduate” (<http://www.isaca.org/cyber/pages/cybersecurity-fundamentals-certificate.aspx>).

This proposed certificate is in line with the UGA strategic plan. The Computer Science Department is one of the few Departments on campus to receive an authorization to hire a tenure track Assistant Professor in the area of Data and Communications Privacy and a joint tenure-track Assistant Professor with Engineering on Secure Big Data.

B) Describe the expected stage of development:

1. Semester/Year of Program Initiation: Fall 2021
2. Semester/Year Full Implementation of Program: Fall 2021
3. Semester/Year First Certificates will be awarded: Spring 2022
4. Annual Number of Graduates expected (once the program is established): 10

Projected Future Trends for the number of students enrolled in the program: Expect continued growth based on the growth of our undergraduate majors from 441 in Fall 2013 to 1,148 in Fall. In addition, the number of Data Science majors is currently at 56, and Engineering majors is increasing as well.

3. Evidence of student demand for program sufficient to sustain reasonable enrollments:

Student interest in the program: In the Department of Computer Science (with over 1,150 majors and more than 200 minors), the current courses related to the certificate program have experienced increasing enrollments. Nationally, a large number of universities have started programs in Cybersecurity. At a national level, Cybersecurity programs are experiencing an undiminished and sustained upward trend. We have completed a formal survey of the undergraduate Computer Science majors, 162 responded, and found that 59%, 34%, 7% “definitely would”, “might”, “would not” consider pursuing a certificate in Cybersecurity, respectively.

- A) Diversity: The certificate program is expected to have diversity composition similar to those in the degree programs it draws from. Advertising and outreach to minorities will be included.

4. Design and curriculum of the program:

A) Detailed Curriculum:

Eligibility: Admission is open to currently enrolled undergraduate students across the university, but is specifically targeted towards undergraduate students in Computer Science, Data Science, and related Mathematical and Engineering disciplines.

Curriculum: Cybersecurity spans all aspects of computer systems and networks, from hardware, to software, to systems' architecture and design. To complete the undergraduate Certificate Program in Cybersecurity and Privacy students must complete **18-20** hours of undergraduate coursework with **8** hours of core courses, and **10-12** hours of elective coursework related to Cybersecurity and Privacy.

The proposed certificate requires students to first acquire the foundations of computer and network security, which will be achieved via two core courses: Computer Networks and Operating Systems. As security threats generally focus on attacking vulnerable computer systems and networks, these first two classes are foundational because they include key concepts on systems and network security that represent a pre-requisite to cybersecurity-specific courses. For instance, the Operating System course teaches concepts such as process isolation and access control. The Computer Networks course includes material related to the confidentiality, integrity, and authenticity of network communications. In addition, it teaches basic concepts related to Web security.

The mainstream cybersecurity class for beginning undergraduate students is CSCI 4250, whereas CSCI 4260 introduces foundational privacy topics.

The list of core and elective courses required for the proposed certificate is the following:

Core Courses (8 hours):

CSCI 4730 – Operating Systems or CSCI 4760 – Computer Networks
CSCI 4250 – Cyber Security or CSCI 4260 – Data Security and Privacy

Electives (10-12 hours) - choose additional courses from:

CSCI 4730 – Operating Systems
CSCI 4760 – Computer Networks
CSCI 4250 – Cyber Security
CSCI 4260 – Data Security and Privacy
CSCI 4270 – Introduction to Computer Forensics
CSCI 4720 - Computer Systems Architecture
CSCI 4780 – Distributed Computing Systems
CSCI 4960 - Faculty Mentored Research in Computer Science with Core ICSP faculty (2-4 hours)
MATH 4450 - Cryptology and Computational Number Theory

The course descriptions are listed below:

CSCI 4730 Operating Systems (4 hr)

Coverage of the key concepts in modern operating systems. Specific topics include process management, synchronization mechanisms, scheduling strategies, deadlock detection/avoidance, memory management, file systems, protection and security, and distributed systems. Concepts will be reinforced through programming projects using a realistic operating system.

Prereq: [(CSCI 4720 or CSEE 4280) and CSCI 2720].

CSCI 4760 Computer Networks (4 hr)

In-depth coverage of computer networks, including digital data transmission and encoding, layered protocol models, Internet protocol, Internet client-server software, and network design methodology.

Prereq: CSCI 2720 and (CSCI 2670 or CSEE 2220).

CSCI 4250 Computer Security (4 hr)

Basic concepts of computer security and the theory and current practices of authentication, authorization, and privacy mechanisms in modern operating systems and networks.

Prereq: CSCI 4730 or CSCI 4760.

CSCI 4260 Data and Communications Privacy (4 hr)

This course focuses on privacy issues related to data collection and analysis, and on private communications. Specifically, it will cover the foundations of privacy-preserving data analysis as well privacy-enhancing technologies that have been so far proposed to provide private and anonymous communications over the Internet.

The course will include the following topics: Applied cryptography, Secure Multi-party computation, Privacy-preserving data analytics, Privacy-enhancing technologies Confidential and anonymous communications, internet censorship and anti-censorship technologies.

Prereq: CSCI 1730.

CSCI 4270 – Introduction to Computer Forensics (4 hr)

The principles and practice of computer forensics. Topics include computer crime, software vulnerabilities, intellectual property, privacy issues, countermeasures, methods and standards for extraction, preservation, and deposition of legal evidence in a court of law.

Prerequisites: CSCI 4730/6730 or CSCI 4250/6250

CSCI 4720 Computer Systems Architecture (4 hr)

Functional components and structure of computing systems. Topics include principles of combinational and sequential logic, number systems and computer arithmetic, hardware subsystem design and test, I/O and memory subsystem principles and techniques, instruction set architecture and implementation, pipelining and system-level parallelism, interconnection networks, trends. Prereq: (CSCI 2670 or CSEE 2220) and CSCI 1730.

CSCI 4780 Distributed Computing Systems (4 hr)

The fundamental concepts in distributed computing and the practical techniques for building distributed systems. Topics include distributed computing models, naming, synchronization, replication and consistency, fault tolerance, and security. Widely deployed distributed systems are used as case studies. Students design, implement, and analyze prototype systems.

Prereq: (CSCI 2720 and CSCI 1730)

CSCI 4960 - Faculty Mentored Research in Computer Science with Core ICSP faculty (2-4 hours)

Content will vary in response to the interests, needs, and capability of the students and faculty involved. Individual, guided study in computer science.

An individual student or team of students will define the research question, the research methods, or in some cases both aspects of a project. The student understands and can explain how his/her part of the project contributes to a larger initiative. This may be accomplished through a thorough literature review of the research area. At the end of the semester, the student will reflect on their experience, interpret both processes and outcomes of research, and be able to articulate what he/she has learned and can identify how failures or successes may shape further research questions or goals. Students are required to submit a paper or a report on their findings, they will also acquire experience in scientific writing. To fulfill the requirements of the course, students will also be required to present their findings to a panel of faculty members or to present their research in the form of a poster at our annual CS Research Day.

This course/program fulfills the Experiential Learning Requirements for students with majors in Franklin College. To see if it satisfies the requirement for non-Franklin students, check <http://engage.uga.edu/>, and search under the Experiential Learning tab.

Prerequisites: Permission of Department

MATH 4450 - Cryptology and Computational Number Theory (3 hours)

Recognizing prime numbers, factoring composite numbers, finite fields, elliptic curves, discrete logarithms, private key cryptology, key exchange systems, signature authentication, public key cryptology. Prerequisite: MATH 4000.

These elective courses are related to Cybersecurity and Privacy as follows:

- Computer Systems Architecture is necessary to understand trusted computing platforms.
- Distributed Computing Systems includes fundamental concepts such as fault tolerance and the security of geographically distributed and complex systems.
- Operating Systems includes topics related to systems security, including OS kernel security.
- MATH 4450 is relevant due to the importance of encryption for the providing integrity and confidentiality of network communications and to enable private multi-party computation.

- Software Security and Cyber Forensics, Data and Communications Privacy, topics in Network and Security Systems, Computer Network Attacks and Defenses, and Cryptology and Computational Number Theory are all directly related to cybersecurity and privacy.

B) Model Programs and Curricula:

The following universities in the state of Georgia that offer certificates in Cybersecurity(<https://cybersecurityguide.org/states/georgia/>):

Augusta State University offers several different Certificates in Cybersecurity
 Columbus University offers certificate in Cybersecurity
 Georgia Institute of Technology offers a Cyber Security Certificate
 Georgia Southern University offers a Cyber Security Certificate
 Kennesaw State University offers a Certificate in Information Technology Security and an Undergraduate Certificate in Cybersecurity

The proposed certificate program in Cybersecurity and Privacy has 2 core courses and electives from Computer Science, and Mathematics. The proposed certificate is more rigorous than the above-mentioned certificates and it additionally offers courses on Privacy and Computer Forensics.

There are a number of other universities offering graduate and undergraduate certificates in Cybersecurity as well as full degree programs at the Master's and Doctoral levels.

- C) Program Accreditation:** The undergraduate Computer Science Degree program is accredited by the Accreditation Board for Engineering and Technology (ABET).

5. Faculty resources:

- A) Full-time faculty:** The current full-time faculty within the Department of Computer Science are sufficient to initiate the proposed certificate program. More than half of the department's faculty have taught the required and/or the elective courses for the certificate.

B) List of involved faculty:

- Ismailcem Budak Arpinar, Associate Professor, Ph.D., Middle East Technical University
- Brad Barnes, Senior Lecturer, Ph.D., University of Georgia
- Suchendra M. Bhandarkar, Professor, Ph.D., Syracuse University
- Liming Cai, Professor, Ph.D., Texas A&M University
- Michael Cotterell, Lecturer, Ph.D., University of Georgia

- Prashant Doshi, Professor, Ph.D., University of Illinois at Chicago
- Shelby H. Funk, Associate Professor, Ph.D., University of North Carolina
- Bill Hollingsworth, Senior Lecturer, Ph.D., University of Cambridge
- Maria Hybinette, Associate Professor, Ph.D., Georgia Institute of Technology.
- Le Guan, Assistant Professor,
- Manijeh Keshtgari, Lecturer,
- Mustakimur Rahman Khandaker, Assistant Professor
- In Kee Kim, Assistant Professor, Ph.D., University of Virginia
- Krzysztof J. Kochut, Professor, Ph.D., Louisiana State University
- Jaewoo Lee, Assistant Professor,
- Kyu Hyung Lee, Associate Professor, Ph.D., Purdue University
- Sheng Li, Assistant Professor,
- Tianming Liu, Professor, Ph.D., Shanghai Jiaotong University
- Chenglin Miao, Assistant Professor,
- John A. Miller, Professor, Ph.D., Georgia Institute of Technology
- Roberto Perdisci, Associate Professor, Ph.D. University of Cagliari
- Shannon Quinn, Assistant Professor, Ph.D., Carnegie-Mellon-University of Pittsburgh
- Lakshmish Ramaswamy, Professor, Ph.D.: Georgia Institute of Technology
- Khaled, Rasheed, Professor, Ph.D.: Rutgers University
- Eman Saleh, Lecturer,
- Thiab Taha, Professor and Head, Ph.D., Clarkson University
- Wenwen Wang, Assistant Professor,
-

Note: More detailed information about the listed Faculty above can be found at:
<https://cs.uga.edu/directory/regular-faculty>

Most of the above courses are taught by one or two of the above listed faculty and therefore, there will be no need to adjust their assignments unless the program expands by admitting a considerable number of students.

- C) Additional faculty: The department has 7 tenure-track faculty members whose core research areas are in Cybersecurity, Privacy, and Computer Forensics. There is no need for additional faculty.

6. Resources needed to support the program:

- A) Library resources: There is no need for additional library resources.
- B) Equipment: There is no need for additional equipment.

7. Physical facilities:

There is no need for additional physical facilities.

8. Expense to the institution:

- A) Funding to initiate the program (first three years): No amount of funding is needed for Years 1-3.
- B) Support for students: The program will not be providing assistantships.

9. Commitments of financial support:

- A) Sources of additional funds: Current funding through the Department of Computer Science will be sufficient to initiate and maintain the certificate program.
- B) Long-range plans: The Department was authorized in December 2020 to hire a Tenure-track Assistant Professor in Data Science. This new hire will teach courses relevant to this certificate.

10. Administration of the program:

The proposed undergraduate certificate in Cybersecurity and Privacy will be administered by the undergraduate Coordinator of the Computer Science Department as well as the Director of the Institute for Cybersecurity and Privacy. The administrators in conjunction with the Department Head will be responsible coordinating course offerings, maintaining student records, promoting activities, securing additional funding, and consulting with the department's curriculum committee regarding courses in the certificate program.

The semester before completing the certificate, students will be required to fill out a certificate completion form. The undergraduate certificate will be awarded to the student upon the completion of her/his undergraduate degree.



UNIVERSITY OF
GEORGIA

Department of Computer Science
415 Boyd Graduate Studies Research Center
200 D.W. Brooks Drive
University of Georgia
Athens, Georgia 30602-7404
TEL 706-542-2911 | FAX 706-542-2966
www.cs.uga.edu

Franklin College of Arts & Sciences
Department of Computer Science

Date: March 08, 2021

To: Dean Alan Dorsey/ Franklin College

From: Thiab Taha, Professor and Head

RE: Proposal for an Undergraduate Certificate in Cybersecurity and Privacy

Dear Dean Dorsey,

The Department of Computer Science in the Franklin College fully supports the proposal for an interdisciplinary Undergraduate Certificate in Cybersecurity and Privacy.

The departmental vote on 03/08/2021 was unanimous in support of the proposal and it has my full support as well.

This certificate program would be useful for students from a variety of disciplines; in particular, computer and mathematical sciences, data science, and engineering. The certificate program aims to develop expertise in various aspects of computer security and privacy, such as systems and software security, network security and data privacy.

We believe that this program is timely and will have a very positive impact on the state security and economy by having skillful workforce in this area upon graduation.

Thank you for your consideration.

Best regards,

Thiab Taha
Professor and Head
Computer Science Department