Date Submitted: 12/12/25 1:32 pm

Viewing: BS-CCSE : Bachelor of Science in Computer and Cybersecurity Engineering

Last approved: 03/12/25 5:28 pm

Last edit: 12/12/25 1:32 pm

Changes proposed by: catino

Catalog Pages Using this Program

Bachelor of Science in Computer and Cybersecurity Engineering

Program Status	Active			
Requestor	Name	Joanette Catino	E-mail	
Origination Date	2025-12-12 ~~2025-2-19~~			
Is this an interdisciplinary program?	No			
Is this an incubator program?				
Is this stem-eligible?	Yes			
Available for direct application?	Yes			
Academic Unit College	Electrical & Computer Engrg Armour College of Engineering			
Program Title	Bachelor of Science in Computer and Cybersecurity Engineering			
Effective Academic Year	2026 ~~2025~~ - 2027 ~~2026~~		Effective Term	Summer 2026
Academic Level	Undergraduate			

In Workflow

1. EECE Chair
2. Academic Affairs
3. Undergraduate Academic Affairs
4. AC Dean
5. Undergraduate Studies Committee Chair
6. Faculty Council Chair
7. Academic Affairs

Approval Path

1. 12/12/25 1:48 pm Erdal Oruklu (oruklu): Approved for EECE Chair
2. 12/15/25 3:31 pm Ayesha Qamer (aqamer): Approved for Academic Affairs
3. 12/15/25 3:38 pm Joseph Gorzkowski (jgorzkow): Approved for Undergraduate Academic Affairs
4. 12/16/25 7:40 am Louis Cattafesta III (lcattafestaiii): Approved for AC Dean

History

1. May 25, 2018 by Sarah Pariseau (sparisea)
2. May 25, 2018 by Sarah Pariseau (sparisea)

3. May 30, 2018 by Sarah Pariseau (sparisea)
4. Jun 13, 2018 by Joanette Catino (catino)
5. Jun 22, 2018 by Sarah Pariseau (sparisea)
6. Jun 22, 2018 by Sarah Pariseau (sparisea)
7. Oct 11, 2018 by Sarah Pariseau (sparisea)
8. Apr 22, 2022 by Joanette Catino (catino)
9. Mar 15, 2023 by Joanette Catino (catino)
10. Mar 12, 2025 by Joanette Catino (catino)

If all courses in a subject in your department are required, please enter each subject followed by the number ranges in the "Quick Add" field in the pop up box when you click the green plus button below. For example: ARCH 100-499.

What courses will factor the major GPA?

Program Type	Degree
Degree Type	Bachelor of Science (BS)

CIP Code

14.0999 - Computer Engineering, Other.

Is there more than one Academic Unit proposer?

No

Program Code	BS-CCSE

Program Attribute

Total Program Credit Hours	133

Please provide a summary and rationale for the requested program revision.

Removed an optional CS course ~~Updated with voted on curriculum changes~~

Program Narrative and Justification

Narrative description of how the institution determined the need for the program. For example, describe what need this program will address and how the institution became aware of that need. If the program is replacing a current program(s), identify the current program(s) that is being replaced by the new program(s) and provide details describing the benefits of the new program(s). If the program will be offered in connection with, or in response to, an initative by a governmental entity, provide details of that initiative.

Bachelor of Science in Computer and Cybersecurity Engineering (CCSE) is a degree program that prepares students for an engineering career that involves design and application of secure and resilient computer hardware and software systems. This is a unique program that combines computer engineering and cybersecurity topics into one major. The program emphasizes the cybersecurity engineering of cyber-physical systems which are becoming more prevalent every day. It is concerned with detection and elimination of vulnerabilities and safe operation of Internet of Things, cloud computing, healthcare, smart/micro grid power systems, computer networks, and wireless communications.

Joint Task Force on Cybersecurity Education defines cybersecurity discipline as "A computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management.

Therefore, CCSE students must also know about human factors, ethical issues, and law in addition to the detailed knowledge of secure hardware/software components to design and build systems for security applications. CCSE program is built on a very strong computer engineering program within the ECE department and is tailored to expand knowledge to counter cyber threats by providing both theoretical fundamentals and actual implementation of cyber infrastructure. Interdisiplinary component of the program is satisfied with the courses that CCSE students can select from the Department of Computer Science and Chicago-Kent School of Law.

Narrative description of how the program was designed to meet local market needs, or for an online program, regional or national market needs. For example, indicate if Bureau of Labor Statistics data or State labor data systems information was used, and/or if State, regional, or local workforce agencies were consulted. Include how the course content, program length, academic level, admission requirements, and prerequisites were decided; including information received from potential employers about course content; and information regarding the target students and employers.

All major industries such as defense, energy, finance, transportation, infrastructure, healthcare are impacted by cybersecurity challenges. There is great need for educated workforce who can help build the safety measures, protect all forms of digital assets, and also understand ethical and legal issues in cybersecurity. However, cybersecurity job market is still straining to find enough trained workers. Demand for talent in the cybersecurity job market outstrips the supply of available workers. U.S. Department of Labor's outlook for "Information Security Analysts" predicts growth by 28% for years 2016-2026. In fact, according to Burning Glass data, Chicago metropolitan area had 10,670 cybersecurity job openings during the 12-month period that ended in September 2017 which was among the highest in large metropolitan areas.

Clearly, cybersecurity education is an important opportunity for Illinois Institute of Technology to attract highly qualified students interested in science and engineering. It is essential to provide a carefully designed, rigorous degree program which can establish IIT as a leading cybersecurity institution. The ECE department has substantial critical mass and resources to achieve this goal. Multiple tenured/tenure track faculty are directly involved in research related to cybersecurity topics and their research has been funded by federal agencies and industry. ECE research on security topics cover a broad spectrum, including cloud computing, healthcare and body area networks, secure networking protocols, cryptography, smart grid power systems and big data. In addition to funded research and graduate theses and dissertations, ECE has been offering cybersecurity courses at both undergraduate and graduate levels. Overall, ECE is ready and well-poised for a new degree program addressing the curriculum challenges identified by the Joint Task Force on Cybersecurity Education (JTF is a collaboration between major international computer societies: Association for Computing Machinery, IEEE Computer Society, Association for Information Systems Special Interest Group on Security, and International Federation for Information Processing Technical Committee on Information Security Education.).

With the introduction of the CCSE degree, ECE department will be able to recruit students who want to be engineers while focusing on cybersecurity. We anticipate total enrollment in ECE programs will increase gradually with the CCSE degree. This may also boost the ECE graduate programs (including a potential Master of Cybersecurity Engineering degree which is under preparation) and result in higher visibility and healthy growth for the ECE department.

One of the potential challenges for UG Admission would be to distinguish the multiple cybersecurity programs offered across multiple colleges at IIT. ECE department will prepare and provide marketing materials for UG Admission, emphasizing the engineering focus with the proposed cybersecurity program. ECE department will also collaborate with other departments to coordinate IIT's push for leadership in cybersecurity education. Our open house and recruitment events will highlight ECE faculty's research projects related to the cybersecurity fields.

Narrative description of any wage analysis the institution may have performed, including any consideration of Bureau of Labor Statistics wage data related to the new program.

According to the Bureau of Labor Statistics, the Greater Chicago area has the fifth highest employment of information security analysts with an annual mean wage of $97,320. Furthermore, Illinois has several major firms listed in the top 500 hottest cybersecurity companies, based on the Cybersecurity Ventures report in 2017. Among them are Cimcore (#75) at Chicago; NowSecure (#124) at Oak Park; Trustwave (#157) at Chicago; Flexera Software (#174) at Itasca; Kenna (#338) at Chicago and MailControl (#404) at Chicago. Multiple Fortune 500 companies in Illinois such as Boeing, United, State Farm, Abbot Laboratories, Caterpillar Inc., etc. are increasingly needing cybersecurity professionals to prevent security breaches and provide security protection for their customers.

ECE department will work closely with the Career Management Center to provide the CCSE program details and highlight the potential companies and industry liaisons.

Narrative description of how the program was reviewed or approved by, or developed in conjunction with, one or more of the following: a) business advisory committees; b) program integrity boards; c) public or private oversight or regulatory agencies (not including the state licensing/authorization agency and accrediting agency); and d) businesses that would likely employ graduates of the program. For example, describe the steps taken to develop the program, identify when and with whom discussions were held, provide relevant details of any proposals or correspondence generated, and/or describe any process used to evaluate the program.

Admission Entry Details

What are the enrollment estimates?

Year 1	20	Year 2	25	Year 3	25

Attach Additional Program Justification Document(s)

Academic Information

Advising

Since quality advising is a key component of good retention, graduation, and career placement, how will students be mentored? What student professional organizations will be formed? How will the department work with the Career Services office to develop industry connections?

Existing advising procedures and strategies in the ECE department will continue in this new degree program. Each student will have an academic adviser assigned in their first semester. Mandatory advising meetings will be enforced. For CCSE degree students, advising faculty will be selected among those that have expertise in cybersecurity, cyber-physical systems, internet of things, and computer networks. About half of the current ECE faculty can be considered in this category. With potential enrollment of 25 students in CCSE, advising load for each faculty member will be feasible.

CCSE students can benefit from multiple student organizations that already exist within the ECE department, including the IIT chapter of the world's largest professional organization, IEEE, and its honor society Eta Kappa Nu. These are well-established and well-run student organizations that are attractive for students who are interested in cybersecurity topics.

Program Resources

Which program resources are necessary to offer this program?

Proposed Catalog Entry

Admission Requirements

Course Requirements

Curriculum

Required Courses

Computer and Cyber Security Engineering Requirements		(47)
ECE 100	Introduction to the Profession I	3
ECE 211	Circuit Analysis I	3
ECE 213	Circuit Analysis II	4
ECE 218	Digital Systems	4
ECE 222	Introduction to Cybersecurity Engineering	3
ECE 242	Digital Computers and Computing	3

ECE 308	Signals and Systems	3
ECE 311	Engineering Electronics	4
ECE 407	Introduction to Computer Networks with Laboratory	4
ECE 441	Smart and Connected Embedded System Design	4
ECE 443	Introduction to Computer Cyber Security	3
ECE 444	Computer Network Security	3
ECE 485	Computer Organization and Design	3
ITMS 478	Cyber Security Management	3
Computer Science Major Requirements		**(16)**
CS 115	Object-Oriented Programming I	2
CS 116	Object-Oriented Programming II	2
CS 330	Discrete Structures	3
CS 331	Data Structures and Algorithms	3
CS 351	Systems Programming	3
CS 450	Operating Systems	3
Cybersecurity Math Elective		**(3)**
Choose one from the following courses:		3
MATH 333	Matrix Algebra and Complex Variables	3
MATH 350	Introduction to Computational Mathematics	3
MATH 410	Number Theory	3
MATH 454	Graph Theory and Applications	3
Cybersecurity Software Engineering Elective		**(3)**
Choose one from the following courses:		3
ECE 448	Application Software Design	3
ECE 449	Object-Oriented Programming and Machine Learning	3
ECE 473	Cloud Computing and Cloud Native Systems	3
ECE 474	Data Science for Engineers	3
Cybersecurity Technical Elective		**(3)**
Choose one from the following courses:		3
ECE 497	Special Problems	3
ECE 586	Hardware Security and Advanced Computer Architectures	3
ITMS 428	Database Security	3

ITMS 446	Active Cyber Defense	3
Cybersecurity Law Elective		**(2-3)**
Select two to three credit hours from the following courses:		2-3
LAW 252	Law of Privacy	3
LAW 285	Cyber Fraud-Priv Class Actions	2
LAW 295	Data Privacy and Security	2
LAW 379	Blockchain and the Law	2
LAW 478	Computer & Network Privacy	3
Mathematics Requirements		**(21)**
MATH 151	Calculus I	5
MATH 152	Calculus II	5
MATH 251	Multivariate and Vector Calculus	4
MATH 252	Introduction to Differential Equations	4
MATH 374	Probability and Statistics for Electrical and Computer Engineers	3
Physics Requirements		**(8)**
PHYS 123	General Physics I: Mechanics	4
PHYS 221	General Physics II: Electricity and Magnetism	4
Chemistry Requirement		**(3)**
CHEM 122	Principles of Chemistry I	3
Interprofessional Projects (IPRO)		**(6)**
See Illinois Tech Core Curriculum, section E		6
Humanities and Social Sciences Requirements		**(21)**
See Illinois Tech Core Curriculum, sections B and C		21
Total Credit Hours		133-134

Minimum degree credits required: 133

Sample Curriculum/Program Requirements

Bachelor of Science in Computer and Cybersecurity Engineering Curriculum

Year 1

Semester 1	Credit Hours	Semester 2	Credit Hours
ECE 100	3	MATH 152	5
MATH 151	5	PHYS 123	4
CHEM 122	3	CS 116	2
CS 115	2	Social Sciences Elective	3
Humanities 200-level	3	ECE 222	3
	16		17

Year 2

Semester 1	Credit Hours	Semester 2	Credit Hours
MATH 252	4	MATH 251	4
PHYS 221	4	ITMS 478	3
ECE 211	3	ECE 213	4
ECE 218	4	ECE 242	3
CS 331	3	CS 330	3
	18		17

Year 3

Semester 1	Credit Hours	Semester 2	Credit Hours
ECE 308	3	CS 450	3
ECE 311	4	ECE 407	4
CS 351	3	MATH 374	3
ECE 443	3	IPRO Elective I	3
Humanities Elective (300+)	3	Social Sciences Elective (300+)	3
	16		16

Year 4

Semester 1	Credit Hours	Semester 2	Credit Hours
Cybersecurity Software Eng. Elective [1]	3	ECE 441[3]	4
ECE 485	3	Cybersecurity Technical Elective[4]	3
Cybersecurity Math Elective [2]	3	ECE 444	3
IPRO Elective II	3	Cyber Security Law Elective[5]	2-3
Additional Hum. or Soc. Sci. Elective	3	Social Sciences Elective (300+)	3
Humanities (300+)	3		
	18		15-16

Total Credit Hours: 133-134

1 Cybersecurity Software Engineering Elective: Choose from the following courses: ECE 448, ECE 449, ECE 473, or ECE 474

2 Cybersecurity Math Elective: Choose from the following courses: MATH 333, MATH 350, MATH 410 or MATH 454

3 Major Design Experience (M) course.

4 Cybersecurity Technical Elective: Choose from the following courses: ECE 497, ECE 586, ITMS 428, or ITMS 446. ECE 497 Special Problems project needs to cover a Cybersecurity related topic.

5 Cybersecurity Law Elective: Choose from the following courses: LAW 252, LAW 285, LAW 295, LAW 379 or LAW 478.

Specialization Requirements

Program Outcomes and Assessment Process

What are your learning objectives in this program? Please list each learning objective in the boxes below:

Note: These should be the same as described in your assessment plan at the bottom of this form.

Upload your assessment plan here:

Undergraduate Program Requirements

What courses will factor the major GPA?

Undergraduate Degree Requirements

Minimum credit hours	133
Specialization required?	

No

Minor required?

No

Proposed General Curriculum

List Major Course Requirements

List Mathematics Requirements

List Science Requirements

List Computer Science Requirements

List Humanities and Social Sciences Requirements

List Interprofessional Project (IPRO) Requirements

List Technical Elective Course Options

List Free Elective Credit Hours (if applicable)

Semester-by-semester plan of study for the degree program

Report to Faculty Council

Reviewer Comments

Key: 440