Program Approval

I. General Information

A. Institution University of Kansas

B. Program Identification

Degree Level:	Bachelor's
Program Title:	Cybersecurity Engineering
Degree to be Offered:	Bachelor of Science
Responsible Department or Unit:	School of Engineering
CIP Code:	11.1003
Modality:	Face-to-Face
Proposed Implementation Date:	Spring 2024

Total Number of Semester Credit Hours for the Degree: **126**

II. Clinical Sites: Does this program require the use of Clinical Sites? No

III. Justification

Cybersecurity is by any measure of great importance in today's world in protecting data, computer systems, and networks from unauthorized access and destruction. The global economy loss to cybercrime in 2021 is estimated to be between $600 billion to 6 trillion. Protecting information systems is key to protecting the nation's critical infrastructures including government entities, health institutions, banking, e-commerce, and academia.

A well-trained workforce is needed to protect the vital information resources from various attacks. With the growing interest from employers in business, industry, and governmental agencies, we recognize the need for an enhanced training in information security from both theoretical and practical aspects at the undergraduate level.

The proposed degree program is designed to provide undergraduate students with knowledge of information security concepts, cryptography, information and network security, and computer systems security. The curriculum for the proposed degree program will incorporate hands-on labs, capstone projects, and real-world system experiences that provide students practical skills for participating in the national security workforce. The program will provide opportunities for undergraduate research. The purpose of this program is to offer a credential that covers both the theoretical and practical aspects of cybersecurity to students who are pursuing cybersecurity as a profession.

The University of Kansas's Department of Electrical Engineering and Computer Science (EECS) has been designated as a National Center for Academic Excellence in Cyber Defense Education (CAE-CDE) and Research (CAE-R) by the National Security Agency (NSA). According to the National CAE Institution Map (2023), KU is one of 45 institutions nationwide to hold both CAE-CD and CAE-R designations. KU is the only institution in the State of Kansas to receive dual designations, and one of the first institutions in Kansas to receive CAE-CD designation (2009).

The EECS department has successfully offered the Undergraduate Certificate in Cybersecurity since 2019. The department offers a diversified set of cybersecurity courses that cover a wide range of topics including cryptography and theoretical modeling, system synthesis and verification, network and database security, anonymity and privacy, and security management. These courses support a nationally recognized cybersecurity externally funded research program. A unique strength of KU's cybersecurity education and research program is its broad spectrum of research activity: from theory to application, from hardware and cyber-physical systems to software and information systems, and to physical-layer communication security to resilient and survivable

networks. The University of Kansas, the School of Engineering, and the EECS department are all committed to making continuous investments to expand cybersecurity education and research capacities.

IV. Program Demand

Market Analysis & Request for Accreditation

The following universities offer Cybersecurity programs in Kansas, and none are accredited:

- Rasmussen University – Overland Park, Topeka (for-profit private university): BS in Cybersecurity
- National American University – Overland Park, Wichita East, Wichita West (for-profit private university): emphasis in Cybersecurity and Forensics in BS in Information Technology
- Fort Hays State University: cybersecurity concentration in BA/BS in Information Networking & Telecommunications
- Kansas State University: BS in Cybersecurity
- Wichita State University: BS in Cybersecurity
- University of Kansas, School of Professional Studies: BAS in Applied Cybersecurity

A search using the Accreditation Board of Engineering and Technology's (ABET) Accredited Program Search tool (search by category) indicates it only accredits 21 computer-focused cybersecurity bachelor's programs in the US through its Computer Accreditation Commission. Of these, only four are in the central plains region – all located in Missouri: the University of Central Missouri, Fontbonne University, Southwest Baptist University, and Southeast Missouri State University. K-State's degree – approved by KBOR in April 2022 - is computer-science based and the school indicated in its proposal it would pursue accreditation through ABET.

This proposal is distinct from other programs in Kansas/Central Plains because it would be the sole engineering-based cybersecurity degree in the state/region and thus designed to meet accreditation requirements through ABET's Engineering Accreditation Commission (as opposed to the Computer Accreditation Commission). KU is at the forefront of the cybersecurity engineering discipline since ABET only accredits three cybersecurity engineering programs in the US at the bachelor's level through its Engineering Accreditation Commission This was determined via a search by category using ABET's Accredited Program Search tool. These programs are at Iowa State University, Louisiana Tech University, and George Mason University.

The ABET Engineering Accreditation Commission (EAC) sets a worldwide standard that "assures confidence that a collegiate program has met standards essential to prepare graduates to enter critical STEM fields in the global workforce," and provides a certificate of international recognition of the quality of the program. ABET accreditation is essential for the degree to be recognized by the students and employers. Therefore, **KU is also requesting approval to seek ABET accreditation for this program. Accreditation costs are included in the financial table in this proposal.**

Furthermore, KU's cybersecurity engineering degree is designed to meet standards by two national centers located at the U.S. Department of Defense's National Security Agency (NSA): the National Center for Academic Excellence in Cyber Defense Education (CAE-CDE) and the National Center for Excellence in Cyber Research (CAE-R). As noted earlier, KU is one of only 45 institutions in the nation to hold both CAE-CD and CAE-R designations, and the only institution in the central plains that would have a cybersecurity engineering degree that meets standards set by CAE-CD, CAE-R, and ABET's Engineering Commission.

The multifaceted elements described below form a strong foundation to support the EECS department's strengths and activities in cybersecurity:

- EECS is 1 of only 6 Science of Security Lablets funded by National Security Agency to conduct foundational research in cybersecurity. The other lablets are at Vanderbilt, Berkley, Carnegie Mellon

University (CMU), University of Illinois—Urbana Champaign (UIUC) and North Carolina State. The Lablet holds annual workshops, which includes tutorials and EECS student presentations. The keynote speakers include Brigadier General Jennifer Buckner, U.S. Army Director of Cyber, Electronic Warfare, Information Operations and the chief information security officer for Cboe Global Markets. Students pursuing KU's Cybersecurity Engineering degree will have the opportunity to participate in these kinds of enhancement activities.

- Cybersecurity research in EECS has been supported by government agencies and industry partners, including NSA, Defense Advanced Research Projects Agency (DARPA), National Science Foundation (NSF), Air Force Research Laboratory (AFRL), National Aeronautics and Space Agency (NASA), Ripple, and Honeywell National Security Campus. Of note Professor Alexandru Bardas just received an NSF Career Award for cybersecurity research.
- Since 2016 KU hosted GenCyber Summer Camps for Teachers sponsored by NSA/NSF. This outreach activity brings 25-30 K-12 teachers to campus every summer to help them teach young students about cybersecurity. This is significant outreach activity that has proven to be sustainable completely with external funding.
- EECS faculty drove the establishment of Kansas Applied Research Lab (KARL), opening up new avenues for research supported from federal resources, especially DoD. The KARL is a unique platform to provide undergraduate research opportunities.
- EECS's CyberCorps: Scholarship for Service program (Jayhawk SFS) provides scholarships for cybersecurity education. SFS is supported by a $4.7 million, five-year grant from the National Science Foundation. Jayhawk SFS program provides scholarship opportunities for students pursuing a BS in Cybersecurity Engineering.
- KU's Information Security Club (the "Jayhackers") is a competition-based student group that focuses on learning security concepts through Collegiate Cyber Defense competitions. This group travels to competitions representing EECS and enhancing our reputation in this field.

The EECS department first offered the Undergraduate Certificate for Cybersecurity in Spring 2020. We have seen steady growth of student matriculation with 12 awards since inception and 16 students have applied to matriculate with this certificate in the Spring of 2023. Spring 2023 headcount for the certificate is 43 students.

In 2009, the EECS Department was designated a National Center for Academic Excellence in Cyber Defense Education (CAE-CDE). As part of this designation, the EECS department has offered several core cybersecurity courses since 2009. Three examples of courses that are presently offered through our curriculum are EECS 465 (Cyber Defense) which enrolled 50 students in the Spring of 2023, EECS 563 (Introduction to Communication Networks) which enrolled 74 students in Fall 2022, and EECS 565 (Introduction to Information & Computer Security) which enrolled 56 students in the Spring of 2023.

V. Projected Enrollment for the Initial Three Years of the Program

Year	Total Headcount Per Year		Total Sem Credit Hrs Per Year	
	Full- Time	Part- Time	Full- Time	Part- Time
Implementation	15	0	450	0
Year 2	25	0	750	0
Year 3	35	0	1050	0

VI. Employment

According to the 2022 Cybersecurity Workforce Demand Factsheet from the National Institute of Standards and Technology (2023), the global shortage of cybersecurity professionals was estimated to be 2.72 million. A U.S. Commerce Department sponsored project shows that there were 597,767 open positions in cybersecurity from

October 2020 through September 2021, while the number of workers employed in cybersecurity-related jobs during the same period was estimated to be 1,053,468. There were 3,849 unfilled cybersecurity positions in the State of Kansas as of September 2021 (10,120 in Missouri), with a supply/demand ratio of 76%, i.e., a 24% gap. There are 4,213 unfilled cybersecurity positions in the KC metro area, with an even lower supply/demand ratio of 75%. The U.S. Bureau of Labor Statistics projects the employment of information security analysts to grow 35% from 2021 to 2031 (the projection was 31% from 2019 to 2029), and rates the growth as "much faster than average".

In addition to major technologies in Kansas, e.g., Cerner, Garmin, T-Mobile, and Honeywell "There are 777 tech companies that I know of, and more than 250 startups in the KCMO/ Kansas area," Brian McClendon Dec 7, 2021, from "Former Google, Uber exec joins maker of Pokémon Go" — and he's building a team of developers in Lawrence. Each of these companies need cybersecurity expertise.

From experiences in the GenCyber Cybersecurity Summer Camps, the student's interests in cybersecurity and the number of Cyber Patriot teams in the state of Kansas and the KC metro area have grown exponentially.

VII. Admission and Curriculum

A. Admission Criteria

The freshmen application process and admission requirements will mirror those of the current B.S. degree programs in the EECS department:

- Must be admissible to the University of Kansas by assured admissions or individual review AND
- Have a 3.0+ high school GPA AND
- Demonstrate mathematics preparedness by:
    - Obtaining a mathematics ACT score of 28+ (or math SAT score of 660+), OR
    - Achieving a 'C' or better in a high school calculus course; OR
    - Earning credit via IB or AP credit for the above-mentioned course in accordance with KU placement credit requirements; OR
    - Achieving at minimum a qualifying score for MATH 125 on the ALEKS mathematics placement exam.
- Important: Simply meeting these requirements will not guarantee admission to EECS

Transfer Student Admissions:

- Applications from all transfer students, whether from other institutions or from within KU, are evaluated on a case-by-case basis.
- Have a grade-point average above 2.5 in college courses.
- Submit mathematics ACT or SAT scores or proof of competence in calculus (C or higher).

B. Curriculum

Year 1: Fall **SCH = Semester Credit Hours**

Course #	Course Name	SCH
EECS 101	New Student Seminar	1
EECS 168	Programming I	4
MATH 125	Calculus I (KU Core 1.2)	4
GE21	KU Core: Written Communication I	3
GE22	KU Core: Oral Communication	3

Year 1: Spring

Course #	Course Name	SCH
EECS 140	Introduction to Digital Logic Design	4
EECS 268	Programming II	4
MATH 126	Calculus II	4
GE21	KU Core: Written Communication II	3

Year 2: Fall

Course #	Course Name	SCH
EECS 210	Discrete Structures	4
EECS 348	Software Engineering I	4
MATH 127	Calculus III	4
EPHX 210	General Physics I for Engineers (KU Core GE 1.1)	3
PHSX 216	General Physics I Laboratory	1

Year 2: Spring

Course #	Course Name	SCH
EECS 330	Data Structures and Algorithms	4
EECS 388	Embedded Systems	4
MATH 290	Elementary Linear Algebra	2
AE41	KU Core: Diversity, Global Awareness	3
GE3N	KU Core: Natural Science	3

Year 3: Fall

Course #	Course Name	SCH
EECS 461	Probability & Statistics	3
EECS 465	Cyber Defense	3
EECS 678	Introduction to Operating Systems	4
PHIL 375	Moral Issues in Computer Technology (KU Core GE 5.1)	3
GE3H	KU Core: Arts/Humanities	3

Year 3: Spring

Course #	Course Name	SCH
EECS 563	Introduction to Communication Networks	3
EECS 565	Introduction to Information & Computer Security	3
Additional Math/Science	Additional math and natural science requirement	3
EECS Elective	Required EECS Elective	3
GE3S	KU Core: Social Science	3

Year 4: Fall

Course #	Course Name	SCH
EECS 569	Computer Forensics	3
EECS 581	Software Engineering II	3
EECS 677	Software Security Auditing	3
EECS Elective	Required EECS Elective	3
CYEN Elective	Required Cybersecurity Engineering Elective	3

Year 4: Spring

Course #	Course Name	SCH
EECS 592	Cybersecurity Design (KU Core 6)	3
EECS 695	Software Reverse Engineering	3
CYEN Elec	Required Cybersecurity Engineering Elective	3
CYEN Elec	Required Cybersecurity Engineering Elective	3
Professional Elective	Required Professional Elective course	3
AE42	KU Core: Diversity, Global Awareness (Goal 4.2)	3

Total Number of Semester Credit Hours …….. 126

C. Request to Exceed 120 Hours

ABET offers a more rigorous Cybersecurity Engineering accreditation through its Engineering Accreditation Commission (EAC) and a less rigorous Cybersecurity accreditation through its Computing Accreditation Commission (CAC). The ABET EAC requires *all* engineering programs (Electrical, Mechanical, Civil, Cybersecurity, etc.) to have at least 30 hours of math and science, whereas the CAC requires only 6 such hours for its less rigorous Cybersecurity category. KU is seeking the more rigorous ABET EAC accreditation for this Cybersecurity Engineering program, and is also seeking to maintain its CAE-CD and CAE-R program designations. All ABET EAC accredited programs in the KBOR system (Electrical, Mechanical, Civil, etc.) exceed 120 credit hours due to the rigorous EAC standards. Nationwide, there are only three ABET EAC accredited Cybersecurity Engineering programs: George Mason University (126 credits), Iowa State University (125 credits), and Louisiana Tech (128 credits).

VIII. Core Faculty

Note: * Next to Faculty Name Denotes Director of the Program, if applicable
FTE: 1.0 FTE = Full-Time Equivalency Devoted to Program

Faculty Name	Rank	Highest Degree	Tenure Track Y/N	Academic Area of Specialization	FTE to Proposed Program
Perry Alexander	Distinguished Professor	PhD	Y	Formal verification and synthesis, trusted systems, and programming language semantics.	.10
Alexandru Bardas	Assistant Professor	PhD	Y	Cybersecurity from a systems perspective, moving target defenses, enterprise network security.	.30
Drew Davidson	Assistant Professor	PhD	Y	System security, secure design, mobile and embedded software program analysis	.20
Morteza Hashemi	Assistant Professor	PhD	Y	Communication systems and networks, network analysis, measurement and simulation	.10
Tamzidul Hoque	Assistant Professor	PhD	Y	Trust verification of hardware, hardware IP protection, trust assurance for COTS IC, FPGA security	.10
Prasad Kulkarni	Professor	PhD	Y	Software security, software	.20

				performance, compiler optimizations, virtual machines and runtime systems	
Fengjun Li	Associate Professor	PhD	Y	Trustable and privacy-preserving federated learning, adversarial machine learning, IoT security and privacy	.20
Bo Luo	Professor	PhD	Y	Trustworthy machine learning, information and system security, IoT/CPS and hardware-enabled security, privacy in online social networks	.30

Number of graduate assistants assigned to this program **4**

IX. Expenditure and Funding Sources

A. EXPENDITURES	First FY	Second FY	Third FY
Personnel – Reassigned or Existing Positions			
Faculty (1.5 Existing FTE)	$180,213	$185,619	$191,187
Administrators *(other than instruction time)*	$6,037	$6,218	$6,404
Graduate Assistants	$40,000	$41,200	$42,436
Support Staff for Administration (*e.g., secretarial*)	$9,200	$9,476	$9,760
Fringe Benefits *(total for all groups)*	$73,207	$75,403	$77,665
Other Personnel Costs	0	0	0
Total Existing Personnel Costs – Reassigned or Existing	$308,657	$317,916	$327,452
Personnel – New Positions			
Faculty	0	0	0
Administrators *(other than instruction time)*	0	0	0
Graduate Assistants	0	0	0
Support Staff for Administration (*e.g., secretarial*)	0	0	0
Fringe Benefits *(total for all groups)*	0	0	0
Other Personnel Costs	0	0	0
Total Existing Personnel Costs – New Positions	0	0	0
Start-up Costs - One-Time Expenses			
Library/learning resources	0	0	0
Equipment/Technology	0	0	0
Physical Facilities: Construction or Renovation	0	0	0
ABET Initial Accreditation	0	$3,350	0
Total Start-up Costs	0	$3,350	0

Operating Costs – Recurring Expenses			
Supplies/Expenses	0	0	0
Library/learning resources	0	0	0
Equipment/Technology	0	0	0
Travel	0	0	0
Other – Annual ABET fee	0	0	$715
Total Operating Costs	0	0	$715
GRAND TOTAL COSTS	$308,657	$321,266	$328,167

B. FUNDING SOURCES *(projected as appropriate)*	Current	First FY (New)	Second FY (New)	Third FY (New)
Tuition / State Funds		$151,200	$252,000	$352,800
Student Fees		$42,750	$71,250	$99,750
Other Sources				
GRAND TOTAL FUNDING		$193,950	$323,250	$452,550
D. Projected Surplus/Deficit (+/-) (Grand Total Funding *minus* Grand Total Costs)		–$114,707	+$1,984	+$124,383

X. Expenditures and Funding Sources Explanations

A. Expenditures

Personnel – Reassigned or Existing Positions

The current EECS Undergraduate Program Director (0.05 FTE faculty) and Undergraduate Program Coordinator (0.2 FTE staff) will administer this degree program, along with the four other existing undergraduate degree programs in EECS.

A total of 1.50 FTE faculty in the department are expected to teach undergraduate-level classes that will have Cybersecurity Engineering degree program students in their classes along with students from the undergraduate degree programs. EECS faculty typically teach about two undergraduate courses per year, which is calculated as 0.2 FTE, which is the typical undergraduate teaching load at a Research I institution. Some individual faculty members are split between Cybersecurity Engineering and the other undergraduate programs in the EECS department, and some are the exclusive instructor of required undergraduate courses, and so 0.10 FTE is calculated per undergraduate course, which results in 0.1 FTE to 0.3 FTE for individual faculty members. All these administration, staff, and faculty salary costs are described in the "Core Faculty" section of the proposal as assigned to the Cybersecurity Engineering program.

Personnel – New Positions

No new positions are required for instruction or to administer this degree program.

Start-up Costs – One-Time Expenses
One-time expenses are limited to ABET's review of the program for initial accreditation. KU requests Board approval to seek ABET accreditation from the Engineering Accreditation Commission. ABET sets the standards for engineering accreditation as well as for programs in the natural sciences, computing, and engineering technology. ABET awards accreditation to programs that meet internationally recognized standards through a peer-review process and 4,564 programs at 895 institutions are accredited in 40 countries.

ABET accreditation assures that programs meet standards to produce graduates ready to enter critical technical fields that are leading the way in innovation and emerging technologies, and anticipating the welfare and safety needs of the public. Sought worldwide, ABET's voluntary peer-review process is highly respected because it adds critical value to academic programs in the technical disciplines, where quality, precision and safety are of the utmost importance.

Operating Costs – Recurring Expenses
ABET charges an annual fee of $715 per program.

B. Revenue: Funding Sources
Funding for the program will be through tuition and student fees. We expect primarily Kansas residents and those qualifying for in-state tuition will be interested in the Cybersecurity Engineering program. The current in-state tuition and student fees for Engineering undergraduate students are $336/credit hour and $95/credit hour, respectively. The projected student semester credit hours from Section V (along with the tuition and fees given above) are used to calculate the revenue from funding sources generated by this program. We have conservatively estimated the number of students interested in the program and expect the program to meet KBOR minimum requirements for enrollments and graduates within three years of inception.

C. Projected Surplus/Deficit
Our budget estimate indicates the degree program will run a surplus beginning in Year 2.

XI. References

Bureau of Labor Statistics. U.S. Department of Labor. *Occupational Outlook Handbook*, Information Security Analysts, Retrieved April 3, 2023 from https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.

Centers of Academic Excellence in Cybersecurity Community. *CAE institution map*. Retrieved April 3, 2023, from https:/www.caecommunity.org/cae-map.

Dorrian, B. (2021, December 7). *Former Google, Uber exec joins maker of Pokémon Go – and he's building a team of developers in Lawrence*. Startland News. Retrieved from https://www.startlandnews.com/2021/12/brian-mcclendon-niantic/.

National Institute of Standards and Technology. U.S. Department of Commerce. *Cybersecurity workforce demand*: Retrieved April 3, 2023 from https://www.nist.gov/system/files/documents/2022/07/06/NICE%20FactSheet_Workforce%20Demand_Final_20211202.pdf