**LETTER OF NOTIFICATION - 10**

**GRADUATE CERTIFICATE PROGRAM**

(12-18 SEMESTER CREDIT HOURS)

1. Institution submitting request: University of Arkansas Fayetteville

2. Contact person/title: Dr. Terry Martin, Vice Provost for Academic Affairs

3. Phone number/e-mail address: (479) 575-2151/tmartin@uark.edu

4. Proposed effective date: Fall 2018

5. Name of proposed Graduate Certificate Program (Program must consist of 12-18

semester credit hours from existing graduate courses): Cybersecurity Graduate Certificate

6. Proposed CIP Code: 11.1003 Computer and Information Systems Security/Information Assurance.

7. Reason for proposed program implementation:

The security challenges facing the United States are increasing and evolving in complexity. A connected world means that cybersecurity reaches almost every industry. Therefore, industries that drive our economy leave the nation vulnerable to new threats. Four out of ten companies that were the victims of cyber attacks said that losses were substantial with one third of the companies reporting a loss of revenue of 20% or more (Cisco, 2017). Data breaches in which medical and/or financial records are potentially put at risk had a total average cost of $3.62 million in a recent survey of over 400 companies (Ponemon Institute, 2017). Amongst the largest of the challenges faced by organizations is that cyber influences are prevalent and daunting due to the numerous motives for bad actors to profit/gain from the information gathered. Unfortunately, these new challenges are met with an increasingly insufficient security workforce. In traditional cybersecurity alone, 209,000 jobs went unfilled in the US (Intel, 2016) and 1 million jobs went unfilled worldwide (Cisco, 2015). As recently as August 2016, a survey showed that only 23% of existing professionals believe that existing security education programs are effective in preparing future security workers (EAB, 2016). The new Cybersecurity Graduate Certificate responds to the need for the future security workforce.

References:

Cisco (2015). http://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-talent.pdf

Cisco 2017 Annual Cybersecurity Report, cisco.com/go/cybersecurity

EAB, 2016. There’s a cybersecurity expert shortage: colleges can help. <https://www.eab.com/daily-briefing/2016/08/05/theres-a-cybersecurity-expert-shortage-colleges-can-help>

Intel. Global Study Reveals Businesses and Countries Vulnerable Due to Shortage of Cybersecurity Talent (2016). Retrieved 23 March 2017 from https://newsroom.intel.com/news-releases/global-study-reveals-businesses-countries-vulnerable-due-shortage-cybersecurity-talent/

Ponemon Institute LLC, “2017 Cost of Data Breach Study”, www.ibm.com, June 2017

8. Provide the following:

a. Curriculum outline - List of courses in new program – Underline required courses

CSCE 5323 Computer Security

CSCE 5433 Advanced Cryptography

CSCE 5833 Computer Architecture Security

CSCE 5333 Computer Forensics

CSCE 5663 Database Security

CSCE 5653 Network Security

CSCE 5763 Privacy Enhancing Technologies

CSCE 5623 Secure Digital System Design

CSCE 5753 Wireless System Security

b. Total semester credit hours required (Program range: 12-18 graduate semester

 credit hours)

A total of 12 hours would be required for the certificate.

c. New courses and course descriptions

These courses have already been taught as special topics courses and now are in the process of becoming permanent courses.

CSCE 5833 Computer Architecture Security (3 credits)

This course will cover fundamental principles and emerging implementation strategies to reason about, design and construct architecture level security capabilities in the manycore era. Coverage includes formal security models, new and emerging considerations for heterogeneous multiprocessor system on chip architectures, hardware and software implementation methods, operating systems for run time security enforcement.

CSCE 5763 Privacy Enhancing Technologies (3 credits)

This course introduces privacy enhancing technologies and hot privacy topics in emerging computing systems. Topics covered include introduction to security and privacy, privacy enhancing technologies, hot privacy and security topics in mobile phones/devices, mobile applications, Big Data systems, Cloud computing, cyber- physical systems, and other emerging computing systems. The course is a combination of lectures and student-led paper presentations. Students will be exposed to many interesting privacy problems, study privacy enhancing technologies, and apply their knowledge to explore an open research problem in a research-oriented project. After completing this course, students will gain a broad knowledge of the state-of-the-art and open research problems. They will also develop skills and enhance potentials to do research on privacy, security, and relevant areas.

CSCE 5623 Secure Digital System Design (3 credits)

This course is to give graduate students from Computer Engineering, Electrical Engineering, and Computer Science an insight of contemporary security-related issues in modern digital systems. In addition to lectures, students will be practicing secure digital system design during the project.

CSCE 5753 Wireless System Security (3 credits)

Wireless systems such as wireless local area networks, cellular and mobile networks, and sensor networks are vulnerable to attacks. The goal of the class is for students to understand how to design secure wireless systems. Security topics include confidentiality, integrity, availability, privacy, and control of fraudulent usage of networks. Issues addressed include basic wireless theory, cryptography, threat modeling, risks, and mitigation techniques.

d. Program goals and objectives

The objectives of the Cybersecurity Graduate Certificate are aligned with both the NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST, 2017) and with the draft National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF) (NICE, 2016) that has been under development by the National Institute of Standards and Technology (NIST). Note that the NICE Cybersecurity Workforce Framework is used by the Federal Office of Personnel Management as a guide to assign cybersecurity codes to federal positions with information technology, cybersecurity, and cyber-related functions (OPM, 2016).

Cybersecurity Graduate Certificate graduates will:

* Possess a comprehensive understanding of the core cybersecurity functions to identify risks, assess risks, protect services, detect events, respond to events, and recover from events.
* Be able to securely provision, operate and maintain, oversee and govern, protect and defend, analyze, collect and operate, or investigate information technology (IT) systems and/or networks.
* Enhance Arkansas’ and the nation’s cybersecurity industry.
* Demonstrate professional skills and behavior.

References:

National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF), Draft NIST Special Publication 800-181, National Institute of Standards and Technology (NIST), Nov. 2016.

NIST Framework for Improving Critical Infrastructure Cybersecurity, Draft version 1.1, National Institute of Standards and Technology (NIST), Jan. 10, 2017.

OPM Federal Cybersecurity Coding Structure, Office of Personnel Management (OPM), Nov. 15, 2016.

e. Expected student learning outcomes

The expected student learning outcomes for a student completing the Cybersecurity Graduate Certificate are based on draft ABET documents (ABET, 2016) and the NICE Cybersecurity Workforce Framework (NICE, 2016).

* An ability to apply security principles and practices to the environmental, hardware, software, and human components of a system.
* An ability to analyze and evaluate systems with respect to maintaining operations in the presence of risks and threats.

References:

ABET Cybersecurity Accreditation. 2016. https://www.fbcinc.com/e/nice/presentations/2016/Track\_D\_Century\_C/D-9\_Part\_B\_Parrish\_2016-10-28.pdf

f. Documentation that program meets employer needs

In addition to the justification discussed in Section 7, a recent proposal by the Arkansas Security Research and Education Institute (ASCENT) for government cybersecurity scholarships included nine letters from federal and state agencies interested in recruiting cybersecurity professionals (see Appendix A). If this proposal is funded, it will increase the demand for the courses and the certificate by providing 6-8 two-year cybersecurity scholarships each year over a five-year period. Another proposal by ASCENT for data-driven security solutions in retail, food, and transportation had ten letters of support from commercial industries interested in cybersecurity technologies and student recruitment (see Appendix B). These government and industrial employers have strong interests in cybersecurity find it difficult to find qualified cybersecurity employees.

g. Student demand (projected enrollment) for program

The Department of Computer Science and Computer Engineering (CSCE) will be offering all of these courses. CSCE faculty are core members of the Center for Information Security and Reliability (CISR) and the Arkansas Security Research and Education Institute (ASCENT). The objective of the University of Arkansas’ Center for Information Security and Reliability (CISR) is to promote education and research in the field of computer security and information assurance. Primarily owing to the effort of CISR, the University of Arkansas was recognized as a Center for Academic Excellence in Information Assurance Research (CAE-R) in 2012 and then again in 2014 by the National Security Agency and Department of Homeland Security. Established in October 2015, ASCENT (http://ascent.uark.edu) focuses on conducting practical and transformative research on security for real-world problems in industry, and strengthening security education at the University of Arkansas to train the next-generation security workforce. Both CISR and ASCENT demonstrate the strong support for cybersecurity in the CSCE department and help drive the demand for cybersecurity courses. Since 2012, the department has been offering 3-5 security-related courses each calendar year for graduate students with a total annual average of 42 students enrolled in these courses. We believe that a graduate enrollment of 10-15 students (42 students annually divided by 4 classes) in the program is a conservative projection with the actual numbers likely to be substantially higher.

h. Name of institutions offering similar programs and the institutions used as a model to develop the proposed program

Several institutions offering similar graduate-level cybersecurity certificates were reviewed by using the directory at the cyberdegrees.org website (Cyber Degrees, 2017). The search was focused on graduate-level cybersecurity programs with similar course offerings as being offered by the CSCE department. Many of the CSCE courses are research-centric and advanced since they are offered at the graduate level. Representative graduate certificate programs that consist of 9-15 credit hours with similar courses were used as a model to develop the certificate and are listed below.

* Kennesaw State University, Information Security and Assurance Certificate, 12 credit hours
* Sacramento State, Certificate in Information Assurance and Security, graduate level, 9 credit hours
* University of Maryland, Cybersecurity Graduate Certificate in Engineering, graduate level, 12 credit hours

In addition to certificate programs, several cybersecurity M.S. programs were reviewed to develop program goals and objectives and expected student learning outcomes. For example, the University of Tulsa has a Cyber Security M.S. program with both thesis and non-thesis options and published program objectives that were used as a guide for the program objectives.

Note that there is a Technical Certificate in Information Assurance offered by the University of Arkansas at Little Rock (UALR). However, this program is the same as the minor in Information Assurance and consists of 21 hours of undergraduate coursework. Therefore, the UALR program can be classified as more of an undergraduate certificate instead of a graduate certificate that is being proposed in this document.

References:

Cyber Degrees. (2017). http://cyberdegrees.org

i. Scheduled program review date (within 10 years of program implementation)

2024-2025

9. Provide documentation that proposed program has received full approval by licensure/certification entity, if required. (A graduate certificate offered for teacher/educator administrator licensure must be reviewed/approved by the Arkansas Department of Education prior to consideration by the Coordinating Board; therefore, the Education Protocol Form must be submitted to ADHE along with the Letter of Notification.)

N/A

10. Institutional curriculum committee review/approval date: December 6, 2017

11. Will this program be offered on-campus, off-campus or via distance delivery? Indicate mode of distance delivery.

On-campus

12. Identify off-campus location. Provide a copy of e-mail notification to other institutions in the area of the proposed off-campus program offering and their responses; include your reply to the institutional responses.

N/A

13. Provide additional program information if requested by ADHE staff.

N/A

President/Chancellor Approval Date: January 8, 2018

Board of Trustees Notification Date: March 29, 2018

Chief Academic Officer: James S. Coleman Date: January 2, 2018