2018

Improving Cyber Defense Education through National Standard Alignment: Case Studies

Ping Wang
Maurice Dawson
Kenneth Williams

International Journal of Hyperconnectivity and the Internet of Things
Volume 2 • Issue 1 • January-June 2018

Improving Cyber Defense Education through National Standard Alignment:
Case Studies

Ping Wang, Robert Morris University, Moon, USA

Maurice Dawson, Department of Information Technology and Management, Illinois Institute of Technology, Chicago, USA

Kenneth L Williams, American Public University System, Charles Town, USA

ABSTRACT

There has been a fast-growing demand for cybersecurity professionals to defend cyber space and information systems. With more and more programs and course offerings in cybersecurity popping up in higher education, it is important to have a consistent and reliable quality standard to guide and evaluate the training and preparation of qualified cyber defense workforce. The national Centers of Academic Excellence in Cyber Defense Education (CAE-CDE) designation program jointly sponsored by the US National Security Agency (NSA) and Department of Homeland Security (DHS) is a rigorous national standard with specific criteria for maintaining the quality of cybersecurity education. This article explains the CAE-CDE program criteria and requirements and discusses the important role of the special designation in improving cyber defense education and workforce development. This article illustrates the educational value and quality impact of the CAE-CDE program with three case studies: (1) University of Missouri – St. Louis; (2) American Public University; and (3) Robert Morris University.

KEYWORDS

Cyber Defense Education (CDE), Centers of Academic Excellence (CAE), Designation, Quality Improvement, Workforce Development

DOI: 10.4018/IJHIoT.2018010102

1. INTRODUCTION

This paper uses case studies to explore the important topic of how to improve the quality of cyber defense education in the United States through national standard alignment. Cyber defense is the core aspect of Cybersecurity, which has been a fast-growing career field and an important area with increasing demand and opportunities for higher education. Information security analyst is only one of the cybersecurity career titles. According to U.S. Department of Labor Bureau of Labor Statistics (BLS), employment of information security analysts is projected to grow 28% from 2016 to 2026, much faster than the average growth rates of 7% for all occupations and 13% for all computer related occupations (U.S. Department of Labor, 2018).

The latest cybersecurity workforce framework published by the National Initiative for Cybersecurity Education (NICE) recognizes the growing need for an integrated cybersecurity workforce with technical and non-technical roles for organizations to address their cybersecurity challenges and implement their missions and business processes connected to cyberspace. The NICE Cybersecurity Workforce Framework (NCWF) emphasizes that "academic institutions are a critical part of preparing and educating the cybersecurity workforce" (National Initiative for Cybersecurity Education, 2017). A recent study shows that top U.S. universities were failing at cybersecurity education with a lack of cybersecurity requirements for graduates and a slow change in curriculum and courses (White, 2016). However, it is encouraging to see more and more 2-year and 4-year academic institutions have started to offer cybersecurity degree programs and courses across the country. Quality assurance is needed for cybersecurity-related degree programs to meet high cybersecurity academic standards in order to prepare the graduates for the growing number of cybersecurity positions (National Initiative for Cybersecurity Careers and Studies, 2017).

The national Centers of Academic Excellence in Cyber Defense Education (CAE-CDE) designation program jointly sponsored by the US National Security Agency (NSA) and Department of Homeland Security (DHS) is a national quality standard for certifying and maintaining high quality of cybersecurity education with rigorous and consistent requirements for program evaluation and close alignment to specific cybersecurity knowledge units. Out of over 5300 colleges and universities in the U.S., only about 200 of them have achieved the CAE-CDE designation status. Attendance at a CAE school will give students confidence in learning, and a degree from a CAE school will give employers confidence in hiring (National Initiative for Cybersecurity Careers and Studies, 2017).

This paper will describe the background for CAE-CDE program, highlight the important application and designation criteria, and use the case study methodology to present three different cases of academic institutions with different CAE status: University of Missouri – St. Louis (UMSL), American Public University System (APUS), and Robert Morris University (RMU). The goal of the study is to illustrate the important role of the CAE designation and the application process in improving the quality of cybersecurity education and workforce preparation at these institutions through alignment of a national standard for quality control.

2. BACKGROUND

The national CAE-CDE program evolved from the initial national CAE in Information Assurance Education (CAE-IAE) program started by NSA in 1998 with DHS joining as a co-sponsor in 2004, and the CAE in IA Research special designation was added in 2008 to encourage doctoral level research in cybersecurity (National Security Agency, 2016). In 2010, the CAE2Y component was created to provide the CAE designation opportunity for two-year institutions, technical schools, and government training centers. Hence, the current CAE-CD program includes these designations: CAE2Y for two-year institutions, and CAE-CDE for four-year institutions, and CAE-R for doctoral universities or Department of Defense schools. All regionally accredited two-year, four-year and graduate level institutions in the United States are eligible to apply for the appropriate CAE designation. The designation is granted to schools which have demonstrated compliance with rigorous CAE criteria and curricula mapping to a required core set of cyber defense knowledge units (KUs) with optional Focus Areas (National Security Agency, 2016).

2.1. Application Requirements

Eligible applicants should submit their CAE applications online, and new applicants should complete a checklist for readiness check to determine if optional application assistance, such as program and curriculum development assistance or application mentoring, is needed. An official Letter of Intent and Endorsement signed by the applicant institution’s Provost or higher is a mandatory requirement to be included in online application. This letter should express institutional commitment and support for the CAE program, identify the institution’s CAE point of contact, and provide information on regional accreditation and list accomplishments in the cyber defense field (National IA Education & Training Programs, 2018).

2.2. Criteria for Measurement

All applications will be reviewed and assessed by qualified independent cyber professionals and subject matter experts from CAE schools, government, and industry. New applications will be assessed by three reviewers, and applications for re-designations will be reviewed by two reviewers. Initial designation is valid for five academic years, and re-application is required for retaining the designation. The following are the latest criteria for assessing CAE applications for the 2018 cycle (National IA Education & Training Programs, 2018). There are specified mandatory points in each of the criteria for the application.

2.2.1. Cyber Academic Curriculum Path

This is to demonstrate a relevant and mature cyber curriculum program in place for at least 3 years with mappings to KUs and NCWF and student enrollment and completion data. There are 10 mandatory points overall for this criterion. The latest Knowledge Units (KUs) and KU mapping template for the 2019 cycle have just been released (National IA Education & Training Programs, 2018).

2.2.2. Student Skill Development and Assessment

This is to show student development activities and assessment in cyber defense, including syllabi, assignments, hands-on labs, competitions, and guest lectures from cybersecurity practitioners. There are 18 mandatory points out of 25 maximum points for this criterion.

2.2.3. "Center" for Cyber Education

This is to an officially established physical or virtual center to serve as a guidance and resource center with an external advisory board for the institution's cyber curriculum and practice. There are 8 mandatory points out of 13 maximum points for this criterion.

2.2.4. Cyber Faculty Qualifications and Courses Taught

This is to show the faculty in charge of the cyber defense program, relevant faculty publications, presentations, and faculty support student cyber activities and clubs. There are 15 mandatory points out of 20 maximum points for this criterion.

2.2.5. Multidisciplinary Practice in Cyber Defense

This is to demonstrate that Cybersecurity is integrated additional degree programs and courses in the same institution. There are 7 mandatory points out of 15 maximum points for this criterion.

2.2.6. Institutional Security Plan

This is to show the institution's security plans, responsible party, and its implementation of cybersecurity practices. There are 6 mandatory points out of 9 maximum points for this criterion.

2.2.7. Cyber Outreach and Collaboration

The institution must demonstrate activities to extend cyber defense practices beyond the institution, including faculty and curriculum sharing with community schools, credit transfer agreement, participation in the CAE community, and outreach activities and industry collaboration. There are 15 mandatory points out of 25 maximum points for this criterion.

3. CASE STUDY: UMSL

3.1. School Profile, Demographics, Mission

The University of Missouri - Saint Louis (UMSL) is the largest public research university in eastern Missouri. It provides excellent learning experiences and leadership opportunities to a diverse student body whose influence on the region upon graduation is immense. UMSL is spread across 470 acres in suburban St. Louis County. UMSL's College of Business Administration is accredited by Association to Advance Collegiate Schools of Business (AACSB) International. UMSL is the region's first and only NSA/DHS designated CAE-CDE. UMSL is the only institution within the eight states that border Missouri to hold any of the 17 available focus areas.

3.2. Cyber Programs and Data

The cybersecurity program at UMSL is a multidisciplinary effort between the Departments of Mathematics and Computer Science in the College of Arts and Sciences and the Department of Information Systems in the College of Business Administration. This collaborative approach allows students to explore the many avenues of information security and adapts to the evolving nature of the field. UMSL has created an undergraduate certificate, graduate certificate, undergraduate minor, and graduate track in cyber security. The programs were created to address the shortfall of 3,800+ jobs in the Saint Louis Metropolitan Region (Cyberseek, n.d.). Table 1 below displays the courses for the cybersecurity certificate programs in the Information Systems Department which require students take at least one computer science course.

The courses all have a hands-on component which enables students to gain more technical depth in varied programming languages, forensic tools, static code analyzers, and offensive security applications. The courses are developed to address the future of national and international cybersecurity (Dawson, Omar, Abramson, & Bessette, 2014). The UMSL program heavily uses Open Source Software (OSS) as it serves as a means for students to understand low-level coding and to inspect source code for security (Dawson, Al Saeed, Wright, & Onyegbula, 2014). Additionally, the labs become reusable learning objects. To enhance student learning, a physical and virtual lab environment was created with both Linux and Windows systems in which the student is given a dedicated Kali Linux virtual machine that allows them to practice offensive security operations in a controlled environment. The lab activities allow students to obtain hands-on experience in offensive and defensive security. Figure 1 below illustrates the virtual network environment at UMSL.

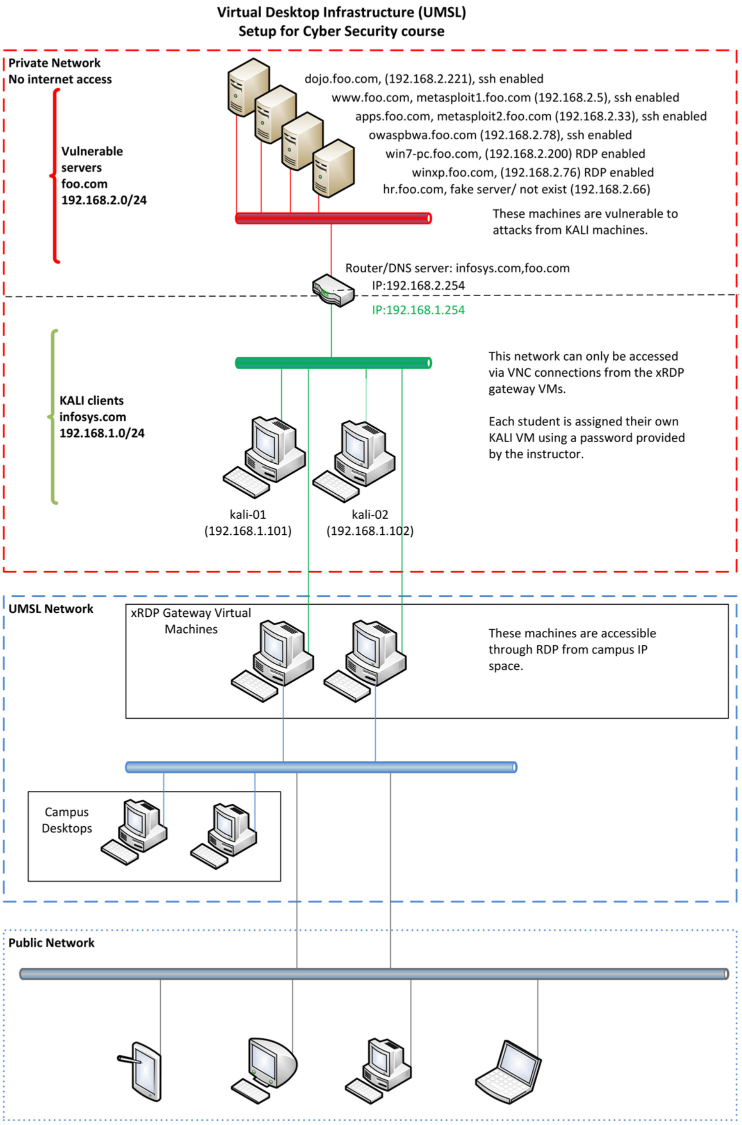
3.3. CAE Status and Accomplishments

The cybersecurity program at UMSL received $493,650 from two NSA grants within the last year. This funding will help develop lab infrastructures, enhance equipment and further advance cyber security curricula. Through two Non-Governmental Organizations (NGOs), faculty and students have also received grants of about

Table 1. UMSL Cybersecurity Certificate Programs

Undergraduate Program	Graduate Program
INFSYS 3848 Introduction to Information Security	INFSYS 6828 Principles of Information Security
INFSYS 3842 Data Networks and Security	INFSYS 6836 Management of Data Networks and Security
INFSYS 3858 Advanced Security and Information Systems	INFSYS 6858 Advanced Cybersecurity Concepts
INFSYS 3868 Secure Software Development	INFSYS 6868 Software Assurance
INFSYS 3878 Information Security Risk Management and Business Continuity	INFSYS 6878 Management of Information Security
CMP SCI 4700 Computer Forensics	CMP SCI 4700 Computer Forensics

Figure 1. UMSL Virtual Network Environment


Virtual Desktop Infrastructure (UMSL)
Setup for Cyber Security course
Private Network
No internet access
Vulnerable servers
foo.com
192.168.2.0/24
dojo.foo.com, (192.168.2.221), ssh enabled
www.foo.com, metasploit1.foo.com (192.168.2.5), ssh enabled
apps.foo.com, metasploit2.foo.com (192.168.2.33), ssh enabled
owaspbwa.foo.com (192.168.2.78), ssh enabled
win7-pc.foo.com, (192.168.2.200) RDP enabled
winxp.foo.com, (192.168.2.76) RDP enabled
hr.foo.com, fake server/ not exist (192.168.2.66)
These machines are vulnerable to attacks from KALI machines.
Router/DNS server: infosys.com,foo.com
IP:192.168.2.254
IP:192.168.1.254
KALI clients
infosys.com
192.168.1.0/24
This network can only be accessed via VNC connections from the xRDP gateway VMs.
Each student is assigned their own KALI VM using a password provided by the instructor.
kali-01
(192.168.1.101)
kali-02
(192.168.1.102)
UMSL Network
xRDP Gateway Virtual Machines
These machines are accessible through RDP from campus IP space.
Campus Desktops
Public Network

$35,000 from John Ogonowski and Doug Bereuter Farmer-to-Farmer Program (F2F). The CAE designation also helped a faculty member to secure a two-year Fulbright Scholar Cybersecurity Specialist Grant valued at about $20,000. Industry partners have provided more than $150,000 to the Information Systems program UMSL in the form of gifts, equipment, internships, and more.

4. CASE STUDY: APUS

4.1. School Profile, Demographics, and Mission

American Public University System (APUS) submitted its application for Center of Academic Excellence (CAE) in Cyber Security Defense (CDE) in January 2018 and received news that the application was successful in April 2018. APUS is accredited by the Higher Learning Commission (HLC) and offers online degree and certificate programs through American Military University (AMU) and American Public University (APU). APUS is an online institution of higher learning serving the needs of military, public service and civilian communities through American Military University (AMU) and American Public University (APU). APUS is a subsidiary of American Public Education, Inc. (APEI) - the parent company that also owns Hondros College of Nursing (HCN) which serves students primarily through five Ohio campuses in Cincinnati, Cleveland, Columbus, Dayton and Toledo. Together, these institutions serve more than 85,000 adult learners worldwide and offer more than 200 degree and certificate programs in fields ranging from cybersecurity, homeland security, military studies, intelligence, and criminal justice to technology, business administration, public health, nursing and liberal arts (American Public Education, Inc., n.d.).

APUS was founded in 1991 as AMU. Since then, approximately 75,000 alumni have graduated from either AMU or APU. As of September 30, 2017, APUS has a student population of over 81,000 students with over 200 degree and certificate programs APUS student enrollment by degree level consists of 59% bachelor's, 16% associates, 16% master's and 9% certificate programs. Demographically APUS student population includes; 88% working adults. The average student age is 33 years old, and the average class size is 9 students. The gender ratio is 64% male versus 36% female (American Public Education, Inc., n.d.).

4.2. APUS Cybersecurity Program

At APUS Cybersecurity is taught as a program within the School of Science Technology Engineering & Math. Students may choose to earn cybersecurity education through certificates, Bachelor or Master programs. The cybersecurity undergraduate certificate examines the digital forensics tools, techniques, and methods used by cyber analysts to detect cybercrime, cyber terrorism, cyber war, cyberstalking, and cyberbullying. The Bachelor of Science in Cybersecurity provides students with both theory and know-how required to strategically assess, plan, design, and implement effective cybersecurity defenses in the public and private sectors. The Master of Science in Cybersecurity Studies takes a broad, multi-disciplinary approach to preventing and responding to large-scale cyber threats and cyber-attacks. The first half of this program provides students with a foundation in network security, cybersecurity, cybercrime, and digital forensics. The second half of this program focuses on the issues, policies, practices, and perspectives of various sectors, critical infrastructures, agencies, and disciplines, such as national security, intelligence, criminal justice, and emergency management (American Military University, n.d.).

4.3. CAE Status and Accomplishments

APUS started the process to achieve the status as a Center of Academic Excellence in Cyber Defense (CD) Education (CAE-CDE) in mid-2017 with a self-assessment of readiness. The assessment of the APUS readiness for the CAE-CDE designation resulted in the assignment of a mentor to assist in the completion of the application (National IA Education & Training Programs, 2018).

Following the result of the self-assessment and assignment of a mentor, a core group of subject matter experts (SME) supported by other members of the APUS staff was convened. This core group was managed by the APUS Provost and consisted of SME from the Cybersecurity program along with support from the APUS accreditation group and other department to include; career services, Academics, and other schools throughout the APUS. Weekly meetings were held with various members of the core group; consisting of both virtual and face-to-face sessions (National IA Education & Training Programs, 2018).

The first significant session of the core group consisted of a face-to-face two-day conference with SME's and the assigned mentor. During this session, selection of the cybersecurity path was finalized; resulting with the selection of 12 courses from the Bachelor of Science in cybersecurity program (see below).

Selected courses from the cybersecurity path (Bachelor of Science in Cybersecurity):

- Scripting Languages for the Administrator - introducing scripting languages to the student to develop a basic knowledge in programming for server administration and security.
- Introduction to Networking – a study of the evolution, the concepts, and the principles of local, distributed and enterprise networking.
- Operating Systems: Hardening and Security – a study of the principles and concepts of Networking Security from the perspective of the Operating System (OS).
- IT Security: Attack & Defense – an examination of the techniques and technologies for penetration of networks, detection of attacks, and prevention of attacks.
- IT Security: Cryptography – an extensive overview of the field of cryptography, which includes but is not limited to a historical perspective of early systems, building to the number theoretic foundations of modern day cryptosystems.
- Computer and Network Security – an analysis of the threats within the organizational network environment along with appropriate mitigation processes.
- Information Security – an examination of the broad range of cybersecurity issues to include the exploration of processes to protect propriety information and security planning with the emphasis on networked computer vulnerabilities.
- Database Systems Security – an introductory study of the principles, practices, procedures, and methodologies to ensure security of data at rest within databases.
- IT Planning: Planning and Policy – an examination of the principles of security planning and policy to include a focus on a variety of security guidelines, policies and plans.

- Cyberlaw and Privacy in a Digital Age – examination of how law have had to change to account for the expanded realm of crimes in the digital age.
- Cyber Warfare – an overview of cyber warfare along with the potential impact of its use by military, terrorist, and criminal organizations.
- Statistics – an introduction to statistical methods and models available to analyze and solve the wide variety of problems encountered in business, science, medicine, education, the social sciences, and other disciplines.

These 12 selected courses formed the core courses used to meet the requirements of the CAE-CDE mandatory core and optional Knowledge Units (KUs). Along with the selection of the core courses for CAE-CDE program, the group selected seven optional Knowledge Units resulting in a total of 22 KUs to measure the readiness for the APUS CAE-CDE designation.

Knowledge Units selected (CAE-CDE Knowledge Units):

- Basic Data Analysis - to provide students with basic abilities to manipulate data into meaningful information.
- Basic Scripting of Introductory Programming - provide students with the ability to create simple scripts/programs to automate and perform simple operations.
- Cyber Defense - provide students with a basic awareness of the options available to mitigate threats within a system.
- Cyber Threats - provide students with basic information about the threats that may be present in the cyber realm
- Fundamental Security Design Principles - provide students with basic security design fundamentals that help create systems that are worthy of being trusted.
- IA Fundamentals - provide students with basic concepts of information assurance fundamentals.
- Intro to Cryptography - provide students with a basic ability to understand where and how cryptography is used.
- IT Systems Components - provide students with an understanding of the basic components in an information technology system and their roles in system operation
- Networking Concepts - provide students with basic understanding of network components and how they interact.
- Policy, Legal, Ethics, and Compliance - provide students with and understanding of information assurance in context and the rules and guidelines that control them
- System Administration - provide students with skill to perform basic operations involved in system administration.
- Databases - teach students how database systems are used, managed, and issues associated with protecting the associated data assets
- Network Defense - teach students the techniques that can be taken to protect a network and communication assets from cyber threats
- Networking Technology and Protocols - provide students with an understanding of the components in a network environment, their roles, and communication methods

- Operating Systems Concepts - provide students with an understanding of the roles of an operating system, its basic functions, and the services provided by the operating
- Probability and Statistics - provide students with the ability to use basic statistics to analyze and attach meaning to datasets
- Programming - provide students with the skills necessary to implement algorithms using programming languages to solve problems
- Operating Systems Hardening - provide students with the ability to apply methods such as managing applications, services, and network ports to improve the robustness of operating systems
- Network Security Administration - provide students with knowledge of the methods of analyzing and mitigating threats within a network environment
- Penetration Testing - provide students with methods of discovering ways of exploiting vulnerabilities to gain access to a system
- Overview of Cyber Operations - provide students with an understanding of the authorities, roles and steps associated with cyber operations
- Cybersecurity Planning and Management - provide students with the ability to develop plans and processes for a holistic approach to cybersecurity for an organization

Subsequent meetings with the matrix team followed over a six-month period to complete the CAE-CDE application. Meetings were also held with members of the NSA CAE-CDE office to include two face-to-face sessions; seeking feedback and clarification to the application process. Shortly after the availability of the submission portal in September 2017, the submission process began, resulting with a determination of completeness by the mentor. This determination initiated the process of an independent pre-assessment of the APUS application that was returned with a report of no deficiencies for the mapping of the core courses to the 22 KUs and criteria. Following a final review from the APUS leadership, the final submission of the application occurred on January 12, 2018. The designation as a Center of Academic Excellence in Cyber Defense Education through year 2023 was received in April 2018. Official letters of notification was sent to APUS, the State Governor, Members of Congress, and appropriate Congressional Committees (National IA Education & Training Programs, 2018).

4.4. Impact of CAE-CDE Application on Programs, Courses, Institution, and Students

The application of the APUS CAE-CDE application is long lasting in its impact on the programs, course, institution, and its students. The cybersecurity program saw changes to the core courses; allowing students to follow a direct path that will result in the achievement of a robust cybersecurity education, ranging from knowledge in software to database security and statistics. All students selecting the cybersecurity program are required to follow this CAE-CDE path. Courses within the CAE-CDE path were also examined to ensure the robustness of the CAE-CDE criteria.

Courses from other schools within APUS were also assessed and selected for submission of the CAE-CDE application. The selected courses resulted in a greater appreciation for the importance of cybersecurity across the APUS; initiating a call for additional cross discipline courses that further increase awareness of cybersecurity threats.

Students within APUS were also impacted by the application for CAE-CDE. As noted above all students selecting the BA in cybersecurity are now expected to complete the path; resulting in a robust cybersecurity education and an enhance career opportunity. Students completing the path can share the news of their completion with potential employers; resulting in an edge over other applicants without equal level of education.

5. CASE STUDY: RMU

5.1. Profile, Demographics, and Mission

Robert Morris University (RMU), founded in 1921, is a selective private non-profit national university located in the Greater Pittsburgh region in western Pennsylvania. RMU has a total enrollment of 4,384 undergraduate and 815 graduate students. RMU is accredited by the Middle States Commission on Higher Education and serves a diverse student population of men and women, working professional, military and veteran students, minorities, and international students. RMU provides a professionally focused education with an emphasis on engaged learning.

5.2. RMU Cyber Programs

Housed in RMU’s School of Communications and Information Systems (SCIS), the Department of Computer and Information Systems (CIS) offers four B.S. degrees in Cyber Forensics and Information Security (BS-CFIS), Computer Information Systems (BS-CIS), Information Sciences (BS-IS), and Data Analytics (BS-DTAN). The BS-CFIS, BS-CIS, and BS-IS degree programs are all accredited by the Computing Accreditation Commission of ABET (ABET, n.d.). The key cybersecurity courses for the BS-CFIS and other programs include Computer and Network Security, Intro to Computer Forensics, Digital Evidence Analysis, IT Security, Control/Assurance, and Mobile Forensics.

The department also offers five M.S. degrees in Cyber Security and Information Assurance, Information Systems Management, Internet Information Systems, Information Technology Project Management, and Data Analytics, as well as one doctoral degree in Information Systems and Communications. In addition to its degree programs, CIS offers undergraduate and graduate certificate programs in Information Systems, Mobile Forensics and Security, and Enterprise Systems. Most CIS degree and certificate programs are offered in both traditional and online formats.

The program selected and used for the CAE Knowledge Unit mapping is the B.S. degree program in Cyber Forensics and Information Security (BS-CFIS). The program is currently accredited by ABET and has articulation agreements accepting transfer students in Cybersecurity from local two-year colleges such as Community College of Allegheny County and Community College of Beaver College. The main goal of the program is for students to "learn techniques used to detect, respond to, and prevent network intrusions. They also master broader concepts such as the responsible use of resources, the appropriate management of risks, and the alignment of information technology with the organization" (Robert Morris University Cyber Forensics and Information Security, 2018, para. 4).

The BS-CFIS program requires 123 credits for graduation, including 39 credits of university core courses in non-major areas, 30 credits of major courses, 21 credits of cyber forensics/information security concentration courses, 15 credits in student-selected area of interest approved by the CIS department, and 18 credits of open electives.

RMU is planning to submit CAE-CDE application for the 2018-2019 cycle using the 2019 Knowledge Units (KUs). The 2019 KU requirement for bachelor's degree programs will require the following:

- **Three Foundational KUs:** Cybersecurity Foundations, Cybersecurity Principles, and IT Systems Components; AND
- **Five Technical Core KUs:** The Technical Core KUs are Basic Scripting and Programming; Basic Networking; Network Defense; Basic Cryptography; Operating Systems Concepts; OR
- **Five Non-Technical Core KUs:** Cyber Threats; Policy, Legal, Ethics, and Compliance; Security Program Management; Security Risk Analysis; Cybersecurity Planning and Management; AND
- 14 Optional KUs selected from the 2019 KU list ranging from Advanced Algorithms to Wireless Sensor Networks. In addition, the Technical Core KUs and Non-Technical Core KUs can be used as Optional KUs.

The following courses and curriculum components from the BS-CFIS program at RMU have been identified as preliminary candidates to map the new KUs for CAE-CDE:

- A Programming course in the option areas of programming in Java, C++, Visual C#, Visual Basic, Cobol, or M.
- An Operating Systems course with three options for students: Operating Systems Concepts, Microcomputing Technology (A+), or Enterprise Operating Systems.
- The Networking Technology (N+) course that covers the fundamentals of computer networking.
- The Computer and Network Security course that addresses the fundamental knowledge and skills in the security and defense of computing and networking.

- The IT Security, Control/Assurance course that addresses both technical and non-technical issues in IT security and information assurance.

5.3. CAE Status and Accomplishments

RMU is in the process of collecting artifacts and preparing documentation to submit the application for a CAE-CDE designation. RMU has submitted a New Applicant Inventory to NSA. Based on the review of the New Applicant Inventory submitted, RMU was assessed to be within one year of applying for the CAE designation. Hence, RMU was referred to the mentoring program with designated mentor as part of the Application Assistance Program (APP) funded by the National Science Foundation. RMU has confirmed its participation in the APP program with a designated Mentee Point of Contact to apply for the CAE-CDE designation. The application submission is projected to be completed within one year. RMU leadership is very supportive of this pursuit, and faculty and students are looking forward to the enhanced cybersecurity teaching, learning, and assessment activities through the CAE-CDE application and designation.

5.4. Impact of CAE pursuit on Cyber Defense Education

The application activities have had a number of positive effects on improving cyber defense education at RMU, which includes the following:

- CIS faculty begin to realize the great value of their course materials and activities in cyber defense through increased awareness and knowledge of the KUs and expectations for learning outcomes to meet the standards of CAE-CDE.
- The teaching and learning activities at the program are more and more focused on the KUs for CAE-CDE that provide students with necessary knowledge, skills, and abilities to enter the cyber defense workforce.
- The entire institution is paying more attention to cyber defense, outreach to community, and collaboration and partnership with community organizations (such as community colleges and high schools) in expanding cyber defense education.
- An Advisory Board has been established with national and local cybersecurity industry experts and faculty representatives from CAE schools to provide valuable input and suggestions on continuous curriculum improvement of the BS-CFIS program at RMU.
- As a result of the CAE-CED application effort, there has been increasing documented evidence of integration of cyber defense education in many different disciplines and programs at RMU, including non-technical programs in nursing and healthcare, criminal justice, business and accounting.

6. CONCLUSION

This paper explains the rigorous quality control criteria and important role of the NSA/DHS CAE-CDE designation in improving the quality of cybersecurity education and workforce development through alignment of a reputable and rigorous national standard. Three case studies of different institutions with different CAE status are presented to illustrate the importance of the CAE designation in enhancing cybersecurity education at these institutions. Updates to the CAE designation and application status for the two applicant schools with more specific data and accomplishments will be presented and discussed in future research reports.

REFERENCES

ABET. (n.d.). ABET Accredited Program Search. Retrieved from http://main.abet.org/aps/Accreditedprogramsearch.aspx

AMU (American Military University). (n.d.). Retrieved from http://www.amu.apus.edu/

APEI (American Public Education, Inc.). (n.d.). Retrieved from http://www.americanpubliceducation.com/phoenix.zhtml?c=214618&p=irol-homelanding

CyberSeek. (n.d.). Cybersecurity Supply/Demand Heat Map. Retrieved December 15, 2017, from http://cyberseek.org/heatmap.html

Dawson, M., Al Saeed, I., Wright, J., & Onyegbula, F. (2014). Open source software to enhance the stem learning environment. In V. Wang (Ed.), *Handbook of research on education and technology in a changing society* (pp. 569–580). Hershey, PA: IGI Global. doi:10.4018/978-1-4666-6046-5.ch042

Dawson, M., Omar, M., Abramson, J., & Bessette, D. (2014). The future of national and international security on the Internet. In A. Kayem & C. Meinel (Eds.), *Information security in diverse computing environments* (pp. 149–178). Hershey, PA: IGI Global. doi:10.4018/978-1-4666-6158-5.ch009

NICCS (National Initiative for Cybersecurity Careers and Studies). (2017, October 6). National Centers of Academic Excellence (CAE). Retrieved from https://niccs.us-cert.gov/formal-education/national-centers-academic-excellence-cae

NICE (National Initiative for Cybersecurity Education). (2017, August). NICE Cybersecurity Workforce Framework (SP800-181). Retrieved from https://csrc.nist.gov/publications/detail/sp/800-181/final

NIETP (National IA Education & Training Programs). (2018). CAE-CDE Criteria for Measurement 2018. Retrieved from https://www.iad.gov/NIETP/CAERequirements.cfm

NSA (National Security Agency). (2016, May 3). National Centers of Academic Excellence in Cyber Defense. Retrieved from https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/

Robert Morris University Cyber Forensics and Information Security. (2018). Retrieved from http://scis.rmu.edu/cis

Robert Morris University Department of Computer and Information Systems. (2018). Retrieved from http://scis.rmu.edu/cis

U. S. Department of Labor. (2018, April). Occupational outlook handbook. Retrieved from https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-6

White, S. K. (2016, April 25). Top U.S. universities failing at cybersecurity education. *CIO*. Retrieved from https://www.cio.com/article/3060813/it-skills-training/top-u-s-universities-failing-at-cybersecurity-education.html

Ping Wang is a Professor of Computer and Information Systems at Robert Morris University and a Certified Information Systems Security Professional (CISSP). He is also a Sun (Oracle) Certified Java Programmer and has over 10 years of consulting experience in Information Technology, E-Commerce, Cybersecurity, and served as a senior developer on a US Department of Defense grant project on Survivability and Information Assurance for three years. Dr. Wang has over 20 years of experience in teaching, research, curriculum development, and program management in higher education including most recently serving as Program Director and Professor of Cybersecurity in the University of Maryland system. He has received three best paper awards for his publications on Cybersecurity at recent international conferences in addition to several other distinguished national and international awards for innovation, teaching, and research.

Maurice Dawson is an Assistant Professor of Information Technology and Management within the School of Applied Technology at Illinois Institute of Technology. Additionally, he serves as Director of the National Center for Academic Excellence in Cyber Security Education and responsible for working with the faculty who are members of this center. Before joining academia, he was an engineering manager for unmanned air systems and senior program manager for rotary wing aircraft. He has a Doctor of Computer Science from Colorado Technical University and a Doctor of Philosophy in Cyber Security from the Intelligent Systems Research Centre at London Metropolitan University. Additionally, he is the co-editor of Developing Next-Generation Countermeasures for Homeland Security Threat Prevention, and New Threats and Countermeasures in Digital Crime and Cyber Terrorism, published by IGI Global in 2017, and 2015 respectively.

Kenneth L Williams is the Program Director for Cybersecurity at American Public University; he is a retired US Army IT officer with 24 years of active service and seven years of federal service as a civilian for the US Army. He has taught cybersecurity and IT courses at APUS since Spring 2016 and at other universities since the Fall of 2010. He has a Graduate and a PhD degree in Cybersecurity from Capella University and has focused intently on various aspects of cybersecurity to include; compliance, governance, and other related aspects of cybersecurity mitigation. Dr. Williams also operated a small business focused on IT/cybersecurity services with the federal government and commercial sectors for several years and assisted several organizations with their cybersecurity issues as a consultant.