2021 ASEE ANNUAL CONFERENCE
Virtual Meeting | July 26–29, 2021 | Pacific Daylight Time
Paper ID #32739

The Need For ABET Accreditation of Associate's Cybersecurity Programs

Dr. Rajendra K. Raj, Rochester Institute of Technology (GCCIS)

Rajendra K. Raj is a Professor of computer science at the Rochester Institute of Technology. His current research interests cover the nexus between data science and cybersecurity, as applied to a variety of domains including healthcare, finance, and other critical infrastructure sectors. Dr. Raj's other focus is computing education at all levels. He volunteers with ABET's Computing Accreditation Commission (CAC), and is currently serving as an officer on the CAC Executive Committee and as a CSAB/ABET Program Evaluator for computer science, cybersecurity, and information technology. Prior to RIT, he worked at a financial services firm, where he developed and managed leading-edge globally-distributed private cloud infrastructures for a variety of financial applications. He earned his Ph.D. in Computer Science from the University of Washington, Seattle.

Dr. Cara Tang, Portland Community College

Cara Tang is a faculty member and leads the Cybersecurity program in the Computer Information Systems department at Portland Community College (PCC). She also chairs the Association for Computing Machinery Committee for Computing Education in Community Colleges (ACM CCECC), and led the task group that created Cyber2yr2020, curriculum guidelines for two-year cybersecurity programs.

Dr. David Gibson, United States Air Force Academy

David Gibson is Professor Emeritus of Computer and Cyber Science at the United States Air Force Academy. During his 34-year career in the U.S. Air Force, he worked in electronic warfare, computer security, space systems, intelligence, and cyber operations. Prior to retiring, he served as Professor and Head of the Department of Computer Science at the Air Force Academy where he led development of the Academy's cyber education, training, and research programs. He was a member of the ACM's Joint Taskforce on Cybersecurity Education. Since 2000, he has volunteered as an ABET program evaluator and is currently on the Executive Committee of ABET's Computing Accreditation Commission. He received his PhD in Computer and Information Science from The Ohio State University.

Dr. Lawrence G. Jones, Accreditation Board for Engineering and Technology

Dr. Lawrence G. Jones has broad and deep experience in multi-million-dollar project management and software engineering consulting, public speaking, and technical publication. He has over 30 years' experience in nonprofit leadership involving accreditation of university STEM programs, performing arts, and software engineering and computer science education. He is currently Chair of the Board of EPIC, a new, "non-stuffy" chamber music program.

Dr. Jones retired in January 2013 as a Distinguished Principal Researcher at the Software Engineering Institute of Carnegie Mellon University. Larry has over 50 years of experience in software development, management, research, and education. He served a career in the US Air Force and is the former Chair of the Computer Science Department at the US Air Force Academy. Larry is a senior member of the IEEE (Institute for Electrical and Electronics Engineers) and the ACM (Association for Computing Machinery). He is a Fellow of ABET and CSAB. ABET is the recognized authority for accreditation of college programs in engineering, computing, technology and applied science programs. ABET accredits over 4000 programs at over 800 institutions in 32 countries. Over 100,000 students graduate annually from ABET-accredited programs. CSAB is the federation of societies supporting accreditation of undergraduate programs in all aspects computing, software engineering and data science. Larry served as CSAB's Secretary/Treasurer and was the 2015-16 President of ABET leading over 2000 volunteers. He is the 2018 recipient of ABET's highest honor, the Linton Grinter Award for Lifetime Contributions.

Casey W. O'Brien, National CyberWatch Center

Casey W. O'Brien is the Assistant Director for Cyber Defense Education and Training with the Information Trust Institute in The Grainger College of Engineering at the University of Illinois at Urbana-Champaign.

Casey has more than 25 years of large-scale information security and IT engineering, implementation, and management experience in challenging and cutting-edge public and private sector environments.

Casey's teaching and research interests include: practice-centered education and training solutions that combine accelerated learning programs, validated assessments, instruction, practice labs, and challenge scenarios to improve information security talent management in organizations; rapid deployment of customizable and adaptive curriculum that raises learner capability maturity in foundational security concepts, tactics, techniques, and procedures; and formative credentialing solutions that increase the number of capable professionals.

Casey is the Technical Editor of five textbooks: Ethical Hacking & Systems Defense, Linux Server Fundamentals, Information Security Fundamentals, Introduction to Scripting, and Networking Fundamentals.

Casey earned a B.A. in Psychology from the University of St. Thomas and an M.A. in Psychology from Duquesne University.

The Need for ABET Accreditation of Associate's Cybersecurity Programs

Rajendra K. Raj
Rochester Institute of Technology
rkr@cs.rit.edu

Cara Tang
Portland Community College
cara.tang@pcc.edu

David Gibson
United States Air Force Academy
david.gibson@afacademy.af.edu

Lawrence G. Jones
ABET, Inc.
lawrence.g.jones@ieee.org

Casey O'Brien
University of Illinois at Urbana-Champaign
cwobrien@illinois.edu

Abstract

Cybersecurity professionals at all levels of preparation are in high demand, with the need still growing rapidly. In response, community colleges have been offering Associate's programs in cybersecurity for over a decade. The content of such programs has been driven by many factors including the needs of local industry, professional certification requirements for entry-level jobs, and education advancement programs under such organizations as the National Security Agency, the National Institute of Science and Technology (NIST), the National CyberWatch Center, and the Association for Computing Machinery (ACM).

A consequence of this diversity of drivers is wide variation in the types of graduates produced, which is not conducive to developing shared expectations, from prospective students to employers. In addition, as a discipline matures, creating standards for educational programs is a professional responsibility of the academic community, as is establishing accreditation criteria to ensure quality is sustained—enter ABET. This paper summarizes the major efforts that led to Associate's degree programs in cybersecurity, along with the motivation to create the first ABET Associate's Cybersecurity Program Criteria. It discusses the process to develop these cybersecurity criteria, describes the current criteria, and presents the current status of the effort. In essence, this process reflects the maturation of the cybersecurity discipline.

1 Introduction

Cybersecurity professionals at all levels of preparation are in high demand, with predictions that there will continue to be a global shortage in the millions [1]. Given the need for professionals to constantly update cybersecurity skills, community colleges responded by creating Associate's degree programs as far back as 2006.

Current Associate's degree programs in cybersecurity have been largely driven by local industry needs, the curricular requirements of the National Centers of Academic Excellence in Cybersecurity (NCAE-C) Cyber Defense Education designation [2], as well as industry certification programs in cybersecurity (e.g., CISSP [3], CompTIA Security+ [4]). Other efforts to advance the consistency of cybersecurity education have been led by the National CyberWatch Center [5] and NIST's National Initiative for Cybersecurity Education (NICE) [6]. As a consequence, current Associate's programs show a wide variation that is not conducive to developing shared expectations from program graduates, whether they are hired by employers or continue with their studies [7].

ABET's entry into cybersecurity education was motivated by the critical need to address the lack of consensus on what constitutes a solid undergraduate cybersecurity education. An ABET strategic priority has been to stay abreast of the changing landscape of technical education. Initial investigations led by senior ABET volunteers examined alternative credentials, such as professional certification programs, and discovered that many of these were in cybersecurity. As ABET developed its first Cybersecurity Program Criteria for 4-year programs and conducted pilot visits [8], the critical role of Associate's degree programs in cybersecurity education became clear. This motivated ABET's exploration of 2-year cybersecurity programs. Feedback from two years of meetings and conference presentations with key stakeholders in the community college space indicated solid interest from 2-year schools in seeking ABET accreditation.

Helping this effort were two recent related developments that clarify what institutions should cover in their Associate's degree cybersecurity programs and what employers should expect from these graduates. Based on Cybersecurity Curricula 2017 (CSEC 2017) [9] for 4-year programs and other factors appropriate for community colleges, the ACM Committee for Computing Education in Community Colleges (ACM CCECC) published the Cybersecurity Curricular Guidance for Associate-Degree Programs (Cyber2yr2020) [10]. Guided by Cyber2yr2020, CSAB (the ABET member society for computing accreditation) and ABET's Computing Accreditation Commission (CAC) developed the Associate's Cybersecurity program accreditation criteria.

This paper presents the background and current status of these developments at the community college level. Section 2 presents the different approaches that have existed to create cybersecurity curricula at the college level. Based on these developments, Section 3 describes the process used by ABET [11] to develop the Associate's Cybersecurity Program Criteria. Finally, Section 4 discusses the role that ABET's accreditation of Associate's Cybersecurity programs has played in helping to define cybersecurity as an academic discipline.

2 Existing Approaches to Cybersecurity Curricula

This section briefly examines the major efforts in developing curriculum in the cybersecurity space, focusing on efforts in the 2-year space. The major efforts in this space have been:

1. The early and ongoing efforts in the U.S. by the National Security Agency (NSA) and the Department of Homeland Security (DHS) in the National Centers for Academic Excellence in cyber defense education, research, and operations [12].
2. NIST's National Initiative for Cybersecurity Education (NICE) framework [6].
3. Another approach at providing concrete curricula in cybersecurity was the Information Assurance and Computer Forensics set of coursework developed by the National CyberWatch Center [5].
4. The broader efforts by the ACM in building curricular guidance in cybersecurity, chiefly CSEC2017 [9] for 4-year undergraduate programs and Cyber2yr2020 [10] for Associate's degree level programs.

The discussion in this section sets the stage for a discussion of ABET's criteria efforts in the Associate's Cybersecurity arena in Section 3.

2.1 National Centers of Academic Excellence in Cybersecurity (NCAE-C)

NSA and DHS jointly sponsor the NCAE-C program, which has been continuously refined since its inception in 1999 to assist U.S. accredited higher education institutions in advancing the study of cybersecurity to serve the needs of the U.S. government and industry [13].

The NCAE-C program has helped establish standards for cybersecurity curriculum, focusing on cybersecurity competency development for students and faculty. Its ethos is to use collaborations inside and among these institutions for developing a shared-sense of cybersecurity education and practices. Academic institutions may be designated as follows [13]:

1. Cyber Defense Education (CAE-CDE), which is awarded to regionally-accredited institutions that offer cybersecurity degrees and certificates at the Associate's, Bachelor's, or graduate levels.
2. Cyber Research (CAE-R), which is awarded to institutions rated by the Carnegie Foundation Basic Classification system as either as R1, R2 or R3.
3. Cyber Operations (CAE-CO), which is awarded to a "deeply technical, inter-disciplinary, higher education program firmly grounded in the computer science, computer engineering, and/or electrical engineering disciplines, with extensive opportunities for hands-on applications via labs and exercises" [13].

Of these programs, the CAE-CDE is the appropriate designation for 2-year institutions. All programs, including those at the community college level, seeking this designation are required to document their programs of study using Knowledge Units (KUs) as appropriately mapped during the designation process [2]. KUs are categorized as Foundational KUs (required of all programs), Core KUs (either technical or nontechnical) that form the program base, and Optional KUs that can be adopted to document additional aspects of their program of study.

Foundational KUs include Cybersecurity Foundations, Cybersecurity Principles, and IT Systems Components. The selected Technical Core KUs include Basic Cryptography, Basic Networking,

Basic Scripting and Programming, Network Defense, and Operating Systems Concepts, which apply to programs of study aimed at technical jobs. For non-technical jobs, each 2-year school's program must cover the Non-Technical Core KUs, which include Cyber Threats; Cybersecurity Planning and Management; Policy, Legal, Ethics, and Compliance; Security Program Management; and Security Risk Analysis. The Optional KUs can complement the program core: for Technical Core programs, the Non-Technical Core can be used as optional KUs, and vice versa.

To make it easier for programs, students, and employers, the CAE-CDE KUs are also mapped to NICE Framework Categories [2].

2.2 The NICE Framework

As originally envisaged, the NIST's NICE Framework [14] had the following components: seven categories, which are a high-level groupings of common cybersecurity functions; thirty-three specialty areas that are distinct areas of cybersecurity work; and fifty-two work roles that detail groupings in terms of specific knowledge, skills, and abilities (KSAs) needed to perform tasks within each work role. The CAE-CDE KUs are mapped to this version of the NICE framework.

After three-years of use of the original NICE Framework [14], NIST released the first major revision [6]. This revision reflects NIST's better understanding of the changes in cybersecurity and "the way we think about how we do work has changed" [15]. The revised Framework increases flexibility to meet the cybersecurity needs of diverse public and private sector stakeholders, thus permitting organizations to tailor the Framework to their unique situations. The main building blocks of the NICE Framework are Tasks, Knowledge, and Skills, which enable the description of "the work" and "the learner" concepts, which helps define a common language to describe cybersecurity work. The revision re-introduces competencies as a mechanism that students, current employees, and job seekers can use to show they have the needed cybersecurity knowledge and skills. Finally, the revision focuses on only the core content, thus reducing the 145 pages in the original Framework [14] to the 27 pages in the revised Framework [6].

2.3 The National CyberWatch curricula

Quality cybersecurity curriculum was in short supply in 2005 when National CyberWatch [5] started and eventually transitioned to a National Science Foundation (NSF) Advanced Technological Education (ATE) National Center for Cybersecurity [16]. The Center worked in conjunction with founding member Anne Arundel Community College in Maryland and developed model Information Assurance and Computer Forensics curricula. This work developed complete courses and multiple degrees and certificates supporting the growth of cybersecurity education nationally. Building on its model curriculum base, the National CyberWatch Center expanded the reach of cybersecurity education curricula in several other ways, including new degree programs, stackable certificate templates, faculty professional development workshops, state-of-the-art virtual lab environments, and articulation and pathways models.

Curriculum development has been guided by the following principles:

- Relevance to employers, students, and schools.

Table 1: Cyber2yr2020: Domains and Crosscutting Concepts

8 Domains	Data Security, Software Security, Component Security, Connection Security, System Security, Human Security, Organizational Security, Societal Security.
6 Crosscutting Concepts	Confidentiality, Integrity, Availability, Risk, Adversarial Thinking, Systems Thinking.

- Alignment to work roles backed by input from commercial and federal partners, as well as labor market demand sources.
- Modularity for easy adoption by a variety of schools.
- Continuous improvement practices.
- Mappings applied to work roles and professional certifications.
- Model articulations with four-year schools.

The technical courses in the National CyberWatch Center degree and certificate programs align to various industry-recognized professional certifications, workforce and competency frameworks, and various work roles. They also provide the necessary information for schools to get approval through their internal Curriculum Instruction Committees [17].

2.4 The Cyber2yr2020 Curricular Guidance for Associate's Programs

ACM has been publishing curriculum guidelines for computing disciplines for decades, and one of the newest disciplines in this series is Cybersecurity. In 2017, ACM published CSEC2017 [9] for Baccalaureate-level programs in Cybersecurity, and in 2020 the ACM Committee for Computing Education in Community Colleges (CCECC) followed with Cyber2yr2020 [10] for Associate's degree programs. Based on CSEC2017, the content of Cyber2yr2020 has been updated for currency and appropriateness at the two-year level. In addition to CSEC2017, other relevant sources that have influenced the guidelines include the CAE-CDE 2-Year Knowledge Units [2] and the NICE Cybersecurity Workforce Framework [6]. The scope of Cyber2yr2020 includes both transfer and career-oriented Associate's degree programs in Cybersecurity.

The Cyber2yr2020 curriculum framework contains 58 competencies across eight security domains plus cross-cutting concepts. The focus on competencies over knowledge is a relatively new development in ACM curriculum guidelines. A competency integrates knowledge, skills, and dispositions in context, where dispositions are "attitudinal, behavioral, and socio-emotional qualities of how disposed people are to apply knowledge and skills to solve problems" [18].

The Cyber2yr2020 framework [10] maintains CSEC2017's division of cybersecurity content into eight domains, which were called "knowledge areas" in CSEC2017 [9]. It also weaves the six CSEC2017 crosscutting concepts throughout the eight domains. These domains and crosscutting concepts are showed in Table 1.

In Cyber2yr2020, each domain has a handful of high-level competencies marked as either essential or supplemental, totaling 58 competencies across the eight domains and cross-cutting concepts.

Each domain is also further divided into subdomains which contain more detailed learning outcomes, also marked as essential or supplemental. The essential portion of the guidelines represents content appropriate for any and all cybersecurity programs at the 2-year level, whereas the supplemental represents content that is appropriate for some programs, depending on program focus. All essential learning outcomes are accompanied by a three-tiered assessment rubric representing emerging, developed, and highly developed standards for the learning outcome. To further support integration into competency-based curricula, competencies and learning outcomes are expressed using action verbs from Bloom's Revised Taxonomy as used in Cyber2yr2000 [19].

The content of Cyber2yr2020 has been aligned with the NICE Cybersecurity Workforce Framework, as well as with the CAE-CDE 2-Year Knowledge Units (KUs). The Cyber2yr2020 competencies and learning outcomes map to 100% of the outcomes and topics found in the Foundational Core and Technical Core CAE-CDE KUs. In addition, Cyber2yr2020 offers program examples: specific two-year Cybersecurity programs that have mapped the competencies of Cyber2yr2020 to the program courses they are covered in. Program examples demonstrate the adaptability and applicability of the curricular framework.

3 The ABET Associate's Program Criteria for Cybersecurity

As part of ABET's Strategic Priorities, a project jointly sponsored by CSAB [20] and ABET's Computing Accreditation Commission (CAC) was launched in July 2017 to investigate the role that ABET could play in accrediting Associate's degree programs in cybersecurity. The team comprising leadership of both bodies actively engaged with community college leaders in cybersecurity and received strong encouragement for ABET to enter this space.

Initial outreach and listening sessions to aid criteria development were held at the following conferences: the Community College Cyber Summit (3CS) in 2017 and 2018; the National Initiative of Cybersecurity Education (NICE) in 2017; the National Cyber Summit (NCS) in 2018; and the Colloquium for Information Systems Security Education (CISSE) in 2018. Follow-up outreach continues at these and other venues. As a result, the team concluded that ABET had a compelling role to play in strengthening cybersecurity education at the community college level in addition to at the 4-year level.

The ABET team engaged actively with all existing curricular efforts mentioned in Section 2. ABET developed strong collaborations with the NCAE-C Program Office, the NICE leadership team, the National CyberWatch Center, and the Cyber2yr2020 efforts. Specifically, the team worked closely with the NSA team leading the NCAE-C program, with several joint conference presentations, a joint agreement on the value proposition of both the CAE-CDE designation and ABET accreditation. This included discussion of aligning the CAE-CDE application and ABET self-study processes where possible, as well as participation and observation by both parties of the other's processes. The focus was on integrating and improving cybersecurity education at the collegiate level.

With this community support, the team formed a 2-Year Cybersecurity Program Criteria Committee. The committee was able to make rapid progress thanks to the existence of 4-year Cybersecurity Program Criteria adopted in 2017 and the initial Cyber2yr2020 drafts. Other useful inputs to the process were existing experiences by ABET's Engineering Technology Accreditation Commission

at the Associate's level, the CAE-CDE requirements at the community college level, as well as the NICE Framework.

The Associate's Cybersecurity Program Criteria were developed and presented for public feedback during January-May of 2019. The refined criteria received initial approval from ABET's CAC in July 2019. This approval allowed pilot accreditation visits to be conducted in the fall of 2020 for the 2020-21 review cycle. Based on Fall 2020 pilot visits, a few minor revisions to Criterion 5 have been proposed. With these revisions, the Associate's Cybersecurity Program Criteria are likely to receive final approval from the CAC in July 2021. With final approval at ABET in Fall 2021, the criteria will be released for general use.

Based on the ACM's CSEC2017 [9], ABET's Cybersecurity Program Criteria for Baccalaureate programs were approved in 2017. ABET has since accredited 15 4-year cybersecurity programs, with several more programs under review in the 2020-21 accreditation cycle.

3.1 Criteria Overview

This subsection describes ABET's Associate's Cybersecurity Program Criteria.

ABET Criteria are designed to ensure that accredited programs provide a high-quality education that meets the needs of the program's constituents. All ABET criteria for computing, engineering, engineering technology and applied and natural sciences, are composed of the following eight criteria, which are briefly described.

1. Students: requires evaluation of student performance, monitoring student progress, policies for transfer students and credits, and procedures to ensure program graduates meet all graduation requirements.
2. Program Educational Objectives: requires establishment and maintenance of Program Educational Objectives that say what graduates should attain a few years after graduation and address the needs of the program's constituents.
3. Student Outcomes: discussed in depth below.
4. Continuous Improvement: requires processes for assessing and evaluating the extent to which the Student Outcomes are being attained and using this information for continuous program improvement.
5. Curriculum: discussed in depth below.
6. Faculty: requires a faculty of an appropriate size with the qualifications, competence, breadth and depth of knowledge, and authority to provide instruction and advising as well as program continuity, stability, and oversight.
7. Facilities: requires adequate and maintained classrooms, offices, laboratories, library services, tools, equipment, and computing resources.
8. Institutional Support: requires institutional support of the program to attract and maintain faculty, staff, and resources adequate to ensure the quality and continuity of the program.

Table 2: Associate's Cybersecurity, Criterion 3, Student Outcomes

Graduates of the program will have an ability to:
1. Analyze a broadly-defined security problem and apply principles of cybersecurity to the design and implementation of solutions.
2. Apply security principles and practices to maintain operations in the presence of risks and threats.
3. Communicate effectively in a variety of professional contexts.
4. Recognize professional responsibilities and make informed judgments in cybersecurity practice based on legal and ethical principles.
5. Function effectively as a member of a team engaged in cybersecurity activities.

Criteria 1, 2, 4, 7 and 8 are "harmonized" across all four ABET commissions, meaning the same understanding applies to all programs accredited by ABET regardless of commission and regardless of level (Associate's, Baccalaureate, and Masters). The other criteria vary by commission, and often by the type of program being accredited.

3.1.1 Criterion 3, Student Outcomes

ABET defines Student Outcomes as what students are expected to know and be able to do by the time of graduation. Student Outcomes thus relate to the knowledge, skills, and behaviors that students acquire as they progress through the program. Table 2 lists the five outcomes that Associate's Cybersecurity programs seeking ABET accreditation need to adopt.

These Student Outcomes must be publicly stated, typically on a program's website and in institutional catalogs. The program may define additional outcomes. Although these five Student Outcomes are similar to ABET's Student Outcomes for programs in other disciplines, especially other computing disciplines, they are unique to Associate Cybersecurity programs. The key aspect of having such outcomes is that an accredited program must regularly to assess and evaluate the extent to which each outcome is being attained in accordance with the continuous improvement imposed by Criterion 4.

Student Outcomes for the Associate's Cybersecurity Program Criteria address design and implementation of solutions, communication skills, profession responsibilities, and teamwork. The five Associate's Cybersecurity student provide a narrower focus on cybersecurity principles and practices. In particular, the second outcome, which focuses on maintenance of operations in the presence of risks and threats, captures what many believe is the key distinction between cybersecurity and other computing disciplines.

3.1.2 Criterion 5, Curriculum

Table 3 shows the proposed Associate's Cybersecurity Program Criterion 5 that includes minor revisions from the initial version approved in 2019. This criterion lays out the curricular requirements for an accredited Associate Cybersecurity program. It is designed to ensure program graduates gain the cybersecurity knowledge and skills required for a career and lifelong professional development in cybersecurity. At the same time, this criterion allows a program significant flexibility in how it covers required topics areas and in the cybersecurity areas it chooses to emphasize.

Table 3: Associate's Cybersecurity, Criterion 5, Curriculum

The program's requirements must be consistent with its program educational objectives and designed in such a way that each of the student outcomes can be attained. The curriculum must combine technical, professional, and general education components to prepare students for a career and lifelong professional development in the cybersecurity discipline.

The program must include at least 30 semester credit hours (or equivalent) of up-to-date coverage that includes:

1. Application of techniques, skills, and tools necessary for cybersecurity practice.
2. Application of the crosscutting concepts of confidentiality, integrity, availability, risk, adversarial thinking and systems thinking.
3. Cybersecurity topics from each of the following areas:
   a) Data Security: protection of data at rest, during processing, and in transit.
   b) Software Security: development and use of software that reliably preserves the security properties of the protected information and systems.
   c) Component Security: the security aspects of the design, procurement, testing, analysis, and maintenance of components integrated into larger systems.
   d) Connection Security: security of the connections between components, both physical and logical.
   e) System Security: security aspects of systems that use software and are composed of components and connections.
   f) Human Security: the study of human behavior in the context of data protection, privacy, and threat mitigation.
   g) Organizational Security: protecting organizations from cybersecurity threats and managing risk to support successful accomplishment of the organizations' missions.
   h) Societal Security: aspects of cybersecurity that broadly impact society as a whole.
4. Programming or scripting skills.
5. Advanced cybersecurity topics that build on the above crosscutting concepts and cybersecurity topics.

The program must ensure its students have the mathematical skills required to meet its student outcomes and program educational objectives.

Criterion 5 requires a minimum of 30 semester credit hours (or equivalent) of up-to-date coverage of cybersecurity topics, but does not specify how many hours a program must dedicate to specific topic areas. Given this flexibility, a key requirement is that the program's curriculum be designed in such a way that the student outcomes (Criterion 3) can be attained.

The eight required topic areas and the six crosscutting concepts in Criterion 5 are identical to the eight security domains in Cyber2yr2020 [10]. As Cyber2yr2020 recommends, Criterion 5 requires some coverage of topics in all eight security domains. However, the Associate's Cybersecurity Program Criteria by design do not prescribe how much coverage is required in each area nor which specific competencies must be addressed. Associate's degree programs that adopt the recommendations of Cyber2yr2020, with at least 30 semester credits of cybersecurity topics, will likely satisfy the curricular requirements for the Associate's Cybersecurity accreditation criteria.

4 Status and Final Remarks

ABET's initial Associate's Cybersecurity Program Criteria worked well when applied in the first two pilot program reviews of community college cybersecurity programs in the fall of 2020. The results of these pilot reviews will be finalized in July 2021 and reported to the programs the following month. ABET is conducting an additional pilot Associate Cybersecurity program pilot review in the 2021-22 accreditation cycle. After the final approval of these criteria in Fall 2021, any Associate's degree cybersecurity program will be able to seek ABET accreditation with a review in the 2022-23 cycle or later.

ABET takes its own quality improvement processes seriously and encourages readers to provide year-long feedback to any Proposed Changes to the accreditation criteria [11].

Finally, it should be noted that the processes used to develop and pilot the Associate's cybersecurity accreditation criteria have laid out general principles for creating Associate's criteria in other computing disciplines, such as computer science or information technology, and newer disciplines, such as data science and artificial intelligence.

Acknowledgments

Edward Sobiesk and Mary Marchegiano also served on the Joint CSAB/CAC Associate's Cybersecurity Criteria Subcommittee and helped to develop the Associate's Cybersecurity Criteria. We thank Elizabeth Hawthorne, Scott Hillman, Stephen Miller, Pam Schmelz, Brandon Sesser, Christian Servin, Melissa Stange, Mary Wallingsford, as well as others who provided input over the past three years. Raj acknowledges support by the National Science Foundation under Award 2021287.

References

[1] Kyle Guercio. Cybersecurity Employment Outlook 2021, December 2020. https://www.esecurityplanet.com/trends/cybersecurity-employment-2021/.

[2] US National Security Agency. Academic Requirements for Designation as a CAE in Cyber Operations, 2019. https://www.nsa.gov/Resources/Students-Educators/centers-academic-excellence/cae-co-fundamental/requirements/\#m8, Accessed Jan 18, 2020.

[3] (ISC)^2, Inc. CISSP—The World's Premier Cybersecurity Certification, 2021. https://www.isc2.org/Certifications/CISSP#.

[4] CompTIA, Inc. CompTIA Security+, 2021. https://www.comptia.org/certifications/security.

[5] National CyberWatch Center. Information Security Curriculum Guide, 2021. https://www.nationalcyberwatch.org/resource/curriculum-guide/.

[6] National Institute of Standards and Technology. NICE Cybersecurity Workforce Framework. NIST Special Publication 800-181 Revision 1, 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf.

[7] Rajendra K. Raj and Allen Parrish. Toward standards in undergraduate cybersecurity education in 2018. *Computer*, 51(2):72–75, 2018. doi: 10.1109/MC.2018.1451658.

[8] Rajendra K. Raj, Vijay Anand, David Gibson, Siddharth Kaza, and Andrew Phillips. Cybersecurity program accreditation: Benefits and challenges. In *Proceedings of the 50th ACM Technical Symposium on Computer Science Education*, SIGCSE '19, page 173–174, New York, NY, USA, 2019. Association for Computing Machinery. ISBN 9781450358903. doi: 10.1145/3287324.3287325. https://doi-org.ezproxy.rit.edu/10.1145/3287324.3287325.

[9] Joint Task Force on Cybersecurity Education. Cybersecurity curricula 2017. Technical report, ACM, IEEE-CS, AIS SIGSEC, and IFIP WG 11.8, December 2017. https://dl.acm.org/citation.cfm?id=3184594, doi = 10.1145/3184594.

[10] Cara Tang, Cindy Tucker, Christian Servin, Markus Geissler, Melissa Stange, Nancy Jones, James Kolasa, Amelia Phillips, Lambros Piskopos, and Pam Schmelz. *Cybersecurity Curricular Guidance for Associate-Degree Programs*. Association for Computing Machinery, New York, NY, USA, 2020. ISBN 9781450375559.

[11] ABET, Inc. Criteria for accrediting computing programs. effective for review during the 2021-22 accreditation cycle, 2021. https://www.abet.org/wp-content/uploads/2021/01/C001-21-22-CAC-Criteria.pdf.

[12] US National Security Agency and the Department of Homeland Security. Centers of Academic Excellence in Cybersecurity, 2018. https://www.nsa.gov/resources/educators/centers-academic-excellence.

[13] National Security Agency Central Security Service. National Center of Academic Excellence in Cybersecurity (NCAE-C), 2021. https://www.nsa.gov/resources/students-educators/centers-academic-excellence/.

[14] National Institute of Standards and Technology. NICE Cybersecurity Workforce Framework. NIST Special Publication 800-181, 2017. https://doi.org/10.6028/NIST.SP.800-18.

[15] Danielle Santos. Back to the Basics: Announcing the New NICE Framework, November 2020. https://www.nist.gov/blogs/cybersecurity-insights/back-basics-announcing-new-nice-framework.

[16] National Science Foundation. National CyberWatch: Cybersecurity Education Solutions for the Nation, 2012. https://www.nsf.gov/awardsearch/showAward?AWD_ID=1204533.

[17] National CyberWatch Center. Technical courses, 2021. https://www.nationalcyberwatch.org/programs-resources/curriculum/technical-courses/.

[18] Stephen Frezza, Mats Daniels, Arnold Pears, Åsa Cajander, Viggo Kann, Amanpreet Kapoor, Roger McDermott, Anne-Kathrin Peters, Mihaela Sabin, and Charles Wallace. Modelling competencies for computing education beyond 2020: A research based approach to defining competencies in the computing disciplines. In *Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education*, ITiCSE 2018 Companion, page 148–174, New York, 2018. ACM. https://doi.org/10.1145/3293881.3295782.

[19] ACM Committee for Computing Education in Community Colleges (CCECC). Bloom's revised taxonomy, 2020. https://ccecc.acm.org/assessment/blooms.

[20] CSAB, Inc. CSAB webpage, 2021. http://csab.org.