Final Report of the Cyber Education Project (CEP) Accreditation Committee

March 14, 2016

Co-chairs:

C. Steven Lingafelt ─ cepaccreditationcochair.steven@gmail.com

Raymond Greenlaw ─ raymond.greenlaw@gmail.com

Executive Summary

In support of the *Cyber Education Project (CEP)*, www.cybereducationproject.org, the Accreditation Committee was formed. This report highlights work of the Accreditation Committee. The committee was charged to

A) Develop draft ABET Computing Accreditation Commission (CAC) Program Criteria for the "Cyber Sciences" based on

1. Results from the CEP's Learning Outcomes Committee
2. Existing related draft bodies of knowledge/curriculum maps
3. Existing relevant computing-based curricula
4. Input from interested stakeholders.

B) Propose, revise, and update draft Program Criteria, as appropriate; and help ABET, CSAB, IEEE, IEEE-CS, ACM, AIS, and other interested professional societies (as they desired to participate) solicit constituent feedback on prototype Program Criteria.

The committee of volunteering individuals and organizations created an "Alpha draft" using various collaboration tools and methods in late 2015. At the Memphis SIGCSE conference, the "Alpha" draft was revised to a "Beta" version. In March 2015, this version was conveyed by Andy Phillips to a CSAB/CAC committee for their continued efforts toward accreditation criteria. This concluded the work of the CEP Accreditation committee.

The significant artifacts representing the committee activities and work products are in the artifact section of the CEP website at www.cybereducationproject.org/project-artifacts.

The co-chairs of the Accreditation Committee would like to thank all of the members of the Accreditation Committee, the CEP members and other participants for their valuable contributions and volunteer work toward this effort.

Table of Contents

Committee Work Approach and Activities

Preparation Phase

Phase Goal: Our goal was to provide all of the needed resources for the Accreditation Committee's success and to prepare members to contribute at a high level.

Assembling the Team

Members voluntarily joined the Accreditation Committee based on solicitation at various events, reading the CEP web site, and personal request. The majority of members had joined by June, 2015, with a few additional members joining in the 2nd half of 2015. A list of members is contained in the appendix of this document. The members made many valuable contributions to this work and for that the co-chairs are extremely grateful.

Collaboration Tools

1) A collaboration space was established using Google Drive, shared documents, and a moderated Google Group with posting and email notification:

   - Google Drive folder: https://drive.google.com/folderview?id=0Byw6slrolpwjei1aLTF4TGhaR0k&usp=sharing
   - Google Group name: CEPaccreditationcommittee
   - Google Group email: cepaccreditationcommittee@googlegroups.com

2) In addition to the Google tools, the committee utilized conference calls for review meetings.

Training and Knowledge

1) A document (*Cyber Education Project (CEP) Accreditation Committee Operational Methods and Practices*) was written and provided to committee members describing:

   - Logistical considerations, including the process for becoming a member of the Accreditation Committee, the method for intra-committee communications, and "how to" information on the use of the Google collaboration tools
   - The structure of the existing Criteria with a focus and commentary on its intersection with CEP's proposed Criteria
   - A time line of committee activities

   A copy of this document is retrained on the Artifacts page of the CEP web site.

2) Training by Art Price (CEP project's ABET focal point) for how to conceptualize and write high-quality criteria was provided to committee members in September 2015. This training was recorded for playback by those unable to attend the training session.

   A copy of the education materials and recording of the training is retained in the Artifacts page of the CEP web site.

3) A pre-public draft of the Learning Outcomes Report, describing topics and learning outcomes was provided to the committee members.

   The subsequent public released Learning Outcomes Report is retained in the Artifacts page of the CEP web site.

Deliberation Phase

Phase Goal: To discussion, deliberate, and consider Criteria, publishing a first draft by the end of 2015.

Following the activation of the collaboration tools and the training, the team received and considered the (draft) Learning Outcomes Committee's observations and recommendations. The team systematically debated the various topics on conference calls, the Google Group forum, and emails, yielding a draft Program Criteria.

The draft was reviewed by the CEP steering committee, resulting in minor modifications.

This draft was published as an "Alpha draft" in November, 2015 and is retained in the Artifacts page of the CEP web site and in the appendices of this report.

At the Memphis SIGCSE conference, the Alpha draft was reviewed and the modifications were published as a "Beta" draft which is retained in the Artifacts page of the CEP web site and in the appendices of this report.

Submit Phase

Phase Goal: To submit the draft Program Criteria to a receiving organization who can continue the process toward ABET acceptance and program utilization.

Andy Phillips presented the "Beta" draft (March 13, 2016) to CSAB for their use in the creation of program criteria. The name of the program criteria has not been finalized, however, at the time of this writing; it appears that the name may be cybersecurity.

This concluded the CEP Accreditation Committee work.

Notable Discussion Topics

Discussions on Existing Criteria

These comments are based on an assessment of existing Program Criteria for CAC (Computer Science, Information Systems, and Information Technology) and EAC (Electrical, Computer, Telecommunication Engineering).

- On average a Program Criteria is one-half a page in length. In general, it is concise and not overly detailed nor prescriptive.
- Program Criteria may specify additional program specific requirements in the areas of Student Outcomes, Curriculum, and Faculty.
- Computer Science has two additional Student Outcomes, Information Systems one, and Information Technology five. Such Student Outcomes always follow a similar format to those contained in the General Criterion Student Outcomes, for example, in Information Technology Student Outcome (k) is an ability to identify and analyze user needs and take them into account in the selection, creation, evaluation and administration of computer-based systems.
- The Curriculum Criterion is the most prescriptive. It typically contains specific topics that must be covered in the program and/or the amount of coverage of such topics, for example, in Information Systems students must have quantitative analysis or methods including statistics and in Computer Science students must have one year of mathematics and science. The statements about material to be covered include broad topics, for example, in Information Technology students must have coverage of the fundamental of system administration and maintenance. Electrical, Computer, Telecommunications Engineering can have up to six additional curriculum requirements, depending on the program's title.
- Computer Science and Information Systems have additional Faculty Criterion requirements. In both cases the requirements begin "Some full-time faculty members …" And, concludes with a statement about the terminal degree. Information Technology does not specify any additional faculty requirements.
- Criteria additions may be selectively applied based on "modifiers" to the program's title. For example, the current EAC engineering programs with a modifier of "telecommunication(s)" in the program's title, have an additional curriculum requirement stated as follows: "The curriculum for programs containing the modifier "telecommunication(s)" must include design and operation of telecommunication networks for services such as voice, data, image, and video transport."

Discussion on Criteria applicable to topics of "Cyber Sciences"

NOTE: The program name(s) associated with the Program Criteria applicable to the topics of "Cyber Sciences" were not established at the time of the committee's work. This was anticipated by the committee to occur later in this process. In February, prior to the March 4th Memphis SIGCSE meeting, the name cybersecurity was established, thus the following recounting of major discussion points will use the term "cyber sciences" as this was the term of art in use at the time of the discussion.

Note that the "Alpha" version was released in November, 2015. The "Beta" version was released March 5th, 2016 (immediately following the SIGCSE workshop).

Scope

It was expected that the Program Criteria for topics of "Cyber Sciences" resemble those of other programs that ABET accredits, as ABET strives for consistency in Program Criteria and the General Criteria. Based on the previous observations, the scope of the Program Criteria was expected to be at most a few additional

- Student Outcomes
- Curriculum topics (and potentially the minimum duration of study for selected topics)
- Faculty requirements

Deviation from the standard ABET Program Criteria structure and scope was viewed as highly unlikely, and would require clear and convincing justification.

"Cyber Sciences" is a term of art ─ useful as a method to categorize a broad set of cyber-related disciplines. Typically, Program Criteria are for a specific program. Thus, it was viewed that proposed Program Criteria would not be as broad as the set of cyber-related disciplines, topics, and studies that "Cyber Sciences" could be considered to encompass.

Criteria Articulation

Given ABET's two models for Criteria articulation:

1. By program name – for example, the CAC has three separate programs
2. By modifier within a single program – for example, the EAC has a single program with six different (program) requirements based on the program-name modifier.

In the same fashion, there may develop additional independent program names, as in the CAC model and/or additional program requirements based on "modifiers" to a single program name, as in the EAC model. This committee did not attempt to resolve or recommend a method of criteria articulation with respect to program names or modifiers.

Criteria 3 (Student Outcomes) and 5 (Curriculum)

The Learning Outcomes Committee developed a set of learning outcomes that provided fundamental guidance for the Accreditation Committee. From the Learning Outcomes Committee's material and other material identified as significant, the Accreditation Committee produced a set of Student Outcomes (in alignment with the current General Computing Criterion 3) that by consensus the committee determined as required to fulfill the intent of the Learning Outcomes Committee's efforts.

By the nature of the ABET-Criteria structure, these Student Outcomes are broad topics that are essential to have in "Cyber Science" courses of study. In some instances, the Student Outcomes are accompanied by curriculum (in alignment with the current General Computing Criterion 5) requirements that may also have a minimum duration of study for the topic.

Within criterion 3, the committee reflected that:

> Security was more than a single component's technical attributes. Security included physical, software and human aspects. Security was reflective of the system, which may be composed of multiple components. These components include a physical embodiment (i.e., software and/or hardware), and a human component (i.e. a user, a policy or regulation). In addition, the components exist within a physical environment that is part of the "system". Thus the term "system" was selected to convey that security was broader than a specific physical object and will, in many cases,

have a primary human component and/or have significant physical environment consideration. For example, in an air traffic control system, the physical security of the "server room" and the physical access to the server's themselves, as well as the firmware within the server, as well as the plane tracking application, as well as the server and application administrators, as well as the end user air traffic controller are all components of the "system".

Within criterion 3, the SIGCSE review observed that a distinctive of these programs is the notion of protection of the system from a "bad" event and reflected in the phrase "in the presence of risks and threats." The concept of "risks and threats" includes both non-human actors (a natural disaster) as well as non-adversarial, potentially unintentional actions (exposure of sensitive information from sending an email to the "wrong" person).

Within criterion 5, the SIGCSE review observed that the fundamentals of cybersecurity were not fully established as terms of art, and thus included illustrations to provide context and illustrations of the terms. The formulation "such as" without "or" or "and" preceding the last element in the illustrative list was intentional to convey that the list is illustrative only -- not a required list and is not comprehensive.

The bold font improves readability during the review process and is not suggested to be included in the final form.

Criterion 7 (Faculty)

The Accreditation Committee determined that it was necessary to include a statement with respect to faculty qualifications. However, the committee noted that in this new field, due to a shortage of qualified faculty, it might be impractical for a program to have faculty members with a terminal degree with a program of study in "Cyber Sciences" or a closely related field. An assessment of this concern is recommended prior to the final release of an ABET Program Criteria.

Open and Unresolved Topics

Criteria Name

The selection of the Program Criteria name was explicitly not considered by the Accreditation Committee. From observation, the name engenders vigorous debate in some forums. To some, "Cyber Sciences" represents a broad set of topics, and thus multiple different programs, perhaps with multiple different accreditation bodies, not restricted to ABET. To others, in order to implement a "first" accreditation Program Criteria, the initial Program Criteria must be associated with one or few areas of the "Cyber Sciences" arena, and thus, the name would be necessarily narrower in its scope. It is observed that the name of the criteria may not be the identical name of the program.

The criteria name has implications on which ABET commission may sponsor the criteria. The topic of alignment with or sponsorship by one or more ABET commissions was explicitly not considered by the Accreditation Committee.

Articulation of the Program Criteria Content

The proposed Program Criteria text could be modified and its intent added to existing Program Criteria, for example, the CAC-covered programs of Computer Science, Information Systems, or Information Technology or the EAC-covered program of Software Engineering, and/or described in a new Program Criteria.

Appendix

Alpha Draft Criteria

Note that the existing CAC Criteria are not reprinted in this section. The following contains only the new Program Criteria for "Cyber Sciences," as it was drafted by the Accreditation Committee. For a full reading of the CAC criterion, see http://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-computing-programs-2015-2016/

Alpha Draft – "Cyber Sciences" Program Criteria
PROGRAM CRITERIA FOR CYBER SCIENCES
AND SIMILARLY NAMED COMPUTING PROGRAMS

Lead Society: CSAB

These program criteria apply to computing programs using computer security, cyber operations, cyber security, information assurance, information security, or similar terms in their titles.

3. Student Outcomes
The student outcomes for cyber sciences programs must include outcomes (6) and (7).

(6) An ability to apply security principles and practices to design and implement computing systems with consideration of the physical, software, and human aspects of the computing system.

(7) An ability to analyze and evaluate cyber systems with respect to security and maintaining operations.

5. Curriculum
Students must have course work or an equivalent educational experience as specified below:

a. Cyber sciences: One and one-third years that includes fundamentals and application of:
   1. Cyber defense and digital forensics.
   2. A variety of computing systems and tools appropriate to cyber sciences.
   3. Cyber ethics, policy, governance, law, and risk management.

b. Behavioral Science: Material that develops an understanding of human behavior relating to cyber systems and operations, including social engineering, social networks, user experience, and organizational behavior.

6. Faculty
Some full-time faculty members, including those responsible for the cyber sciences curriculum development, must hold a terminal degree with a program of study in cyber sciences or a closely related field.

Beta Draft Criteria

Beta Draft – "Cybersecurity" Program Criteria
PROGRAM CRITERIA FOR CYBERSECURITY
AND SIMILARLY NAMED COMPUTING PROGRAMS

Lead Society: CSAB

These program criteria apply to computing programs using cybersecurity, computer security, cyber operations, information assurance, information security, or similar terms in their titles.

3. Student Outcomes
The student outcomes for cybersecurity programs must include outcomes (6) and (7).

(6) An ability to apply security principles and practices to the design and implementation of the physical, software, and human components of the system.

(7) An ability to analyze and evaluate cyber systems with respect to security and maintaining operations in the presence of risks and threats.

5. Curriculum
Students have course work or equivalent educational experiences that include the fundamentals of cybersecurity:

1. **Cyber Defense,** such as cryptography, data security, network security, information assurance.
2. **Cyber Operations**, such as cyber attack, penetration testing, cyber intelligence, reverse engineering, cryptanalysis.
3. **Digital Forensics,** such as hardware and software forensics, incident response, cybercrime, cyber law enforcement.
4. **Cyber Physical Systems**, such as Supervisory Control and Data Acquisition (SCADA) systems, internet-of-things (IOT), industrial control systems.
5. **Secure Software Development**, such as secure systems design, secure coding, deployability, maintainability, usability of secure information system.
6. **Cyber Ethics**, such as ethical use of information systems, privacy and anonymity, intellectual property rights, professional responsibility, global societal impact of information systems.
7. **Cyber Policy, Governance, and Law**, such as government and institutional cyber policy and practices, regulatory authorities for cyber systems and operations, cyber law.
8. **Cyber Risk Management**, such as cyber resilience, mission assurance, disaster recover, business continuity, security evaluation, cyber economics.
9. **Human Behavior Relating to Cyber Systems and Operations,** such as social engineering, social networks, user experience, and organizational behavior.

6. Faculty
At least some full-time faculty members, including those responsible for the cybersecurity curriculum development, must hold a terminal degree with a program of study in cybersecurity or a closely related field.

Accreditation Committee Composition

Co-chairs

- C. Steven Lingafelt – IEEE CEAA, IBM
- Raymond Greenlaw – United States Naval Academy

Members

Name	Representing Organization	Location	Org. Type A = Academic G = Government I = Industry P = Prof. Society
Steve Beaty	MSU Denver	Denver, CO	A
Jean Blair	Military (Army) Academy	West Point, NY	G
Doris Carver	Louisiana State University	Baton Rouge, LA	A
Marcin Filipiak	IBM Poland	Poznan, Poland	I
Tirthankar Ghosh	St. Cloud State University	Cloud, MN	A
John Impagliazzo	Hofstra University	Fort Salonga, NY	A
Nancy Miller	Grantham University	Lenexa, KS	A
Allen Parrish	University of Alabama	Tuscaloosa, AL	A
Andrew Phillips	Naval Academy	Annapolis, MD	G
Prakash Ranganathan	University of North Dakota	Grand Forks, ND	A
Stephen Seidman	Texas State University	San Marcos, TX	A
Mark Stockman	University of Cincinnati	Cincinnati, Ohio	A
Pearl Wang	George Mason University	Fairfax, VA	A
Vera Zdravlovich	Senior Advisor at CyberWatch, Prince George's Community College	Largo, MD	I

Note that any person who volunteered was accepted as member of the committee.

In addition, the IEEE-CS professional society provided a named representative, Stephen Seidman.

ABET provided a named ABET focal, Art Price.

SIGCSE Workshop Participants

Jean Blair

Scott Buck

Doris Carver

Belinda Copus

Sue Fitzgerald

David “Hoot” Gibson

Harold Grossman

John Impagliazzo

Sidd Kaza

Steven Lingafelt

Allen Parrish

Andrew Phillips

Art Price

Mark Stockman

CEP Committee Composition

Steering Committee

- Chair: Andy Phillips, United States Naval Academy
- Co-chair: Jean Blair, United States Military Academy
- Communications: Allen Parrish, The University of Alabama
- Chief of Staff: Chris Inglis, United States Naval Academy
- And all of the others listed on the following committees

Stakeholder Committee

- Co-chair: Sue Fitzgerald, Metropolitan State University
- Co-chair: Diana Burley, George Washington University

Learning Outcomes Committee

- Co-chair: David Gibson, U.S. Air Force Academy
- Co-chair: Elizabeth Hawthorne, Union County College

Industry Advisory Board

- Chair: Scott Buck – Intel Corporation

Accreditation Committee

- Co-chair: Raymond Greenlaw, United States Naval Academy
- Co-chair: Steven Lingafelt, IEEE CEAA, IBM

Glossary

Acronym	Name	Link
ABET	The organization prior to 2005 known as the Accreditation Board for Engineering and Technology	www.abet.org
ACM	Association for Computing Machinery	www.acm.org
AIS	Association for Information Systems	aisnet.org
CAC	Computing Accreditation Commission	www.abet.org/about-abet/governance/accreditation-commissions/computing-accreditation-commission/
CEP	Cyber Education Project	www.cybereducationproject.org
CSAB	Computing Sciences Accreditation Board	www.csab.org
EAC	Engineering Accreditation Commission	www.abet.org/about-abet/governance/accreditation-commissions/engineering-accreditation-commission/
IEEE	Institute of Electrical and Electronics Engineers	www.ieee.org
IEEE-CS	IEEE Computer Society	www.computer.org

Acknowledgments

The co-chairs of the Accreditation Committee thank all of the members of the Accreditation Committee for their valuable contributions and volunteer work toward this effort. Your efforts are greatly appreciated and valued. We also thank all members of the Steering Committee for their important contributions and efforts to this work, and for their collaborative and giving nature. And, finally, thanks to Andy Phillips for his valuable and untiring leadership and focus during the Cyber Education Project.