An Interactive Workshop on Draft Program Criteria for Cyber Sciences

ABET Symposium – April 2016

Led by members of the Cyber Education Project (CEP)

Andrew Phillips - United States Naval Academy, Jean Blair - United States Military Academy,
Allen Parrish - The University of Alabama, Chris Inglis - United States Naval Academy,
Sue Fitzgerald - Metropolitan State University, Diana Burley - George Washington University,
David Gibson – United States Air Force Academy, Elizabeth Hawthorne - Union County College,
Scott Buck – Intel Corporation, Raymond Greenlaw - United States Naval Academy,
C. Steven Lingafelt - IEEE CEAA & IBM
This Session’s Goals

• **Goal 1**: socialize the current draft ABET Program Criteria for *Cybersecurity*

• **Goal 2**: solicit input for improving and refining the Draft Criteria

• Our focus will be on Program Criteria ONLY
  • Student Outcomes
  • Curriculum
  • Faculty

• The evolution of the draft will be described first
The Cyber Education Project (CEP)

• What were the goals of the CEP?
  • **Goal 1:** To develop curriculum guidelines for the “cyber sciences”
  • **Goal 2:** To develop ABET program criteria for one or more programs among those within the “cyber sciences”

• Who is CEP?
  • Academia, Industry, Government, Professional Societies
Professional Society Engagement

- ACM, IEEE-CS, and IEEE are **formally** engaged with CEP
  - ACM and IEEE-CS are co-sponsoring a delegation to produce a **curricular volume (similar to CS2013)**
    - Leaders are Diana Burley (GWU) and Matt Bishop (UC-Davis)
- ACM “official” representatives to CEP:
  - Sue Fitzgerald (Metro State), Beth Hawthorne (Union County)
- IEEE-CS “official” representatives to CEP:
  - Allen Parrish (Alabama), J. Ekstrom (BYU)
- IEEE “official” representative to CEP:
  - Steven Lingafelt (IBM)
- SIGSEC of AIS also is significantly involved although AIS has not formally “signed on”
  - David Biros (Oklahoma State), Yair Levy (Nova Southeastern U)
- CSAB “owns” Cybersecurity criteria development on behalf of ABET
Where Have We Been So Far?

- July 2014 – ABET Commission meeting, Arlington VA
- November 2014 – NICE/NSF CAE Meeting, Columbia MD
- March 2015 – SIGCSE, Kansas City MO
- June 2015 – 8th Annual Southeastern Cyber Security Summit, Huntsville AL
- June 2015 – 19th CISSE Colloquium, Las Vegas NV
- June 2015 – Community College Cyber Security Summit, Las Vegas NV
- July 2015 – ABET Commission meeting, Baltimore MD
- August 2015 – AMCIS, Puerto Rico
- August 2015 – Academy of Science and Engineering (ASE) International Conference on Cyber Security, Stanford University
- November 2015 – NICE, San Diego CA
- December 2015 – ICIS, Fort Worth TX
- March 2016 – SIGCSE, Memphis TN
Cy·ber Scien·ces (n.)
Defining the “Cyber Sciences”

The **Cyber Sciences** are computing-based disciplines involving technology, people, and processes aligned in a way to enable “assured operations” in the presence of risks and adversaries. They involve the creation, operation, analysis, and testing of secure computer systems (including network and communication systems) as well as the study of how to employ operations, reasonable risk taking, and risk mitigations. The Cyber Sciences are interdisciplinary courses of study, and include aspects of law, policy, human factors, ethics, risk management, and other topics directly related to the success of the activities and operations dependent on such systems, often in the context of an adversary.
CEP Learning Outcomes Goal #1

- **Goal**: Develop learning outcomes and curricular guidance which characterize the knowledge, skills, and abilities to be gained by students in undergraduate “cyber sciences” programs

  - Results of the work ...
    - Final report is available on the CEP website
    - There are MANY learning outcomes that define SEVERAL different kinds of programs that fall under “Cyber Sciences”
    - Hence ... the Cyber Sciences is/are a “Big Tent” consisting of a variety of related but different Cyber fields

- This work is the FOUNDATION for the draft criteria

Draft “Cyber Sciences” Knowledge Areas
Cyber Education Project
Learning Outcomes Committee
David Gibson and Beth Hawthorne, Co-chairs
October 2015
Bottom line ... Cyber Sciences ➔ Cybersecurity

• While the “Cyber Sciences” have curricular elements that extend outside of traditional computing disciplines, the “core” of Cybersecurity in particular (and of the Cyber Sciences more generally) remains computing

• Many computing-based programs exist today with names that would fit under this type of program criteria (e.g. information assurance, computer security, information security, cyber operations)
Cybersecurity ≠ Cyber Sciences

• CAC will accredit programs in Cybersecurity
  • These are computing based programs
  • CSAB is leading the development of the criteria

• Other Cyber Sciences disciplines (Cyber Engineering?) may be better associated with other commissions.
CEP & ABET Survey to Determine Degree of Interest in Obtaining ABET Accreditation for Programs in “Cyber Sciences.”

- Survey of 670 institutions’ ABET focal points – 1/25/16 to 2/29/16
- 98 responses with meaningful data (15%) – 91% from U.S.
- Full report at www.cybereducationproject.org/project-artifacts

<table>
<thead>
<tr>
<th>Program State</th>
<th>ABET Accredited</th>
<th>Count</th>
<th>Strong Pilot Interest</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Existing Program</strong> with interest in “Cyber Sciences” ABET accreditation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Existing Yes</td>
<td>Yes</td>
<td>20</td>
<td>12</td>
</tr>
<tr>
<td>Existing No</td>
<td>No</td>
<td>38</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>Sub Total:</td>
<td>58</td>
<td>31</td>
</tr>
<tr>
<td><strong>Contemplated Future Programs</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contemplated -na-</td>
<td>-na-</td>
<td>27</td>
<td>2</td>
</tr>
<tr>
<td>Likely to reassess interest in a “Cyber” program prior to the '19-20 academic year</td>
<td></td>
<td>28</td>
<td></td>
</tr>
<tr>
<td>Grand Total</td>
<td></td>
<td>113</td>
<td>33</td>
</tr>
</tbody>
</table>
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 must have course work or an 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
Some full-time faculty members, including those responsible for the cyber security curriculum development, must hold a terminal degree with a program of study in cyber security or a closely related field.
Our Approach for Today

• We will dissect and discuss this draft in three parts
  • Please provide your thoughts on EACH as we work thru them

• The order ...
  • Header material
  • Faculty
  • Student Outcomes
  • Curriculum (the largest / hardest part)
Scope:
These program criteria apply to computing programs using cybersecurity, computer security, cyber operations, information assurance, information security, or similar terms in their titles.

6. Faculty
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.
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 must have course work or an 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.
Conclusion

• Thanks for participating!

• Please stay involved!