ABET CYBERSECURITY ACCREDITATION

Two Distinct Efforts

CAC

Cybersecurity

EAC

Cybersecurity Engineering

Undergraduate, B.S. programs

General Versus Program Criteria

- CAC and EAC have “General Criteria” that apply to all programs:
  - CAC – In computing
  - EAC – In engineering
- Cybersecurity and Cybersecurity Engineering criteria are considered to be “Program Criteria”
  - Cybersecurity – Proposed as one option under CAC
  - Cybersecurity Engineering – Proposed as one option under EAC

Cybersecurity Criteria

- Assumes new changes to the ABET General Computing Criteria:
  - Criterion 3 (Student Outcomes)
  - Criterion 5 (Curriculum)
  - Both are currently under review
- Cybersecurity Program Criteria:
  - Inserts additional required Student Outcomes for Cybersecurity (extends Criterion 3)
  - Inserts additional Curriculum requirements for Cybersecurity (extends Criterion 5)

DRAFT Criterion 3 General Student Outcomes

The program must have documented and publicly stated student outcomes that include (1) through (5) below and any additional outcomes required by applicable Program Criteria. The program may define additional student outcomes at its discretion.

1. An ability to analyze a problem, and to identify and define the computing requirements appropriate to its solution.
2. An ability to design, implement, and evaluate a computer-based solution to meet a given set of computing requirements in the context of the discipline.
3. An ability to communicate effectively with a range of audiences about technical information.
4. An ability to make informed judgments in computing practice based on legal and ethical principles.
5. An ability to function effectively on teams to establish goals, plan tasks, meet deadlines, manage risk, and produce deliverables.

DRAFT Criterion 5 General 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 requirements specify subject areas, but do not prescribe specific courses. The program must include each of the following in a manner appropriate to its discipline:

1. At least **one academic year of up-to-date coverage of fundamental and advanced computing topics** that provides both breadth and depth.
2. College-level mathematics.
3. Current techniques, skills, and tools necessary for computing practice.
4. **Information assurance and security principles and practices.**
5. Concepts involving the local and global impact of computing solutions on individuals, organizations, and society.

DRAFT Cybersecurity Student Outcomes

3. Student Outcomes

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

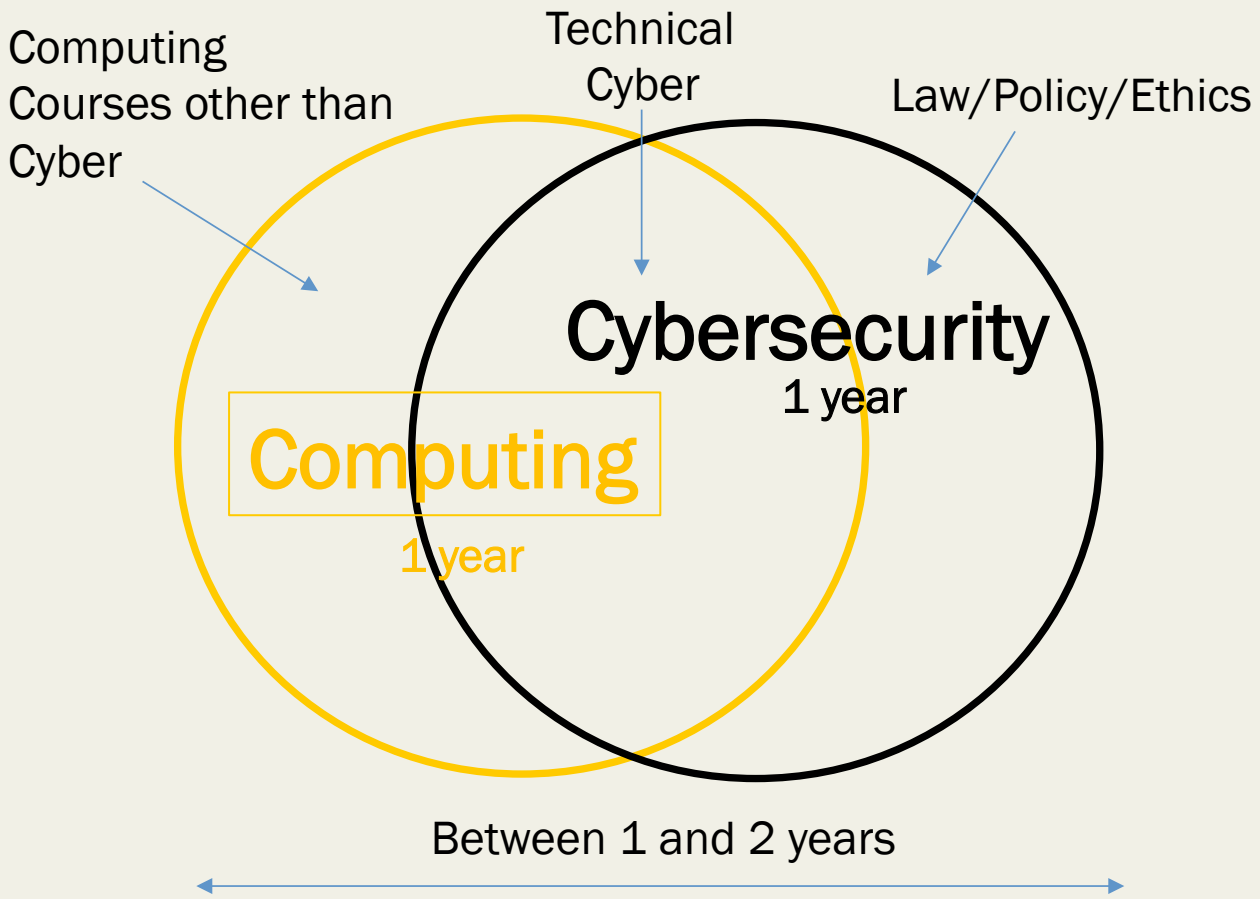
6) An ability to apply security principles and practices to the environmental, hardware, software, and human components of a system.
7) An ability to analyze and evaluate systems with respect to maintaining operations in the presence of risks and threats.

DRAFT Cybersecurity Curriculum

5. Curriculum. Students have at least one year of course work or equivalent educational experiences in cybersecurity that *must* cover fundamental and advanced topics from the following:

1. **Information Security** topics such as information confidentiality, data integrity, availability, cryptography, and cryptanalysis.
2. **Software Security** topics such as secure software development, software reverse engineering, and/or malware analysis.
3. **System Security** topics such as availability, authentication, access controls, secure systems design, computer network defense, computer network attack/penetration testing, reverse engineering (hardware), cyber physical systems, digital forensics, and supply chain management.
4. **Usable Security** topics such as identity management, social engineering, social networks, and human-computer interaction.
5. **Organizational Security** topics such as risk management, incident response, mission assurance, disaster recovery, business continuity, security evaluations/compliance, organizational behavior, intelligence, and economics.
6. **Societal Security** topics such as cybercrime, cyber law, ethics, policy, privacy, intellectual property, professional responsibility, and global societal impacts.

Computing - Cybersecurity



Cybersecurity Engineering Program Criteria

IEEE PROGRAM CRITERIA FOR SECURITY, CYBERSECURITY, INFORMATION ASSURANCE AND SIMILARLY NAMED ENGINEERING PROGRAMS
DRAFT, NOT FOR USE OR DISTRIBUTION, NOT APPROVED BY EAC
Lead Society: Institute of Electrical and Electronics Engineers
Cooperating Society CSAB

These program criteria apply to engineering programs that include "security", "cybersecurity", "information assurance" or similar modifiers in their titles.

1. Curriculum
The structure of the curriculum must provide both breadth and depth across the range of engineering topics implied by the title of the program.

The curriculum must
- Include probability, statistics, and cryptographic topics including applications appropriate to the program.
- Include discrete math and specialized math appropriate to the program, such as, abstract algebra, information theory, number theory, complexity theory, finite fields.
- Include engineering topics necessary to analyze and design complex devices, software, and systems containing hardware, software and human components.
- Provide both breadth and depth across the range of engineering and computer science topics necessary for the:
  1) application of security principles and practices to the design, implementation, and operations of the physical, software, and human components of the system as appropriate to the program
  2) application of protective technologies and forensic techniques
  3) analyzing and evaluation of components and systems with respect to security and to maintaining operations in the presence of risks and threats
  4) consideration of legal, regulatory, privacy, ethics, and human behavior topics as appropriate to the program

2. Faculty
The program must demonstrate that faculty members teaching core engineering topics understand engineering problem solving methods and engineering practice with specific relevance to security.

black is text drawn from existing IEEE criteria, blue text is addition

Next Steps

- Approval of first draft criteria (by Fall 2017)
- Some possible pilot visits in Fall 2017
- Final approval of criteria in Fall 2018
- Visits in Fall 2019?
- Need volunteers to help us pilot and refine the criteria

TOWARD CURRICULAR GUIDELINES IN CYBERSECURITY: AN UPDATE FROM THE ACM JOINT TASK FORCE ON CYBERSECURITY EDUCATION

NICE

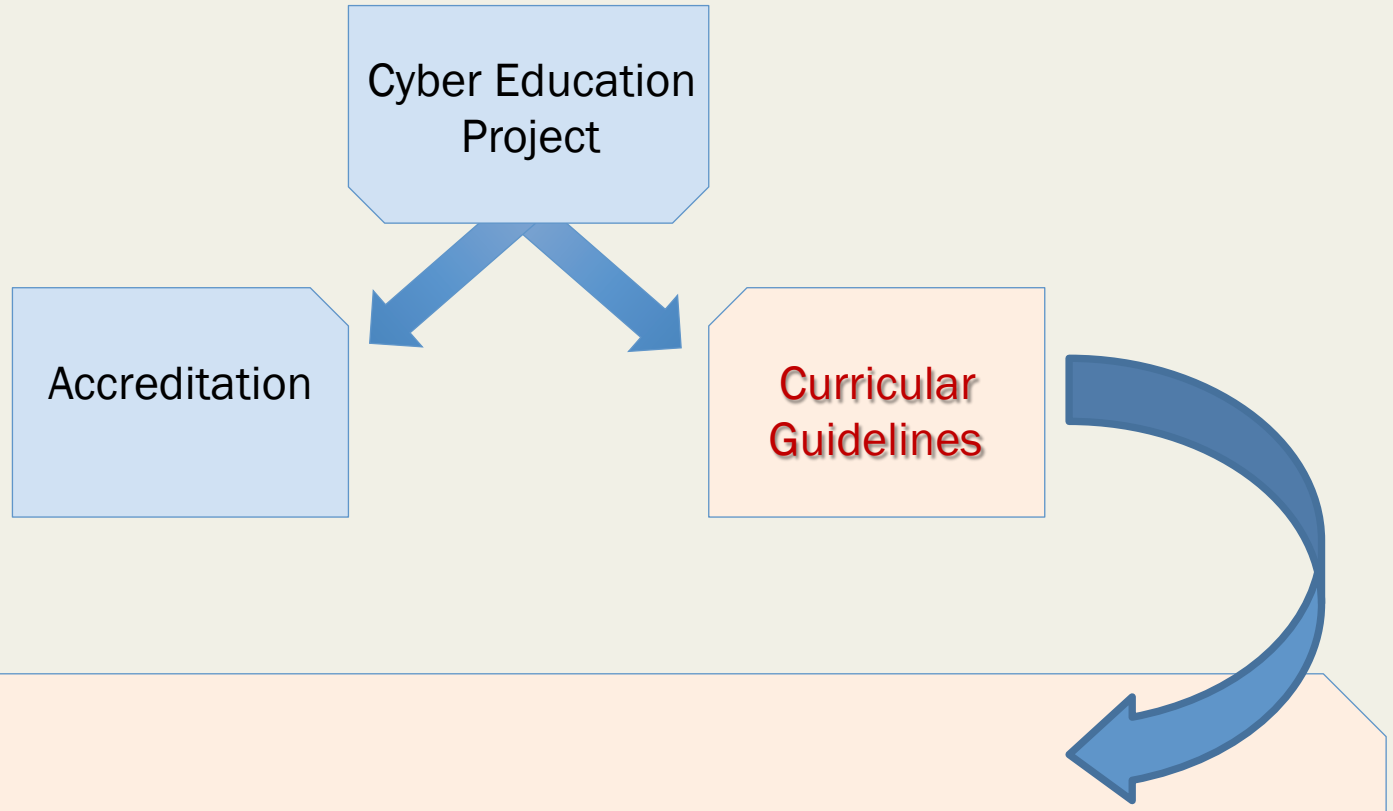
Kansas City, MO

November 2, 2016

csec2017.org

ACM JTF Origin & Purpose

Origin:



Purpose:

To develop comprehensive undergraduate curricular guidance in cybersecurity education that will support future program development and associated educational efforts.

Milestones

Date	Milestone
September 2015	JTF formally launched
October 2015	Delegations from all collaborators seated

Collaborators

- ✓ Association for Computing Machinery (ACM)
- ✓ IEEE Computer Society (IEEE CS)
- ✓ Association for Information Systems Special Interest Group on Security (AIS SIGSEC)
- ✓ International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8)
- ✓ Cyber Education Project (CEP)

JTF Delegates

- Co-chairs

  Diana Burley, George Washington University (ACM/CEP)

  Matt Bishop, University of California, Davis (ACM/IFIP)

- Members

  Scott Buck, Intel Corporation (ACM/CEP)

  J. Ekstrom, Brigham Young University (IEEE CS/CEP)

  Lynn Futcher, Nelson Mandela Metropolitan University (ACM/IFIP)

  David Gibson, US Air Force Academy (ACM/CEP)

  Elizabeth Hawthorne, Union County College (ACM/CEP)

  Siddharth Kaza, Towson University (ACM)

  Yair Levy, Nova Southeastern University (AIS SIGSEC)

  Herb Mattord, Kennesaw State University (AIS SIGSEC)

  Allen Parrish, U.S. Naval Academy (IEEE CS/CEP)

Milestones

Date	Milestone
December 2015	JTF develops working definition of cybersecurity to guide and bound curricular development efforts

…**Cybersecurity** is defined as a "computing-based discipline involving technology, people, information, and processes to enable assured operations. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management in the context of adversaries."

Community Engagement

Upcoming Meetings

- CYBERSEC: European Cybersecurity Forum - September 26-27, 2016, Krakow, Poland
- Cyber Maryland Conference - October 20-21, 2016, Baltimore, MD
- CyCon US: International Conference on Cyber Conflict - October 21-23, 2016, Washington, DC
- National Initiative for Cybersecurity Education (NICE) Conference - November 1-2, 2016, Kansas City, MO
- 3rd Annual Journal of Law and Cyber Warfare - November 3, 2016, New York, NY

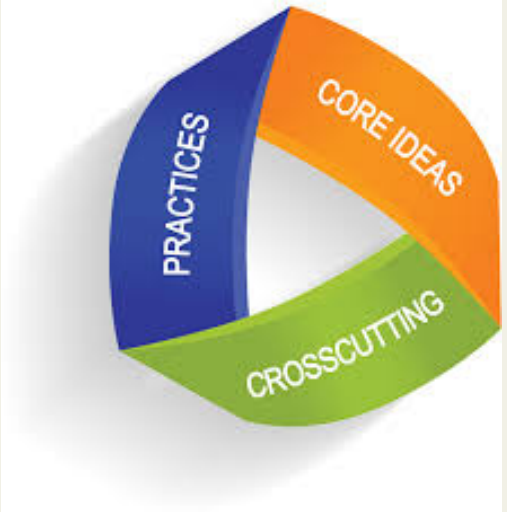
Previous Meetings

- Community College Cyber Summit (3CS) - July 22-24, 2016, Pittsburgh, PA
- Americas Conference on Information Systems (AMCIS) - August 11-14, 2016, San Diego, CA
- National Cyber Summit - June 8-9, 2016, Huntsville, AL
- Colloquium for Information Systems Security Education - June 13-15, 2016, Philadelphia, PA
- International Security Education Workshop - June 13-15, 2016, Philadelphia, PA *(co-located with CISSE)*
- Women in Cybersecurity (WiCyS) - March 31 - April 2, 2016, Dallas, TX
- ACM SIGCSE - March 2-5, 2016, Memphis, TN
- Cyber Education Project Industry Advisory Board - February 26, 2016, Webinar
- National Science Foundation Cyber Corps PI Meeting - January 14, 2016, Arlington, VA
- NICE Interagency Coordinating Council - January 14, 2016, Arlington, VA
- Pre-ICIS Workshop on Security & Privacy (WISP) - December 13, 2015, Ft. Worth, TX

JTF Curricular Thought Model v1

- Modification of U.S. National Research Council, Next Generation Science Standards (nextgenscience.org)

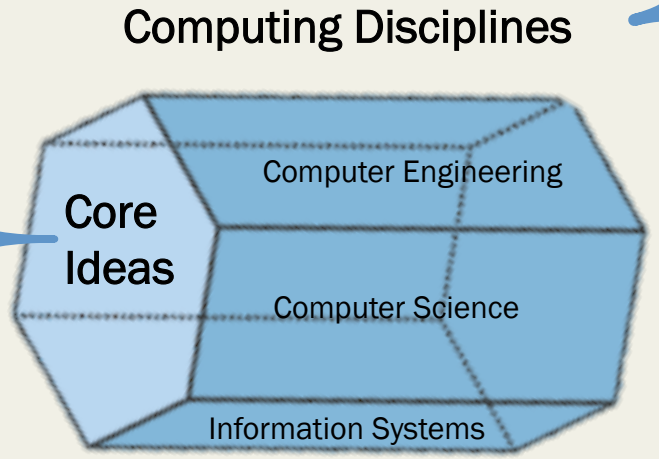
- **Core Ideas** = Knowledge Areas/Domains
- **Cross-cutting Concepts**
  - Adversarial Thinking
  - Risk
  - Confidentiality
  - Integrity
  - Availability
  - Access control
- **Practices** = Cybersecurity Knowledge + Skills connected with Focus Areas



Cyber Curricular Thought Model v2 (based on survey)

Computer Engineering
Computer Science
Information Systems
Information Technology
Software Engineering
Mixed Disciplinary Majors
(xx Informatics or Computational xx)

Information Security
Software Security
System Security
Usable Security
Organizational Security
Societal Security



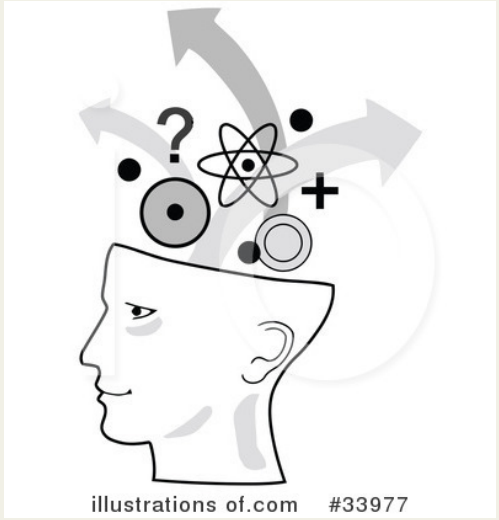
Cross Cutting Concepts

Confidentiality Integrity Adversarial Thinking

Risk Management Availability *Access Control*

8 DRAFT Core Ideas

- Information Security
- Software Security
- System Security
- Usable Security
- Organizational Security
- Societal Security



DRAFT Core Ideas Breakout (4 of 6)

- Information Security
  - confidentiality
  - data integrity
  - availability
  - cryptography
- Software Security
  - secure software engineering
  - software reverse engineering
  - malware analysis
- Usable Security
  - identity management
  - social engineering
  - social networks
  - human-computer interaction
- System Security
  - availability
  - authentication
  - access controls
  - secure systems design
  - computer network defense and computer network attack/ penetration testing
  - hardware reverse engineering
  - cyber physical systems
  - digital forensics
  - supply chain management

DRAFT Core Ideas Breakout (2 of 6)

- Organizational Security
  - risk management
  - mission assurance
  - disaster recovery
  - business continuity
  - security evaluations/compliance
  - organizational behavior
  - intelligence
  - economics
- Societal Security
  - cybercrime
  - Cyber law
  - ethics
  - policy
  - privacy
  - intellectual property
  - professional responsibility
  - global societal impacts

2016 ISEW ~ 75 Participants

Sponsors: Intel, NSF,
I3P

International Panel Discussion

Small Group Breakout Sessions

International Efforts

- **Survey sent internationally**
  - Received jumpstart from IT2017 survey
  - Michel Kabay, Prof. Information Assurance, Norwich University
    - taught internationally in UK, Germany, Japan, China, and Canada

- **Global Advisory Board (GAB)**
- Co-Chaired by **Lynn Futcher**, South Africa, Chair IFIP WG 11.8
  Jill Slay, Australia, Director, Australian Centre for Cyber Security
  - International representatives from academia and government
    - Indonesia, Malaysia, Japan, Asian Pacific CERT, and Singapore
  - Dr. Steven Wong, Singapore Institute of Technology
    - Developed the first and only cybersecurity degree program in Singapore
    - President of Singapore Association of Information Security Professional (AISP)

International Efforts

- Diana Burley spoke in Singapore at the U.S.-Singapore *TCTP*
  Cybersecurity Workshop for government officials from the Association of South East Asian Nations (ASEAN)
- U.S. State Department & Singapore Cyber Security Agency
- **ASEAN countries**: Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, and Vietnam. **Other countries**: Japan, Australia, and Papua New Guinea.

International Efforts

- Diana Burley invited to give “Future Stream” keynote at the **European Cybersecurity Forum** in Krakow, Poland this September

DIANA L. BURLEY

Co-chair, Association for Computing Machinery Joint Task Force on Cybersecurity Education - USA

- JTF co-chairs invited by the Cyberspace Administration of China to give keynote at **1st China Cybersecurity Summit** during talent cultivation workshop. Also this September; scheduling conflict.

Industry Advisory Board

- Started with CEP in Q1 2015 and continues with JTF
- Lead by Scott Buck of Intel Corp.
- ~15 Companies from high tech, aerial space, automotive, communication, utilities, …
- Resource for the reviewing and commenting in the creation of Learning Outcomes (LO) cybersecurity curriculum
  - Categorize the topic areas as of low, medium, or high importance for personnel in cyber related positions
- Provide guidance in job titles and descriptions relating to cybersecurity, and provide insight of industry specific to cybersecurity related skills most important to industry

Next Steps Toward Curricular Guidance

- Industry Advisory and Global Advisory Boards
- International Survey, Closed mid October – Processing Results
- Community Engagement: U.S. and Abroad
- NICE conference, Nov 1-2, 2016, Kansas City, MO
- *ACM Inroads* EduBits column, Dec. 2016 edition
- **Initial Public Draft (v.1)** for Review and Comment, Dec. 2016
- SIGCSE Special Session, March 8-11, 2017, Seattle, WA
- IFIP WISE conference, WG 11.8 workshop, May 29-31, 2017, Rome, Italy
- **Final Public Draft (v.2)** for Review and Comment, June 2017
- **Endorsed Curricular Guidelines in Cybersecurity (CSEC),** Dec. 2017
  - "Living document" – Wiki? XML?

Questions/Comments