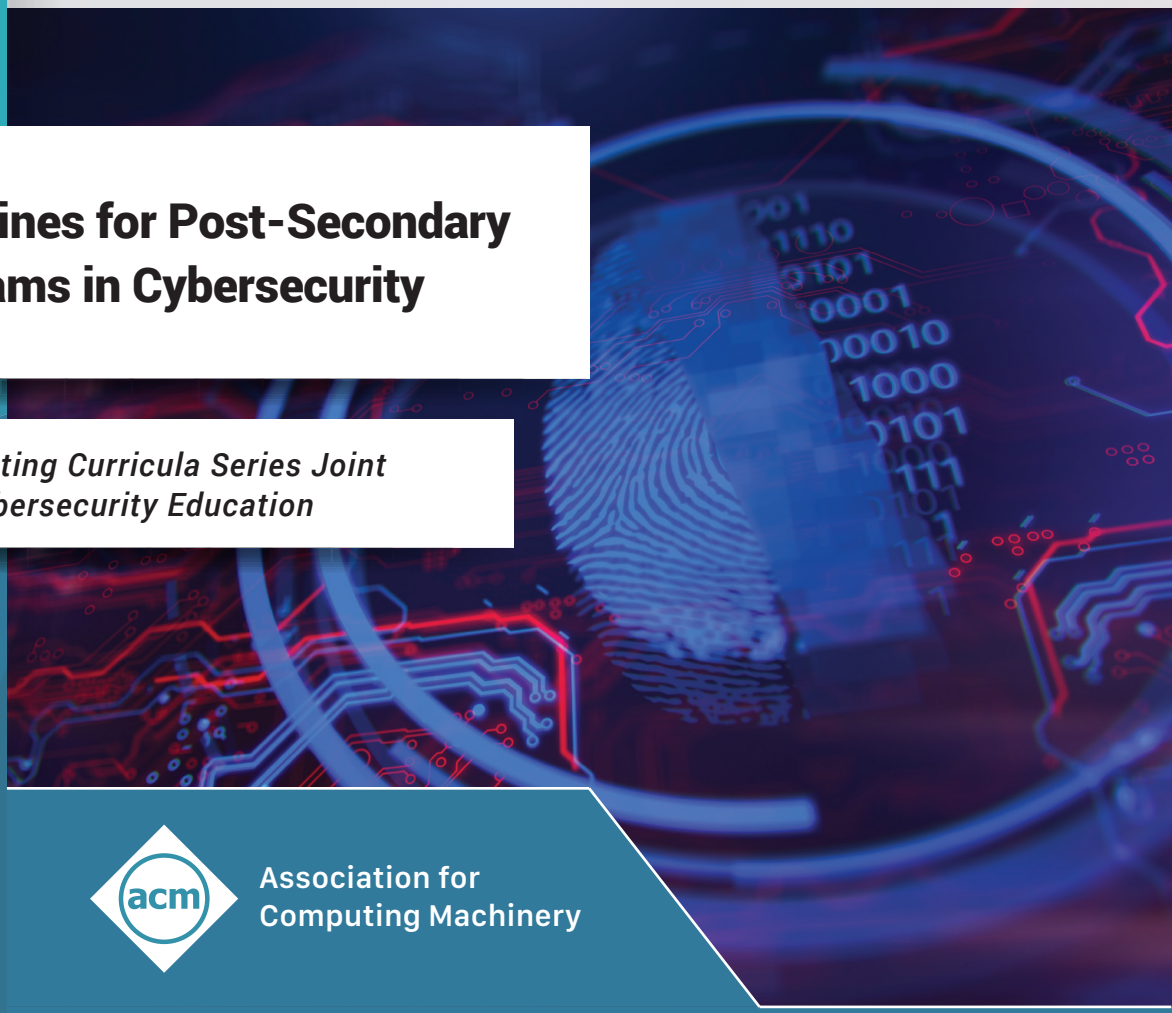
CYBERSECURITY CURRICULA 2017

Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity

A Report in the Computing Curricula Series Joint Task Force on Cybersecurity Education



Association for Computing Machinery

IEEE computer society

ASSOCIATION FOR INFORMATION SYSTEMS

ifip

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

Version 1.0 Report
31 December 2017

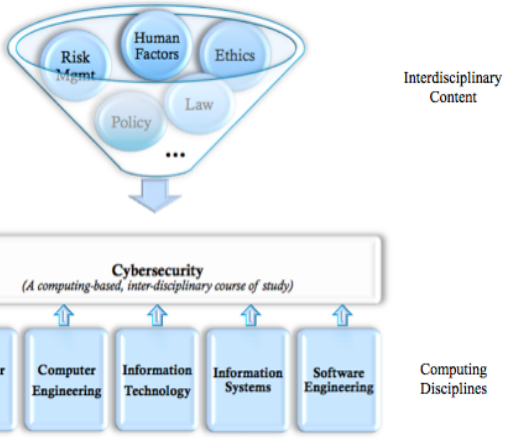
With an estimated shortfall of 3.5 million workers by the year 2021, global cybersecurity workforce needs are acute, broad and growing. To close the increasingly significant gap between supply and demand, cybersecurity workforce stakeholders must leverage scalable initiatives that can accelerate workforce development by: (1) implementing comprehensive curricular guidance and (2) linking academic programs to professional practice. **Cybersecurity Curricula 2017 (CSEC2017)**[1], the first set of global cybersecurity curricular guidelines, is one such initiative.

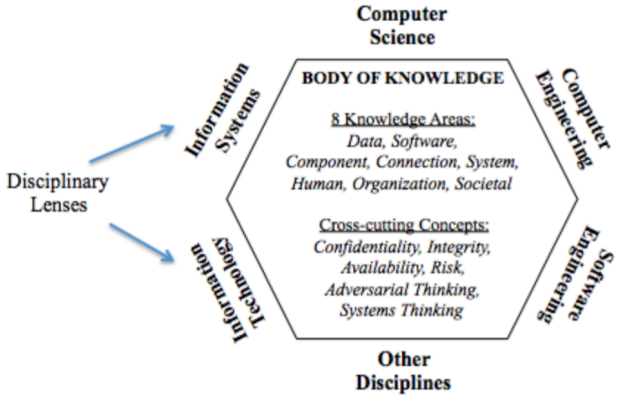
Released in February 2018 after a nearly three-year process; Advised by more than 325 subject matter experts from 35 countries; and Endorsed by the four leading global computing societies –

CSEC2017 will be the leading resource for comprehensive cybersecurity curricular content at the post-secondary level.

CSEC2017 highlights include:

- Structures the cybersecurity discipline as a computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management;
- Offers flexible guidance based on a comprehensive view of the cybersecurity field and specific disciplinary demands;





- Supports the alignment of educational offerings (formal and informal) along the full K-12 - professional development continuum;
- Serves as the foundation for emerging cybersecurity accreditation efforts; and
- Provides a structure for linking cybersecurity curricula to workforce frameworks.

Implementing these curricular guidelines will strengthen the talent pipeline and enable the acceleration of cybersecurity workforce development efforts. In the implementation phase, project leaders will assist with the alignment of the curricular guidelines to (1) academic cybersecurity offerings (both existing and new); and (2) government and industry employment needs. To aid implementation of the guidelines across a variety of academic programs, the CSEC2017 team will assist institutions develop course and curricular exemplars. The exemplars, which will be shared through the community engagement website, illustrate how to align curricular offerings with the CSEC2017 guidelines. To aid government and industry, the project team will assist with the development of workforce exemplars and roadmaps that link specific work role requirements to the guidelines. Exemplar and roadmap development will be ongoing as more institutions seek to align their programs to the recommendations.

To learn more, visit http://cybered.acm.org or contact CSEC Co-chairs:

- Dr. Diana Burley, George Washington University (dburley@gwu.edu)
- Dr. Matt Bishop, University of California at Davis (mabishop@ucdavis.edu)

[1] See http://cybered.acm.org for additional information. The US National Science Foundation and the US National Security Agency provided additional project sponsorship.