2027 ASEE Annual Conference & Exposition

Cybersecurity and Cybersecurity Engineering Constituent Committee (CYBCC)

Call for Papers

Toronto, Ontario, Canada, June 20–23, 2027

The Cybersecurity and Cybersecurity Engineering Constituent Committee (CYBCC), ASEE's newest home for educators, researchers, practitioners, and students in cybersecurity education, invites the submission of abstracts and subsequent full papers, Work-in-Progress (WIP) papers, workshop proposals, and special sessions for presentation at the 2027 ASEE Annual Conference & Exposition in Toronto, Ontario, Canada.

The committee's scope spans the full breadth of cybersecurity education—technical practice, governance and management, policy, human factors, and workforce development—with particular attention to cybersecurity engineering: the rigorous application of engineering design principles (including probability, statistics, cryptography, and discrete mathematics) to specify, analyze, design, test, and protect complex systems that integrate hardware, software, and human components. CYBCC is intended to complement, not duplicate, ASEE's existing computing-oriented divisions by centering the security of engineered systems and the preparation of the cybersecurity workforce.

With most modern systems incorporating complex and networked hardware and software components supporting critical functions and critical infrastructure, security can no longer be treated as an elective concern bolted on after a system is built. The CYBCC provides a forum for advancing secure-by-design thinking across *all* engineering disciplines, not just computing, and for preparing a workforce equipped to meet a persistent and well-documented shortage of qualified cybersecurity professionals.

We welcome submissions equally from cybersecurity educators and professionals and from authors whose primary affiliation lies outside cybersecurity and computing. Papers describing how security is taught, integrated, or applied within other engineering disciplines, including but not limited to mechanical, electrical, biomedical, civil, chemical, industrial, and aerospace engineering—are highly valued and central to the committee's interdisciplinary mission.

Suggested Topic Areas

We welcome work on cybersecurity educational research, classroom practice, curriculum design, laboratory development, workforce development, and any other appropriate cybersecurity related engineering education topic, including but not limited to:

Cybersecurity Education, Curriculum, and Accreditation

- Development, evaluation, and accreditation of cybersecurity and cybersecurity engineering programs: ABET CAC and EAC criteria, NSA National Centers of Academic Excellence in Cybersecurity (NCAE-C) designations, and alignment with the NICE Workforce Framework.
- Distinguishing security awareness from security engineering in curriculum design: pitching security content at the right level for each discipline and degree.
- Secure-by-design thinking integrated across the engineering curriculum rather than isolated in a single course.
- Curriculum modernization informed by industry frameworks, threat intelligence, workforce demand data, and industry-recognized certifications.
- Cybersecurity management, governance, and policy education, including manageability, sustainability, and operation under compliance requirements.
- Pathways into the field: K–12 outreach, community college articulation, associate through doctoral degree programs, and professional reskilling.

Teaching, Learning, and Assessment

- Design and delivery of security laboratories, including virtualized, cloud-based, and remote-access lab infrastructure.
- Capstone design, undergraduate research, competitions, and other experiential learning in cybersecurity and cybersecurity engineering.
- Competency-based education: assessment of student learning, skills validation, and mapping learning outcomes to workforce roles.
- Evidence-based instructional practices and rigorous evaluation of educational interventions: what works, what doesn't, and how we know.
- Faculty development, including preparing new faculty and supporting existing faculty in modernizing security courses and hands-on laboratories.

Traditional and Emerging Technical Topics in Security Education

- Network security, secure system design, and security architecture; hardware, embedded, and firmware security.
- Cryptography and cryptographic systems education, including quantum-safe cryptography and security in a quantum-capable cyberinfrastructure.
- Software security: secure software architecture, secure coding, application security, and secure software supply chain.
- Digital forensics education, forensic engineering education, and incident response.
- Threat detection, threat hunting, penetration testing, and intrusion detection and prevention (IDS/IPS).
- Governance, Risk, and Compliance (GRC) and Security Operations Center (SOC) education.
- Cloud, big data, and enterprise security; privacy, data protection, and local and global privacy standards.

Interdisciplinary and Application-Domain Security

- Cybersecurity needs of biomedical and medical devices, healthcare systems, and health data.
- Security of critical infrastructure: power grids, water systems, transportation, smart cities, and industrial control/SCADA systems.
- Security of the Internet of Things (IoT), wireless sensor networks, and cyber-physical systems.
- Automotive, aerospace, maritime, and autonomous-system security; robotics, manufacturing, and operational technology (OT).
- Teaching security concepts within non-computing engineering disciplines, and collaborations between security programs and other departments.

Artificial Intelligence and Security

- AI- and machine-learning-based threat detection and defense and teaching these methods.
- Security, robustness, and adversarial vulnerabilities of AI/ML systems themselves.
- Generative AI in the security classroom: opportunities, academic integrity, and responsible use.

Workforce Development, Human Factors, and Global Perspectives

- Industry–academia integration: co-designed curricula, industry-sponsored labs, apprenticeships, internships, work-based learning, and advisory board engagement.
- Preparing graduates for cybersecurity related roles: certifications, competencies, and career pathways.
- Human factors, usable security, social engineering, and security awareness training.

- Ethics, law, and policy in cybersecurity education; broadening participation and expanding access to cybersecurity and cybersecurity engineering education.
- Global and international perspectives: international cybersecurity education models, cross-border partnerships, and global workforce development.

Submission Categories

The CYBCC welcomes submissions in the following categories:

1. **Full Papers**: complete research or evidence-based practice papers.
2. **Work-in-Progress (WIP) Papers**: reports on ongoing efforts; titles must begin with "Work in Progress:".
3. **Special Sessions and Panels**: non-traditional format sessions, including panel discussions and thematic paper groupings on topics of high relevance.
4. **Tutorial Workshops**: instructional sessions on topics of value to the cybersecurity education community, such as curriculum development or laboratory design.

Submission Guidelines

- **Abstract Deadline:** October 2026 (see the ASEE conference website for the exact date).
- Abstracts should be approximately 500 words and must be submitted through ASEE's online submission system (NEMO).
- Authors should consult the Author's Kit on the ASEE conference website for complete formatting and submission requirements.
- Authors of accepted abstracts will be invited to submit full papers for peer review and potential inclusion in the conference proceedings.
- The CYBCC follows ASEE's **Publish-to-Present** policy: to be presented at the conference, a paper must be both submitted and accepted for publication.

Workshop and Special Session Proposals

Proposals for tutorial workshops and special sessions should be e-mailed directly to the CYBCC Program Chair beginning October 1, 2026, and should include:

- Presenter information: full name, e-mail address, and institutional affiliation for each presenter.
- The objective of the workshop or session, and its primary and secondary topic areas.
- Whether the event will be ticketed and, if so, the proposed ticket price.
- A billing address for any expenses that may be incurred (food, services, room technology, etc.).

Workshop presenters are encouraged to supplement workshop fees with grants and subsidies. The Program Chair reserves the right to cancel any accepted workshop that is likely to incur a financial loss.

Workshop and special session proposal deadline: December 15, 2026.

Author Deadlines

All dates below are tentative and will be confirmed on the ASEE conference website.

- Abstracts: October 2026
- Draft Papers: January 2027
- Revised Papers: February 2027
- Author Registration: April 2027

- Final Papers: April/May 2027

Questions and Contacts

CYBCC Chair
Walter Schilling, Ph.D.
Professor and Program Director, Cybersecurity Systems
Diercks School of Advanced Computing
Milwaukee School of Engineering
Email: schilling@msoe.edu

CYBCC Program Chair
Doug Jacobson, Ph.D.
Professor and Director: ISU Center for Cybersecurity Innovation and Outreach
Sunil & Sujata Gaitonde Professorship in Cybersecurity
Iowa State University
Email: dougj@iastate.edu

We look forward to your submissions and to building a vibrant, interdisciplinary community around cybersecurity and cybersecurity engineering education.