WORCESTER POLYTECHNIC INSTITUTE

National Cybersecurity Teaching Academy (NCTA) at WPI

Funded by the National Centers of Academic Excellence in Cybersecurity program, WPI is one of the national NCTA sites to train high school teachers and grant them 18-credit-hour graduate-level certificates in teaching cybersecurity. **Credits from this certificate can be applied to an MS in Integrated STEM from WPI**. Scholarship available. Please apply ASAP!

Highlights of NCTA at WPI:

- Format: Virtual (lectures and labs all online)
- Target Participants: nation-wide high school teachers interested in teaching security
- Time: Summer 2025, Summer 2026 and Summer 2027
- Contact: Drs. Jun Dai (jdai@wpi.edu) and Xiaoyan Sun (xsun7@wpi.edu)
- Support: scholarship to fully cover tuition
- Accomplishment: an 18-credit-hour graduate-level certificate to teach cybersecurity.
- Program Site: wpi.edu/+NCTA
- Application Link: www.surveymonkey.com/r/2025_ncta_scholarship_application
- Application Deadline: Jan 15, 2025

Course Structure of NCTA at WPI

- CS 591 Fundamentals in Cyber Security for Teachers
  This course covers network and computer security, addressing intrusion methods, privilege escalation, and defense strategies. Topics encompass networking, OS fundamentals, vulnerabilities, cyber defenses, and security administration.

- CS 592 Introduction to Digital Forensics for Teachers
  This course explores digital forensics, including forensic lab environment, data acquisition, electronic discovery, legal aspects, technical methodologies in Linux, Mac, and Windows forensics, data hiding and steganography, network, and mobile forensics.

- CS 593 Cyber Security Teaching Methods
  This course covers cybersecurity guidelines (e.g., HSCCG, CSEC, CAE Knowledge Units, NCWF) and effective teaching methods, including cultural relevance, knowledge scaffolding, differentiation, assessment, and instructional technologies (e.g., CTFs, competitions).

- CS 594 Advanced Digital Forensics and Incident Response for Teachers
  This course covers computer forensics fundamentals and focuses on providing practical hands-on experiences. Students learn to use practical digital forensic tools for evidence data acquisition and analysis, data recovery, file system analysis, file carving, data hiding, and network forensics.

- CS 571 Case Studies in Computer Security
  This course examines security challenges and failures holistically, taking into account technical concerns, human behavior, and business decisions. Using case studies, students will explore the interplay among these dimensions in creating secure computing systems and infrastructure.

- CS 587 Cyber Security Capstone Experience
  The capstone project has students apply security concepts to real-world problems. Students will propose a project idea in cybersecurity in writing with concrete milestones, receive feedback, and pursue the proposal objectives.