NEW JERSEY CENTER
FOR TEACHING & LEARNING

Progressive Science Initiative® (PSI®)
CSCI6353: Learning and Teaching AP Cybersecurity

Primary Student Contact:	Maria Surace	maria@njctl.org
Faculty Team:	Dr. Bob Goodman	bob@njctl.org
	Maria Surace	maria@njctl.org
	Katy Goodman	katy@njctl.org

Course Credit: 3.0 NJCTL credits

Dates & Times:
This is a 3-credit, self-paced course, covering 6 modules of content. The exact number of hours that you can expect to spend on each module will vary based upon the module coursework, as well as your study style and preferences. You should plan to spend approximately 15 hours per credit working online, and up to 30 hours per credit working offline.

Graduate Student Handbook: www.njctl.org/graduate-handbook/

COURSE DESCRIPTION:
This teacher training course is designed to prepare educators to effectively teach AP Cybersecurity by building both cybersecurity content knowledge and instructional expertise. Participants will explore core topics such as threats, vulnerabilities, risk management, device security, application security, data protection, cryptography, and secure system design while examining strategies for making complex technical concepts accessible to students. Through scenario-based learning, instructional planning, formative assessment design, and analysis of student misconceptions, educators will develop practical approaches for engaging learners and promoting cybersecurity problem-solving skills. The course emphasizes real-world applications, AP-aligned instructional practices, and effective assessment techniques to support student success in AP Cybersecurity. Upon completion, participants will be equipped with the knowledge, resources, and confidence needed to implement a rigorous and engaging AP Cybersecurity program.

Note: This course is not a CollegeBoard sponsored workshop. CollegeBoard does offer AP Summer Institutes and 1-Day workshops.

STUDENT LEARNING OUTCOMES:
Upon completion of the course, the student will be able to:

1. Demonstrate proficiency in core cybersecurity concepts and practices, including threats, vulnerabilities, risk management, device security, application security, data protection, access controls, cryptography, and cybersecurity investigations, as outlined in the module learning outcomes.
2. Integrate PSI instructional materials (including presentations, labs, activities, scenario analyses, formative assessments, and review resources) to support student learning and deliver effective AP Cybersecurity instruction.
3. Create a student-centered learning environment through the use of formative assessment questions, analysis of student responses, and facilitation of collaborative discussions that promote critical thinking, problem-solving, and deeper understanding of cybersecurity concepts.
4. Implement instructional strategies that support mastery learning, including multiple opportunities for practice, feedback, reassessment, and application of cybersecurity knowledge and skills consistent with PSI pedagogy.
5. Design and implement AP-aligned learning experiences that incorporate cybersecurity scenarios, literacy and communication skills, differentiation strategies, and authentic problem-solving opportunities to support success for diverse learners.

TEXTS, READINGS, INSTRUCTIONAL RESOURCES:
Required Texts:

- PSI AP Cybersecurity uses a free digital textbook accessible at: https://njctl.org/materials/courses/ap-cybersecurity/
- Participants will download SMART Notebook presentations, homework files, labs, and teacher resources from the PSI AP Cybersecurity

COURSE REQUIREMENTS:
In order to receive a Passing grade, the participant must complete the following course requirements:

1. Activities: A variety of learning activities are incorporated throughout the course to promote participant engagement and understanding of both cybersecurity concepts and effective instructional practices. These activities include:
   - Engaging with module lessons that model PSI instructional strategies, including minimized direct instruction, frequent formative assessment, and student-centered learning.
   - Completion of formative assessment questions aligned to module learning objectives, including analysis of correct and incorrect responses to strengthen content knowledge and instructional decision-making.
   - Participation in discussion boards that provide opportunities to collaborate with peers and course instructors regarding cybersecurity content, instructional strategies, student misconceptions, and implementation of AP Cybersecurity curriculum materials.
   - Analysis of cybersecurity scenarios, investigations, artifacts, and case studies that mirror authentic cybersecurity challenges and support classroom application.
2. Short Answer Assignments: Each module requires one (1) original short-answer response to a given prompt. These assignments are designed to encourage participants to reflect on instructional

practices, analyze student learning challenges, evaluate teaching strategies, and connect module content to classroom implementation. Responses should demonstrate thoughtful consideration of both cybersecurity concepts and effective pedagogy.

3. Mastery Exercises: For each module, mastery exercises assess participant understanding of cybersecurity content and instructional practices. These assessments consist primarily of multiple-choice questions aligned to module objectives. Participants may retake mastery exercises, with questions drawn from a larger question bank to provide varied opportunities for demonstrating mastery.
4. Scenario-Based Investigations and Applied Activities: Throughout the course, participants engage in cybersecurity investigations, scenario analyses, artifact interpretation, and problem-solving activities that model the types of experiences students will encounter in AP Cybersecurity courses. These activities are designed to deepen content knowledge while demonstrating effective instructional approaches for teaching cybersecurity concepts.
5. Module Exams: One module exam is completed at the conclusion of each module. These assessments include multiple-choice, short-answer, artifact analysis, and free-response questions aligned to module standards, objectives, and AP Cybersecurity expectations. Exams provide participants with opportunities to demonstrate both content mastery and analytical reasoning skills.
6. Final Reflection Assignment: At the conclusion of the course, participants complete a reflective assignment examining their growth as cybersecurity educators. The reflection requires participants to analyze instructional strategies, student learning considerations, course experiences, and future implementation plans while making meaningful connections between cybersecurity content and classroom practice.
7. Final Exam: At the end of the course, participants complete a comprehensive final exam consisting of multiple-choice, short-answer, artifact analysis, and free-response questions. The assessment measures understanding of cybersecurity concepts, risk analysis, security controls, investigations, and instructional applications addressed throughout the course and reflects the rigor and style of AP Cybersecurity assessments.

GRADE DISTRIBUTION AND SCALE:

Grade Distribution:

Module Exams	70%
Final Exam	10%
Programming Assignments/Labs	6%
Short Answer Assignments	6%
Mastery Exercises	6%
Reflection Paper	2%

Grade Scale:

A	93 – 100
A-	90 – 92
B+	86 – 89
B	83 – 86
B-	80 – 82
C+	77 – 79
C	73 – 76
C-	70 – 72
D	60.0 – 69.9
F	59.9 or below

ACADEMIC STANDING:

NJCTL has established standards for academic good standing within a student's academic program. Students enrolled in any NJCTL online course must receive an 80 or higher to successfully complete a course and receive credit for that course. An 80 is equivalent to a GPA of 2.7 or B-. Additionally, students in an endorsement program must receive a cumulative GPA of 3.0 for all courses combined in order to successfully complete the program.

ACADEMIC INTEGRITY:

Students must assume responsibility for maintaining honesty in all work submitted for credit and in any other work designated by the instructor of the course. Academic dishonesty includes cheating, fabrication, facilitating academic dishonesty, plagiarism, reusing /repurposing your own work, unauthorized possession of academic materials, and unauthorized collaboration.

CITING SOURCES WITH APA STYLE:

All students are expected to follow proper writing and APA requirements when citing in APA (based on the APA Style Manual, 6th edition) for all assignments.

DISABILITY SERVICES STATEMENT:

We are committed to providing reasonable accommodations for all persons with disabilities. Any student with a documented disability requesting academic accommodations should contact the Dean of Students, Melissa Axelsson, for additional information to coordinate reasonable accommodations for students with documented disabilities (melissa@njctl.org).

NETIQUETTE:
Respect the diversity of opinions among the instructor and classmates and engage with them in a courteous, respectful, and professional manner. All posts and classroom communication must be conducted in accordance with the student code of conduct. Think before you push the Send button. Did you say just what you meant? How will the person on the other end read the words?

Maintain an environment free of harassment, stalking, threats, abuse, insults or humiliation toward the instructor and classmates. This includes, but is not limited to, demeaning written or oral comments of an ethnic, religious, age, disability, sexist (or sexual orientation), or racist nature; and the unwanted sexual advances or intimidations by email, or on discussion boards and other postings within or connected to the online classroom.

If you have concerns about something that has been said, please let your instructor know.

CLASS SCHEDULE:

Module	Module Learning Outcomes	Assignments
1 – Introduction to Security	**• Differentiate between threats, vulnerabilities, risks, and security controls.• Explain the CIA Triad and its role in cybersecurity decision-making.• Analyze common cyber threats and attack vectors.• Apply risk management concepts to cybersecurity scenarios.• Utilize PSI instructional strategies to teach foundational cybersecurity concepts.**	**• Short Answer Assignment• Scenario-Based Activities• Mastery Exercises• Module Exam**
2 – Securing Spaces	**• Identify common computing devices and their security challenges.• Explain authentication methods and account security practices.• Analyze device vulnerabilities and indicators of compromise.• Apply security controls to protect devices and user accounts.• Evaluate attack scenarios involving malware and compromised devices.**	**• Short Answer Assignment• Scenario-Based Activities• Mastery Exercises• Module Exam**
3 – Securing Devices	**• Analyze system logs and security events.• Explain the role of monitoring tools and security operations.• Investigate indicators of compromise and suspicious activity.• Apply incident response processes to cybersecurity scenarios.• Evaluate evidence to determine appropriate mitigation strategies.**	**• Short Answer Assignment• Scenario-Based Activities• Mastery Exercises• Module Exam**
4 – Securing Networks	**• Explain fundamental networking and communication security concepts.• Analyze network vulnerabilities and attack methods.• Evaluate the effectiveness of network security controls.• Apply secure communication practices to organizational scenarios.• Investigate network-based threats and recommend mitigations.**	**• Short Answer Assignment• Scenario-Based Activities• Mastery Exercises• Module Exam**
5 – Securing Applications & Data	**• Analyze application vulnerabilities and attack techniques.• Differentiate between data states and data classification levels.• Apply access control models and least privilege principles.• Compare symmetric and asymmetric cryptography and their uses.• Evaluate application security controls, vulnerability management practices, and data protection strategies.• Investigate attacks against applications and data systems and recommend mitigations.**	**• Short Answer Assignment• Scenario-Based Activities• Mastery Exercises• Module Exam**
6 – Reflection & Final Exam	**• Synthesize cybersecurity concepts and instructional strategies learned throughout the course.• Reflect on growth as a cybersecurity educator.• Analyze instructional practices that support student understanding of cybersecurity concepts.• Develop plans for implementing AP Cybersecurity curriculum and PSI pedagogy in the classroom.**	**• Final Reflection Paper• Final Exam**