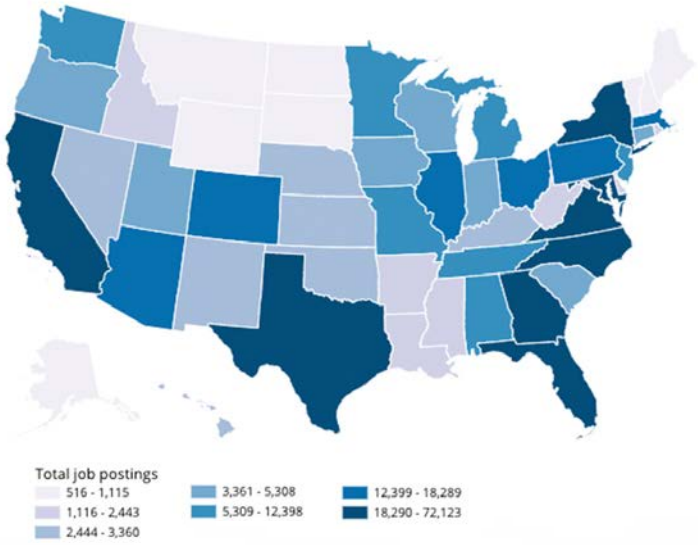
THE CYBERSECURITY CURRICULUM GUIDELINES FOR HIGH SCHOOL STUDENTS

The need for the Cybersecurity Curriculum Guidelines (CCG) is one of importance, as our society continues to become more dependent on computers. While the demand for highly educated and trained cybersecurity professionals is more than a half-million, the number of individuals ready to fill these positions is severely lacking.

The National Cryptologic Museum Foundation provides opportunities for learning and partnerships to advance Cybersecurity education to prepare the next generation to succeed in the cyber workforce of tomorrow. As more high school teachers integrate cybersecurity into their classrooms, the need for a coherent curriculum becomes critically important.



Cybersecurity employment in the United States

With over 500,000 openings, the need for cybersecurity practitioners grows every day. Many are unaware of the cross discipline nature of available jobs and the knowledge, skills and abilities required. Cyberseek.org provides the detailed, actionable data about supply and demand in the cybersecurity job market. By accessing this vital information, students, teachers, counselors, and parents will understand what courses they should take, where to begin a cybersecurity career and what is required to do so. The interactive heat map locates the jobs and the career pathway shows key jobs and their interrelationships. Keep this website bookmarked!

To see the most current vacancies in your state, visit cyberseek.org

The Introduction to Cybersecurity Guidelines has four levels:

The guidelines were developed using the Backward Design Model (Wiggins McTighe 2005) and, designed by educators from high school and higher education. These Guidelines steer curriculum in what should be taught rather than how to teach it and provides students with a visible guide to complete the course. Introduction to Cybersecurity is intended to be equivalent to an intro course in cybersecurity at either a community college or university.

Ethics Cybersecurity has broad ethical implications. It exists within social, organizational, and personal values that undergird beliefs about right and wrong. The Guidelines outline important aspects of cybersecurity ethics that students should be exposed to and investigate.

Establishing Trust The overarching purpose for cybersecurity is to establish and maintain trust. Users and computers need to be trusted. The Guidelines emphasize the cybersecurity principles, the CIA triad and how to question assumptions as the basis for establishing trust and how to apply them.

Ubiquitous Connectivity Networks are used daily by most people in the world. There is no single network but rather a collection of different network technologies that together form a network of networks called the Internet. This makes it necessary for students to understand and effectively use the methods and tools for securing networks.

Data Security Keeping data secure and private is essential for individuals, groups, and governments. Students will study relevant laws and policies governing data; evaluate the tools used to connect cyber-physical systems; and practice using the encryption techniques needed to secure data.

System Security Hardware and software work together to achieve an objective. Adversaries exploit weaknesses in the system to disrupt confidentiality, integrity, or availability. System security helps explain why hardware and software have vulnerabilities, introduces students to some specific vulnerabilities, and addresses the consequences of less secure hardware and software.

Adversarial Thinking Practitioners need to identify critical assets, design and implement systems to protect the assets, identify ways to detect when the protections fail, respond to the failures, and ultimately recover to a working state. To accomplish this, one must think about what can go wrong. The students learn to challenge assumptions and thinking about opposing forces.

Risk The guidelines indicate essential aspects of risk that students in a cybersecurity course should experience, i.e., risk assessment, the inherently uncertain and complex nature of cybersecurity risk due to complexity of systems of systems, the presence of adversaries, the logical malleability of computing, and the dynamic and distributed nature of computing.

Implications Advances and decisions at a local level in computing, connectivity, and big data are driving a global, interconnected phenomenon and have significant cybersecurity implications. The students need to know important historical events and their cybersecurity implications examining the evolution of the threat environment at the local and global level.

The Cyber Center for Education and Innovation (CCEI)

is a private-public partnership between the National Cryptologic Museum Foundation and the National Security Agency. The CCEI will become a cross-sector enterprise delivering programs to encourage government, industry, and academia to share insights, knowledge, and resources to strengthen cybersecurity protection and workforce development across the nation while also revitalizing the National Cryptologic Museum.

NATIONAL CRYPTOLOGIC MUSEUM FOUNDATION
CYBER CENTER FOR EDUCATION & INNOVATION
★ HOME OF THE NATIONAL CRYPTOLOGIC MUSEUM ★

cryptologicfoundation.org ▪ NCMFinfo@cryptologicfoundation.org ▪ 443-795-4498