K-12 Cybersecurity Learning Standards Fact Sheet

The K-12 Cybersecurity Learning Standards will help increase cybersecurity literacy and build a robust pipeline of future cybersecurity talent.

- The standards aim to ensure that students not only have a foundational understanding of cybersecurity, but also the skills and knowledge needed to pursue cybersecurity careers in greater numbers.

The K-12 Cybersecurity Learning Standards are the first effort to align cybersecurity learning criteria across all 50 states.

- Until now, there have only been a few models of state-developed cybersecurity standards and no national standards specific to cybersecurity.
- The standards aim to bridge this gap and help align developers and teachers.

The K-12 Cybersecurity Learning Standards will be used in schools and districts around the country.

- States now have the option to adopt the K-12 cybersecurity learning standards ahead of the 2022-2023 school year.
- Districts can also adopt the standards in full or embed them into existing content standards.

The K-12 Cybersecurity Learning Standards center around three core themes: Computing Systems (CS), Digital Citizenship (DC) and Security (SEC).

- These themes represent key fundamentals in cybersecurity education.
- Each core concept covers a range of cutting-edge cybersecurity topics, from the Internet of Things (IoT) to Threat Actors.

The K-12 Cybersecurity Learning Standards are critical to guaranteeing that the future cybersecurity workforce is equipped to handle the cybersecurity challenges of tomorrow.

- The global cybersecurity workforce shortage is projected to reach 1.8 million unfilled positions by 2022, making the effort to standardize and prioritize cybersecurity curriculum in K-12 classrooms more important than ever.
- The standards aim to build a strong, more diverse talent pipeline to protect U.S. national security and maintain U.S. competitiveness on the world stage, while helping address the cybersecurity workforce shortage.

Since the kickoff of this initiative in September 2020, CYBER.ORG has engaged experts across various fields to help craft the standards.

- CYBER.ORG convened a writing committee of K-12 educators and collected input from key stakeholders across education, government, and industry to increase the relevancy and value of the standards.
- Some of the organizations involved in the standards process include: EduTech, Maricopa County Regional School District, Grambling State University, Louisiana Tech University, Palo Alto Networks, Southwest Airlines, Cybersecurity Infrastructure Security Agency (CISA), National Initiative for Cybersecurity Education (NICE), and the National Security Agency (NSA).
- The standards development process was facilitated by McREL International, a nonprofit, nonpartisan education research, development and service organization that helps schools, districts and education agencies improve outcomes for students.