National K-12 Cybersecurity Education Implementation Plan

Introduction

The K12 Cybersecurity Education Implementation Plan's intent is to establish a coordinated, coherent portfolio of National K-12 Cybersecurity Education activities so that efforts and assets are deployed effectively and efficiently for greatest potential impact. The intent is to encourage a more deliberate focus among new and existing efforts and create synergies among programs and agencies. This plan is created to implement the NICE Strategic Plan and supports the Federal Cybersecurity Workforce Strategy.

The implementation of the strategies and actions shared will increase the quantity, quality, and diversity of students pursuing cybersecurity careers by developing and maintaining a National K-12 Cybersecurity Education Implementation Plan that supports and guides the community on cybersecurity academic and career pathways through:

- rigorous academic programs,
- learning experiences,
- exposure to career opportunities,
- high quality teacher professional development, and
- information regarding available internship and scholarship prospects.

ROADMAP

1. Increase Career Awareness
2. Infuse Cybersecurity Across the Education Portfolio
3. Stimulate Innovative Educational Approaches
4. Identify Academic and Career Pathways

1.<u>Increase Career Awareness:</u> *Increase and Sustain Youth and Public Engagement in Cybersecurity Activities*

a. Establish a cybersecurity career awareness campaign targeting educators, students, parents, administrators, and counselors.
b. Develop co-curricular experiences (e.g., competitions, camps, clubs, boy/girl scouts, etc.) for youth that excite them about careers in cybersecurity and introduce them to the corresponding academic pathways.
c. Increase the appeal of the cybersecurity profession to a diverse audience.

2.<u>Infuse Cybersecurity Across the Education Portfolio</u>: *Design Cybersecurity Education for the future STEM and Cybersecurity Workforce*

a. Infuse cybersecurity concepts into classroom instruction that align to the NICE Cybersecurity Workforce Framework.
b. Develop and replicate programs that support youth obtaining knowledge, skills, and abilities required for success in the future STEM and Cybersecurity Workforce.

3.<u>Stimulate Innovative Educational Approaches</u>: *Improve K-12 Cybersecurity Education Instruction*

a. Increase coordination among teacher preparation, professional development, support, and recognition efforts within existing and proposed cybersecurity educator programs.
b. Stimulate innovative educational approaches to accelerate learning and skills development.

4.<u>Identify Academic and Career Pathways:</u> *Increase the number of youth pursuing a cybersecurity or cybersecurity related degree, certificate or job*

a. Develop a nationally recognized cybersecurity *career* pathway for high school students that improves upon state Career Technical Education (CTE) and Programs of Study (POS).
b. Develop a nationally recognized cybersecurity *academic* pathway for elementary, middle and secondary school students.

c. Increase the number of schools who are providing dual enrollment, early college programs, and other creative efforts that challenge students academically and provide opportunities to reduce the time and cost of obtaining a college degree.