National K12 Cybersecurity Education ROADMAP

Email: nice@nist.gov

Website: www.nist.gov/nice

December 7, 2021

NICE
NATIONAL INITIATIVE FOR
CYBERSECURITY EDUCATION

TABLE OF CONTENTS

Introduction

The National K12 Cybersecurity Education ROADMAP establishes a coordinated, coherent portfolio of National K12 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 government agencies.

The five major elements and accompanying strategies of the National K12 Cybersecurity Education ROADMAP align to the 2021-2025 National Initiative for Cybersecurity Education (NICE) Strategic Plan which was released in November 2020. The development and maintenance of the National K12 Cybersecurity Education Roadmap will support and guide the community on K12 cybersecurity education, and sharing these strategies will increase the quantity, quality, and diversity of students pursuing cybersecurity careers.

1. Increase Cybersecurity Career Awareness

Grow and sustain youth and public engagement in promoting cybersecurity career awareness and exploration

1.1 Communicate the value and purpose of a national K12 cybersecurity education strategy (i.e., the K12 Cybersecurity Education Roadmap) and the need for engagement

1.2 Expand public awareness and engagement of the cybersecurity career awareness campaign targeting educators, students, parents, counselors, and others that influence career choices

1.3 Support effective co-curricular experiences (e.g., competitions, camps, clubs, informal experiences, etc.) for youth that excites them about careers in cybersecurity and introduces them to multiple corresponding career pathways

1.4 Improve the appeal and understanding of the cybersecurity work roles identified in the Workforce Framework for Cybersecurity (NICE Framework)

1.5 Promote participation of underserved groups in cybersecurity activities and education programs to support diversity, equity, inclusion, and accessibility

1.6 Identify and disseminate successful methods and metrics for building cybersecurity career awareness

2. Engage Students Where Disciplines Converge

Identify, design, and share cybersecurity resources for the future STEM and cybersecurity workforce

2.1 Engage students where disciplines converge using cybersecurity as an interwoven and complex pursuit that blends disciplines and industry sectors and makes STEM and cybersecurity learning meaningful and inspiring

2.2 Assist in building computational literacy by infusing cybersecurity concepts aligned to the NICE Framework into the learning process focusing on the holistic convergence[1] of educational disciplines

2.3 Determine and share proven methods and metrics for recognizing successful and meaningful programs and content

2.4 Develop and replicate successful content and programs that support youth obtaining cybersecurity credentials (e.g., diplomas, degrees, certificates, certifications, badges) that assess learners' cybersecurity competencies using evidence-based practices and assessments that can be emulated by other stakeholders

[1] *The National Science Foundation defines convergence as the deep integration of knowledge, techniques, and expertise from multiple fields to form new and expanded solutions for addressing scientific and societal challenges and opportunities. Convergence refers to not only the convergence of expertise across disciplines but also the convergence of academic, government, and industry stakeholders to support scientific investigations and enable rapid translation of the resulting advances. Convergence integrates knowledge, tools, and ways of thinking from multiple disciplines to form a comprehensive means to tackling scientific and societal challenges that exist at the interfaces of multiple fields. The Federal Coordination in Science, Technology, Engineering, and Mathematics Education (FC-STEM) Convergence Interagency Working Group recognizes that new global problems cannot be solved by looking at them through a single lens or a particular mindset. Instead, experts from different disciplines must work together and blend their knowledge, theories, expertise, methods, data, and research to create coherence and comprehensive solutions. This needs to be modeled at every level of education and research and should be incorporated in K-20 learning.*

3. Stimulate Innovative Educational Approaches

Enrich K12 cybersecurity education instruction and learning

3.1 Enhance coordination among teacher preparation, professional development, support, and recognition efforts within instructional training options and existing and proposed cybersecurity educator programs

3.2 Stimulate innovative and effective educational approaches to accelerate learning and skills development leveraging work done in other domains

3.3 Improve the quality of cybersecurity instruction and learning by advocating for implementation of proven pedagogical practices and supporting innovative and evidence-based instructional strategies (e.g., differentiated instruction, game-based learning, blended learning, team science learning, expeditionary learning, simulations, hands-on activities)

3.4 Promote increasing the number of educators who can effectively promote cybersecurity careers and prepare youth for obtaining cybersecurity or cybersecurity-related credentials

3.5 Recognize and publicize proven methods and metrics for recognizing proven pedagogical practices and evidence-based learning methods and experiences

3.6 Develop communities of practice that enable educators and community members to discuss best practices, challenges, opportunities, and implement instructional changes

4. Promote Cybersecurity Career Pathways[2]

Cultivate youth pursuing cybersecurity or cybersecurity-related credentials (e.g., diplomas, degrees, certificates, certifications, badges)

4.1 Inspire, cultivate, and develop exceptional cybersecurity talent through a continuum of opportunities to enrich our current and future cybersecurity workforce

4.2 Support and promote cybersecurity career preparedness for students through a variety of learning pathways (e.g., Career Technical Education-CTE, Programs of Study-POS, youth apprenticeship, pre-apprenticeship, PTECH, early college programs, and other “alternative” opportunities)

4.3 Encourage schools to provide 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 cybersecurity or cybersecurity-related credential

4.4 Promote youth work-based learning experiences (e.g., internships, externships, job shadowing, apprenticeships)

4.5 Identify and share proven methods and metrics for recognizing successful cybersecurity career preparedness opportunities

[2] *Workforce Innovation and Opportunity Act (WIOA) defines a career pathway as “a combination of rigorous and high-quality education, training, and other services that: (A) aligns with the skill needs of industries in the economy of the State or regional economy involved; (B) prepares an individual to be successful in any of a full range of secondary or postsecondary education options, including registered apprenticeships; (C) includes counseling to support an individual in achieving the individual’s education and career goals; (D) includes, as appropriate, education offered concurrently with and in the same context as workforce preparation activities and training for a specific occupation or occupational cluster; (E) organizes education, training, and other services to meet the particular needs of an individual in a manner that accelerates the educational and career advancement of the individual to the extent practicable; (F) enables an individual to attain a secondary school diploma or its recognized equivalent, and at least one recognized postsecondary credential; and (G) helps an individual enter or advance within a specific occupation or occupational cluster.” [Section 3(7) of WIOA] for additional information see PCRN: Career Pathways Systems (ed.gov) and Building Career Pathways Programs & Systems: Insights from TAACCCT (dol.gov).*

5. Prioritize Research

Enhance efficiency and effectiveness of K12 cybersecurity education programs and instructional practices

5.1 Develop a systematic approach to identify and share content and instructional best practices in educational and engagement environments

5.2 Advance K12 cybersecurity programs by sharing educational and engagement environments based on evidence using a systematic approach

5.3 Curate and communicate K12 cybersecurity career awareness and preparedness research

5.4 Generate a results-oriented annual report to guide K12 cybersecurity education process and progress

Next Steps

The NICE K12 Community of Interest and other members of the NICE Community Coordinating Council are continually developing actions for the strategies identified for each of the five elements of the ROADMAP that align to the NICE Strategic Plan. Further, the K12 Community of Interest continues to identify indicators of success for each action. The K12 Community of Interest maintains an environmental scan of existing programs, resources, and activities and encourages other community members to add to the "evergreen" environmental tracker resource. The K12 Community of Interest will also establish project teams, as necessary, to pursue actions, many in coordination with other NICE Working Groups. To learn more about the NICE Community Coordinating Council, NICE K12 Community of Interest, and current project teams or to get involved, visit www.nist.gov/nice/community.