NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Strategic Plan

2021-2025

GOAL 1 CAREER DISCOVERY

Career Discovery

Promote the Discovery of Cybersecurity Careers and Multiple Pathways

OBJECTIVES

- 1.1 Identify and share effective practices for promoting cybersecurity career awareness and discovery to diverse stakeholders
- 1.2 Increase understanding of multiple learning pathways and credentials that lead to careers that are identified in the Workforce Framework for Cybersecurity (NICE Framework)
- 1.3 Develop and utilize proven tools and resources to identify individuals most likely to succeed in a cybersecurity career
- 1.4 Provide information and tools about cybersecurity-related career options to those who influence career choices (e.g., teachers and faculty, school counselors, career coaches, career development personnel, mentors, and parents or guardians)
- 1.5 Galvanize employers to promote discovery and exploration of cybersecurity career opportunities and work-based learning experiences

GOAL 2 LEARNING PROCESS

Learning Process

Transform Learning to Build and Sustain a Diverse and Skilled Workforce

OBJECTIVES

- 2.1 Foster proven learning methods and experiences shown to effectively build and sustain a diverse, inclusive, and skilled cybersecurity workforce
- 2.2 Advocate for multidisciplinary approaches that integrate cybersecurity across varied curricula that support diverse learners from a variety of backgrounds and experiences
- 2.3 Improve the quality and availability of credentials (e.g., diplomas, degrees, certificates, certifications, badges) that validate competencies
- 2.4 Facilitate increased use of performance-based assessments to measure competencies and the capability to perform NICE Framework Tasks
- 2.5 Encourage the use of Learning and Employment Records to document and communicate skills between learners, employers, and education and training providers
- 2.6 Champion the development and recognition of teachers, faculty, and instructors as part of the in-demand workforce

GOAL 3 TALENT MANAGEMENT

Modernize the Talent Management Process to Address Cybersecurity Skills Gaps

OBJECTIVES

- 3.1 Enhance the capabilities of organizations and sectors to effectively recruit, hire, develop, and retain the talent needed to manage cybersecurity-related risks
- 3.2 Utilize new technologies such as machine learning and automated approaches to increase connections and fit between employers and job seekers
- 3.3 Align qualification requirements according to proficiency levels to reflect the competencies and capabilities required to perform tasks in the NICE Framework
- 3.4 Promote the establishment of more entry-level positions and opportunities that provide avenues for growth and advancement
- 3.5 Encourage and enable ongoing development and training of employees, including rotational and exchange programs, to foster keep current talent with diverse skills and experiences
- 3.6 Nurture effective practices in reskilling the unemployed, underemployed, incumbent workforce, and transitioning veterans to prepare them for careers in cybersecurity

GOAL 4 NICE FRAMEWORK

Expand Use of the Workforce Framework for Cybersecurity (NICE Framework)

OBJECTIVES

- 4.1 Document and widely disseminate methods, resources, and tools shown to successfully expand use of the NICE Framework
- 4.2 Align the NICE Framework to the NIST Cybersecurity Framework, NIST Privacy Framework, and other cybersecurity, privacy, and risk management publications
- 4.3 Establish processes for regularly reviewing, improving, and updating the NICE Framework
- 4.4 Explore development of new tools or integration of NICE Framework data into existing tools to increase access and facilitate interoperability
- 4.5 Identify and highlight components of the NICE Framework (Tasks, Knowledge,and Skill Statements) that could be potentially performed via automated techniques
- 4.6 Expand international outreach to promote the NICE Framework and document approaches being used in other countries

GOAL 5 RESEARCH

Drive Research on Effective Practices for Cybersecurity Workforce Development

OBJECTIVES

- 5.1 Collaborate with stakeholders to research and disseminate results on factors that influence the impact of cybersecurity education, training, and workforce development
- 5.2 Inspire bold investigation of critical societal and global issues impacting cybersecurity education and workforce, synthesizing data-driven evidence, and providing trustworthy advice
- 5.3 Prioritize research on the most effective and proven practices for blending successful learning practices across education, training, and workforce development settings
- 5.4 Utilize research results to inform programs and curriculum design, foster continuous learning opportunities, impact learner success, and ensure equitable access

ABOUT NICE

The National Initiative for Cybersecurity Education (NICE) is a partnership among government, academia, and the private sector focused on education, training, and workforce development that will strengthen the cybersecurity posture of organizations. This "cybersecurity workforce" includes those whose primary focus is on cybersecurity as well as those in the workforce who need specific cybersecurity-related knowledge and skills in order to perform their work in a way that enables organizations to properly manage the cybersecurity-related risks to the enterprise. The NICE Strategic Plan outlines the vision, mission, values, goals, and objectives for both the organization and the greater NICE community. It is the result of the extensive experience of – and engagement with – NICE partners. NICE will develop implementation plans and metrics through a consultative process that includes the NICE Interagency Coordinating Council and the NICE Community Coordinating Council. Actions based on this plan will be pursued and results achieved by organizations and individuals working collaboratively and through their independent efforts. NICE is led by the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce.

VISION

Prepare, grow, and sustain a cybersecurity workforce that safeguards and promotes America's national security and economic prosperity.

MISSION

To energize, promote, and coordinate a robust community working together to advance an integrated ecosystem of cybersecurity education, training, and workforce development.

VALUES

Foster Communication and encourage openness to build trust.

Facilitate Collaboration, combining the knowledge and skills of stakeholders with multiple viewpoints and approaches to achieve the best outcomes.

Share and Leverage Resources to support community-developed approaches and solutions.

Act Based on Evidence, pursuing objective and reliable sources of information and using data to inform actions or decisions.

Evaluate and Improve our effectiveness by using quantitative metrics and qualitative measures.

Challenge Assumptions, examining rationale for past and present education, training, and workforce approaches and applying critical analysis to future solutions.

Stimulate Innovation, inspiring and experimenting with new approaches in a search for creative and innovative solutions that might disrupt or defy the status quo.

Model Inclusion, advocating and enabling engagement of stakeholders from diverse backgrounds and with varying viewpoints.

NICE Communication Channels

NICE WEBSITE

nist.gov/nice

eNEWSLETTER

nist.gov/nice/enewsletter

NICE EMAIL DISTRIBUTION LIST

tinyurl.com/subscribe-nice

NICE WEBINAR SERIES

nist.gov/nice/webinars

EMAIL US

nice@nist.gov

linkedin.com/company/nist-nice

twitter.com/NISTcyber

#NICEatNIST