IMPLEMENTATION PLAN

NICE Strategic Plan

Email: nice@nist.gov

Website: www.nist.gov/nice

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

TABLE OF CONTENTS

INTRODUCTION

The 2021-2025 National Initiative for Cybersecurity Education (NICE) Strategic Plan was released in November 2020. The NICE Strategic Plan included five goals, each with several objectives. After the release of the Strategic Plan, the NICE Program Office and NICE Community Coordinating Council began work to form an Implementation Plan for the established goals and objectives.

The Implementation Plan process began with an environmental scan of existing programs and activities. Following this review, work began to establish strategies, tactics, and success measures for each objective in the Strategic Plan. Figure 1 provides a visual representation of each component of the Strategic and Implementation Plans. Additionally, the following definitions were used:

- Goals – ***high-level*** descriptors of the outcome to create (What)
- Objectives – ***specific*** outcomes that define the goal (What)
- Strategies – ***high-level*** plan that will be followed to achieve the goals (How)
- Tactics – ***specific*** actions to take to achieve the goals (How/Detail)
- Success Measures – ***measure*** impact and document outcomes

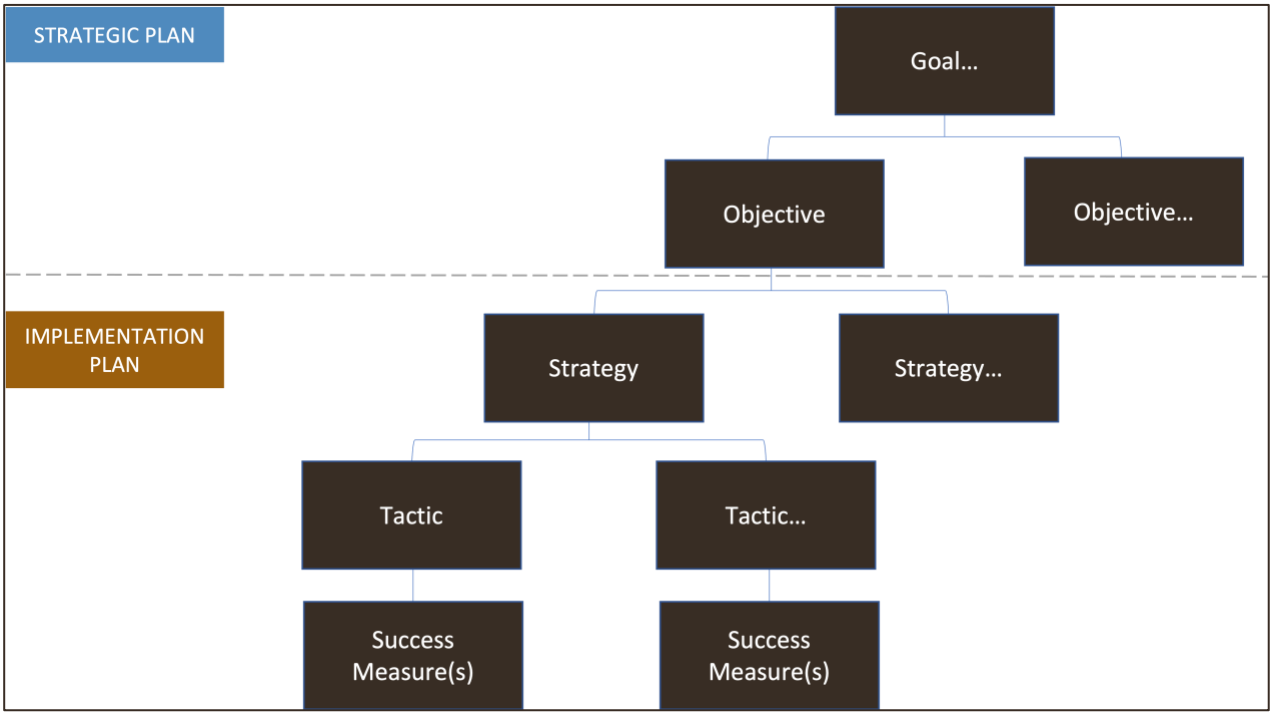

Figure 1 - Structure for the NICE Strategic Plan Implementation Plan

ACKNOWLEDGEMENTS

This Implementation Plan was developed by members of the NICE Community Coordinating Council. In particular, the three Working Groups of the NICE Community Coordinating Council led the development of strategies, tactics, and success measures for the three correlating NICE Strategic Plan goals: Promote Career Discover, Transform Learning Process, and Modernize Talent Management. While NICE appreciates and acknowledges the efforts of all Community members who participated in the Implementation Plan development, NICE would like to specifically recognize the co-chairs of the three Working Groups for their significant contributions.

Promote Career Discovery Working Group Co-Chairs:

- James "Jimmy" Baker, Cybersecurity Evangelist and Author
- Monica Gomez, Cisco Systems, Inc.
- Roland Varriale II, Argonne National Laboratory

Transform Learning Process Working Group Co-Chairs:

- Richard Spires, Richard A. Spires Consulting
- Dr. Aurelia T. Williams, Norfolk State University

Modernize Talent Management Working Group Co-Chairs:

- Lynsey Caldwell, Leidos
- Kevin Perry, Chief, United States Army
- Dr. Melissa Woo, Michigan State University

In addition to these Working Group co-chairs, NICE thanks the remainder of the NICE Community Coordinating Council Leadership Team: co-chairs Dr. Marni Barker-Stein and Dr. Jon Brickey; and co-chairs of the communities of interest Terrance Campbell, Tony Bryan, Laurin Buchanan, Jennifer Oddo, Amelia Philips, Thomas Trevethan, and Bradley Wolfenden.

GOAL 1

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

Strategies

- 1.1.1 Identify and share effective practices in career awareness, discovery, and development to include successful strategies for diversity, equity, inclusion, and accessibility (DEIA) initiatives
- 1.1.2 Establish and maintain a program and activity directory of projects, initiatives, and resources related to cybersecurity career awareness, exploration, preparation, placement, maintenance, and mentoring
- 1.1.3 Promote relevant conferences and convenings, foster and advance advocacy campaigns such as Cybersecurity Career Awareness Week and promote community champions for building cybersecurity career ecosystems
- 1.1.4 Create a Cybersecurity Careers Ambassadors program to promote cybersecurity career awareness, exploration, and development
- 1.1.5 Coordinate, implement, and continue to evaluate effective cybersecurity career awareness communication touch points with multiple 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)

Strategies

- 1.2.1 Identify and track multiple learning pathways and credentials aligned to NICE Framework Work Roles and Competencies
- 1.2.2 Identify and develop tools and resources that promote learning pathways and credentials aligned to NICE Framework Work Roles and Competencies
- 1.2.3 Share messaging to attract, develop, and retain talent and relay the innumerable and varied career options in cybersecurity
- 1.2.4 Collaborate and support alignment of the NICE Framework Work Roles and Competencies with career tools and resources

1.3 Develop and utilize proven tools and resources to identify individuals most likely to succeed in a cybersecurity career

Strategies

- 1.3.1 Identify and track proven tools and resources to identify individuals most likely to succeed in a cybersecurity career
- 1.3.2 Establish and maintain a program and activity directory of tools, instruments, and resources used to identify individuals most likely to succeed in cybersecurity
- 1.3.3 Promote recognition strategies, scholarships, assistantships, and fellowships that identify and encourage individuals to succeed in cybersecurity

1.3.4 Encourage educational institutions to offer dual enrollment, early college programs, and other creative efforts that challenge students academically

1.3.5 Promote the cybersecurity ecosystem to provide competitions, challenges, and other innovative ways that provide opportunities 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)

Strategies

1.4.1 Identify, track, and disseminate successful programs and effective resources and tools, including those that increase participation of women, minorities, veterans, persons with disabilities, and other underrepresented populations in the cybersecurity workforce

1.4.2 Convene and collaborate with career influencers to identify specific resource needs to disseminate content around cybersecurity career awareness, selection, reskilling, upskilling, and retention

1.4.3 Identify, develop, and disseminate effective strategies that improve the appeal and understanding of cybersecurity Work Roles and Competencies and promote participation of underserved groups in cybersecurity activities and education programs

1.4.4 Enhance coordination and communication among cybersecurity employers and career influencers

1.4.5 Elevate public awareness about cybersecurity focus areas, Work Roles, job openings, and wages, including variance by location

1.5 Galvanize employers to promote discovery and exploration of cybersecurity career opportunities and work-based learning experiences

Strategies

1.5.1 Identify, develop, and disseminate communication tools and resources that help employers overcome common barriers to providing work-based learning experiences

1.5.2 Identify, track, measure, and disseminate successful cybersecurity work-based learning opportunities

1.5.3 Provide a resource which connects individuals with business partners who are interested in offering work-based learning opportunities or other kinds of career development activities

1.5.4 Leverage corporate social responsibility to promote discovery and exploration of cybersecurity careers and work-based learning experiences

1.5.5 Evaluate and disseminate cybersecurity employers' requirements and preferences of individuals seeking cybersecurity work-based learning experiences

GOAL 2

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

Strategies

- 2.1.1 Identify and promote effective learning methods and educational practices and programs that grow and develop a diverse and inclusive cybersecurity workforce
- 2.1.2 Inspire the adoption of successful approaches that lead to the retention of a diverse and inclusive cybersecurity workforce
- 2.1.3 Equip learners with in-demand cybersecurity competencies and skills that they can demonstrate to employers
- 2.1.4 Foster the pursuit of personal effectiveness competencies that will enable lifelong learning to sustain a 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

Strategies

- 2.2.1 Promote cybersecurity as a foundational competency across many different disciplines or careers
- 2.2.2 Encourage digital citizenship and digital literacy at all age levels
- 2.2.3 Establish the importance of cybersecurity as a priority in the discovery, design, and development of new technologies
- 2.2.4 Discover and promote creative and effective mechanisms for attracting and including learners with differing learning styles

2.3 Improve the quality and availability of credentials (e.g., diplomas, degrees, certificates, certifications, badges) that validate competencies

Strategies

- 2.3.1 Articulate a common definition of credentials that includes a variety of examples for cybersecurity and shows alignment to the NICE Framework
- 2.3.2 Seek evidence to document and communicate the value of stackable credentials that allow learners to progress on a cybersecurity career path
- 2.3.3 Increase the accessibility and affordability of credentials for cybersecurity
- 2.3.4 Discover or develop criteria and processes for identifying the quality of a credential

2.4 Facilitate increased use of performance-based assessments to measure competencies and the capability to perform NICE Framework Tasks

Strategies

- 2.4.1 Raise awareness of the value and importance of using performance-based assessments to measure competencies and the capability to perform NICE Framework Tasks
- 2.4.2 Work to ensure that academic degree programs and industry-recognized certifications effectively measure cybersecurity Competencies and the ability to perform NICE Framework Tasks
- 2.4.3 Partner with product and service companies to support efforts to have performance-based assessments to measure cybersecurity competencies and the capability to perform NICE Framework Tasks
- 2.4.4 Formalize internships that provide experience and verifiable competencies in the ability 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

Strategies

- 2.5.1 Raise awareness of the value of Learning and Employment Records (LERs)
- 2.5.2 Establish the necessary infrastructure, policies, processes, and systems for sustaining the use of LER's
- 2.5.3 Identify and showcase pilot projects or early adopters of LER's
- 2.5.4 Encourage employers to document achievements of their employees for inclusion in an LER system

2.6 Champion the development and recognition of teachers, faculty, and instructors as part of the in-demand workforce

Strategies

- 2.6.1 Determine the scope and significance of the cybersecurity educator workforce gap
- 2.6.2 Influence policies that enable hiring and retention of qualified and diverse educators
- 2.6.3 Promote professional development and mentoring opportunities for educators
- 2.6.4 Establish recognition programs for cybersecurity educators at all levels
- 2.6.5 Explore expansion of NICE Framework to include competencies or work roles for cybersecurity educators

GOAL 3

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

Strategies

- 3.1.1 Advance employer readiness by ensuring that appropriate personnel, especially human resource and talent acquisition teams, are informed of cybersecurity recruitment and hiring best practices
- 3.1.2 Identify barriers that may exist in current practices for increasing the diversity of the cybersecurity workforce and promote appropriate interventions
- 3.1.3 Promote use of effective cybersecurity competency and skills assessment as part of the hiring and selection process
- 3.1.4 Investigate trends and factors that affect retention or mobility of cybersecurity workforce and design corresponding interventions to increase retention or facilitate mobility

3.2 Utilize new technologies such as machine learning and automated approaches to increase connections and fit between employers and job seekers

Strategies

- 3.2.1 Explore new paradigms and innovative approaches to increase the efficiency and effectiveness of talent management systems
- 3.2.2 Identify existing and emerging tools that can more rapidly help connect employers with qualified applicants
- 3.2.3 Encourage the use of Learning and Employment Records in human resource systems as a mechanism for the ongoing documentation of employee achievements
- 3.2.4 Showcase success stories of how employers are improving their ability to find talent

3.3 Align qualification requirements according to proficiency levels to reflect the competencies and capabilities required to perform tasks in the NICE Framework

Strategies

- 3.3.1 Encourage the development of job descriptions with qualification requirements that are aligned to the NICE Framework
- 3.3.2 Document and showcase employers who specify qualification requirements as part of their career pathways
- 3.3.3 Promote adoption of streamlined job announcements with required versus preferred qualifications that are known to encourage diverse candidates
- 3.3.4 Specify unique regulatory or other knowledge and skill requirements of certain sectors to increase likelihood of applicant career readiness
- 3.3.5 Clarify the appropriateness of academic degrees, industry-recognized certifications, work experience, and other credentials for cybersecurity roles

3.4 Promote the establishment of more entry-level positions and opportunities that provide avenues for growth and advancement

Strategies

- 3.4.1 Investigate the return on investment and retention rates for employing and developing entry-level talent versus hiring mid-career talent
- 3.4.2 Ensure that entry-level positions are scoped appropriately and do not have onerous or unreasonable qualification requirements
- 3.4.3 Recommend employers to emphasize diversity of background and experience for entry-level positions
- 3.4.4 Connect local employers seeking entry level talent to the education and training providers in their community that prepare entry-level talent

3.5 Encourage and enable ongoing development and training of employees, including rotational and exchange programs, to foster and keep current talent with diverse skills and experiences

Strategies

- 3.5.1 Encourage employers to build and invest in a training culture that includes executive support
- 3.5.2 Identify and promote role-based training sources for NICE Framework aligned knowledge and skills, including access to sector-specific knowledge
- 3.5.3 Develop existing staff for cybersecurity roles
- 3.5.4 Emphasize the importance of including development of professional skills or “soft” skills and promote resources that describe them, how to obtain them, and how to assess them
- 3.5.5 Promote hands-on learning experiences and collaborative projects that are crucial to developing high performing teams

3.6 Nurture effective practices in reskilling the unemployed, underemployed, incumbent workforce, and transitioning veterans to prepare them for careers in cybersecurity

Strategies

- 3.6.1 Promote adoption of skills assessments as an approach that enables those with related experience or recent training to qualify for work roles
- 3.6.2 Identify effective practices that can scale for transitioning military to civilian work roles that leverage their experience and skills
- 3.6.3 Encourage employers to consider leveraging the incumbent workforce to transition to cybersecurity careers and focus on reskilling opportunities
- 3.6.4 Encourage local and regional community engagement between employers with education and training providers that focuses on reskilling or upskilling the unemployed and underemployed to facilitate talent development and discovery

GOAL 4

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

Strategies

- 4.1.1 Illustrate and illuminate how the NICE Framework can be used in practice
- 4.1.2 Document and promote successful uses of the NICE Framework
- 4.1.3 Utilize the NICE Framework Resource Center as a central place to document and share content related to the NICE Framework
- 4.1.4 Encourage and promote increased use of the NICE Framework with public and private organizations

4.2 Align the NICE Framework to the NIST Cybersecurity Framework, NIST Privacy Framework, and other cybersecurity, privacy, and risk management publications

Strategies

- 4.2.1 Publish a guide on the authoring of Task, Knowledge, and Skill (TKS) statements to support consistency in the NICE Framework, improve understanding and adoption, and serve as a model for related workforce frameworks, guides, and publications to follow and adopt
- 4.2.2 Publish a guide on the authoring of Competency statements to support consistency in the NICE Framework, improve understanding and adoption, and serve a model for related workforce frameworks, guides, and publications to follow and adopt
- 4.2.3 Review existing NICE Framework mappings and develop a consistent mapping approach as a resource for others to follow
- 4.2.4 Align the NICE Framework to targeted publications and resources

4.3 Establish processes for regularly reviewing, improving, and updating the NICE Framework

Strategies

- 4.3.1 Define and put into action a regular ongoing, transparent, community-involved review and update process for NICE Framework Task, Knowledge, and Skill statements, Competencies, and Work Roles
- 4.3.2 Provide the NICE Framework supplemental materials on a web-based platform that will enable improved access, provide machine-readable versions of the content, and accommodate regular updates
- 4.3.3 Update NICE Framework content to align to the 2020 revision based upon a comprehensive review

4.4 Explore development of new tools or integration of NICE Framework data into existing tools to increase access and facilitate interoperability

Strategies

- 4.4.1 Conduct an environmental scan and assessment of existing tools that use the NICE Framework to inform recommendations for next steps
- 4.4.2 Consult the NICE Community to identify needs and desired features for NICE Framework tools
- 4.4.3 Identify and pursue opportunities to integrate the NICE Framework into existing tools or to develop new tools

4.5 Identify and highlight components of the NICE Framework (Tasks, Knowledge, and Skill statements) that could be potentially performed via automated techniques

Strategies

- 4.5.1 Review and update existing TKS statements that could potentially be performed via automation
- 4.5.2 Engage the NICE Framework Users Group to identify potential future areas of automation and how they might impact existing NICE Framework Tasks

4.6 Expand international outreach to promote the NICE Framework and document approaches being used in other countries

Strategies

- 4.6.1 Identify materials that would be helpful for other countries if translated into their native language
- 4.6.2 Conduct an environmental scan and maintain a repository of international approaches to creating a common lexicon for cybersecurity or similar workforces
- 4.6.3 Host or attend convenings where the NICE Framework can be shared with international groups
- 4.6.4 Identify and disseminate resources for international use of the NICE Framework
- 4.6.5 Engage international stakeholders during NICE Framework public comment periods

GOAL 5

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

Strategies

- 5.1.1 Curate, summarize, and categorize evidence-based and systemic research areas or topics, approaches, measurement and metric tools, and assessment paradigms
- 5.1.2 Foster collaborative approaches to efficiently map, explore, and characterize research related to cybersecurity and associated disciplines for education, training, and workforce development
- 5.1.3 Collaborate with multiple stakeholders in the research ecosystem to support intramural and extramural research on factors that influence the success of cybersecurity education, training, and workforce development and disseminate successful practices
- 5.1.4 Encourage industry, federal agencies, organizations, associations, and non-profit entities to further the research agenda with all cybersecurity education, training, and workforce development efforts

5.2 Inspire bold investigation of critical societal and global issues impacting cybersecurity education and workforce, synthesizing data-driven evidence, and providing trustworthy advice

Strategies

- 5.2.1 Increase the impact and benefit from research resources and products by making them more accessible to the public, machine-readable, and aligned with FAIR (findable, accessible, interoperable, and reusable) principles
- 5.2.2 Increase the visibility of societal and global issues impacting cybersecurity workforce development through collaborations with international partners and associations to inspire bold cybersecurity workforce investigation, 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

Strategies

- 5.3.1 Identify, curate, track, and maintain research based effective practices and resources for cybersecurity education, training, and workforce development
- 5.3.2 Enhance coordination and communication among cybersecurity employers, educators, and training providers

5.4 Utilize research results to inform programs and curriculum design, foster continuous learning opportunities, impact learner success, and ensure equitable access

Strategies

5.4.1 Identify and document successful and proven approaches, techniques, and model programs that transform learning and skills development for cybersecurity careers or in other areas that could be applied to cybersecurity

5.4.2 Proactively use evidence-based and systemic research and data to ensure best practices are incorporated into program and curriculum design, are labor-market responsive, and have the greatest possible impact on learner success

NEXT STEPS

The NICE Community Coordinating Council Working Groups are continually developing tactics for the strategies identified in this Implementation Plan. Further, the Working Groups continue to identify measures of success for each tactic. Additionally, the Working Groups will continue to conduct an environmental scan of existing programs and will encourage other community members to pursue the objectives and strategies in accordance with their organizational missions and priorities. The Council will also establish project teams, as necessary, to pursue actions to address any gaps in support of this Implementation Plan.

To learn more about the NICE Community Coordinating Council and current project teams or to get involved, visit www.nist.gov/nice/community.