‘National Initiative for Cybersecurity Education (NICE) Community Coordinating Council

Project Charter:
Improve the Quality and Availability of Credentials

January 12, 2022

Project Team Leads:
Nancy Austin, PhD and Jeremy Rabson, MBA, SANS | GIAC

Table of Contents

1. Project Team Description

As cybersecurity matures as a discipline, the importance of credentials (to include academic degrees and certifications) becomes ever more critical to supporting the development of the cybersecurity workforce. **The National Initiative for Cybersecurity Education (NICE) is part of the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce**, and is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development. NICE recognizes this throughout its guiding documents, statements, and values calling attention to the importance of innovation, collaboration, and a diversity of opinions.

This project falls under the auspices of the Transform Learning Working Group, which focuses on Goal 2 of the NICE Strategic Plan: Transform Learning to Build and Sustain a Diverse and Skilled Workforce. In its recently published Implementation Plan, NICE defined within this goal an objective to improve the quality and availability of credentials (e.g., diplomas, degrees, certificates, certifications, badges) that validate competencies (1). This project will address this credential-related objective and address the strategies identified in the NICE implementation plan that support achieving this objective.

2. Project Team Purpose

Summary (the Elevator Pitch)

"Cybersecurity is still a relatively young and very dynamic discipline with a plethora of credentials offered by academic, commercial, and non-profit organizations. This project's purpose is to improve the quality and transparency of cybersecurity-related credentials, while also increasing the accessibility and affordability of such credentials for individuals currently in or for those who wish to enter the cybersecurity field. "

Statement of Purpose

Currently, many cybersecurity-related certifications were developed before the existence of the NICE Framework, and as such, there were no standards regarding the knowledge and skills or competency areas that any particular certification should address. Thus, it is difficult for those wanting to increase their skills in cybersecurity to assess the many credential programs to choose which credential would best fit their needs. Further, many credential programs are costly, especially for those looking to enter the cybersecurity workforce. **The purpose of this project team is to bring more clarity, increase the value, and address the affordability of credentials for those that are already cybersecurity professionals or who aspire to enter the field**.

Scope

The scope of this project is to fully address Objective 2.3 of the NICE Implementation Plan, namely to improve the quality and availability of credentials (e.g., diplomas, degrees, certificates, certifications, badges) that validate competencies. Within that objective, four strategies support meeting that objective. These strategies are:

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 credentials for cybersecurity careers
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

3. Project Team Objectives

Within each strategy outlined in the Scope section, there is a draft list of success measures that this project team will seek to achieve. These strategies and success measures include:

Strategy 2.3.1 - Articulate a common definition of credentials that includes a variety of examples for cybersecurity and shows alignment to the NICE Framework

- Review and consider adoption of the definition from the Glossary of Credentialing Terminology
- Differentiate credentials, as necessary, by proficiency levels (e.g., basic, intermediate, and advanced)
- Encourage credential providers to communicate to learners and employers the relationship of the credential to the NICE Framework, especially the capabilities associated with competencies or work roles

Strategy 2.3.2 - Seek evidence to document and communicate the value of credentials for cybersecurity careers

- Produce or update one-pagers such as The Value of Certifications (https://www.nist.gov/system/files/documents/2018/07/24/nice_value_of_certifications_7.19.18.pdf) or The Value of a Higher Education
- Identify criteria for measuring and articulating the value of credentials
- Describe and differentiate the value of credentials derived from education (2 or 4 year or graduate or professional degrees), training (industry-recognized certifications), on the job learning, or self-paced learning (e.g., MOOCs)
- Establish effective practices and solutions for documenting achievements during employment or converting workplace experience into the equivalent of a recognized credential
- Clarify the purpose of a credential when a learner already has the skill
- Show the relationship between the effectiveness of the "learning process" for knowledge and skills development and the resulting "credential."

Strategy 2.3.3 - Increase the accessibility and affordability of credentials for cybersecurity

- Increase awareness and transparency of available credentials for cybersecurity-related competencies or work roles
- Endorse a central repository of available degrees and credentials
- Identify existing ways in which credentials are available based on financial need through scholarships or other creative mechanisms
- Identify ways to lower the cost of credentials
- Ensure that access to credentials supports the need to diversify the workforce, including learners from disadvantaged socio-economic backgrounds

Strategy 2.3.4 - Discover or develop criteria and processes for identifying the quality of a credential

- Identify or establish benchmarks or measures of quality (e.g., academic accreditation, ANSI 17024, etc.)
- Encourage more rigorous and trusted academic credentials with an emphasis on competency- and skills-based credentials

4. Project Team Deliverables

The team's final deliverables are dependent on the knowledge the project team develops through its iterative process. The earliest deliverables will include an environmental scan to understand the landscape of what currently exists in terms of cybersecurity credentials. The team will leverage existing artifacts from NICE and other organizations to the degree they support the project team objectives.

References

1. **The National Initiative for Cybersecurity Education .** Imple Tomentation Plan. 2021.