IMPROVE THE QUALITY AND AVAILABILITY OF CREDENTIALS

NICE | community coordinating council

JULY 2022

Research paper for discussion from the NICE Community Coordinating Council, Transform Learning Process Working Group, Improve the Quality and Availability of Credentials Project Team.

Nancy Austin, PhD, Project Team Lead

Jeremy Rabson, MBA, SANS | GIAC, Project Team Lead

Team members: Jeff Grann, Kane Porter, Ben Mossé, Charmaine Sheeler-Mitchell

The Transform Learning Process Working Group focuses on the NICE Strategic Plan's objective to improve the quality and availability of credentials (e.g., diplomas, degrees, certificates, certifications, badges) that validate competencies (2.3). The group conducts an ongoing environmental scan of programs, projects, and initiatives related to this strategic plan's goals and objectives to assess the scope and sufficiency of efforts. The group also identifies gaps where more attention and effort are needed. The group identifies strategies and tactics necessary to meet its objective.

Authored January 2022 - July 2022
Published July 2022

Table of Contents

Executive Summary

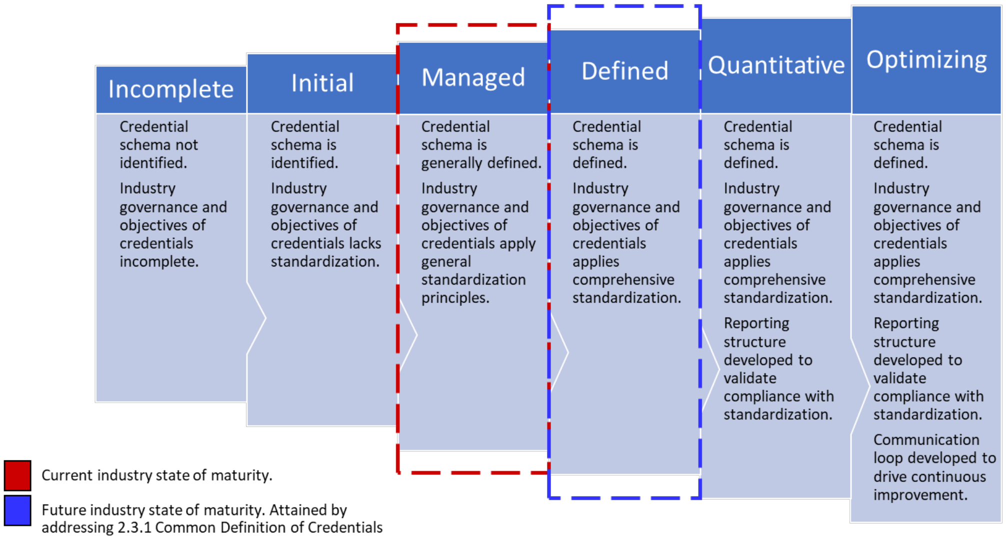
“Cybersecurity is still a relatively young and very dynamic discipline with a plethora of credentials offered by academic, commercial, and non-profit organizations. This project’s purpose is to improve the **quality and transparency** of cybersecurity-related credentials, while also increasing the accessibility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

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.

Strategy 2.3.1:
Articulate a common definition of credentials

Problem: *Why is a common definition of credentials necessary?*
A preliminary environment scan of cybersecurity careers revealed complicated frameworks, poor UX, and lack of transparency for pathways & ROI, which is creating market confusion about the value of credentials (degrees, certificates, certifications).

Maturity Levels for Credentials



Incomplete	Initial	Managed	Defined	Quantitative	Optimizing
Credential schema not identified.	Credential schema is identified.	Credential schema is generally defined.	Credential schema is defined.	Credential schema is defined.	Credential schema is defined.
Industry governance and objectives of credentials incomplete.	Industry governance and objectives of credentials lacks standardization.	Industry governance and objectives of credentials apply general standardization principles.	Industry governance and objectives of credentials applies comprehensive standardization.	Industry governance and objectives of credentials applies comprehensive standardization.	Industry governance and objectives of credentials applies comprehensive standardization.
				Reporting structure developed to validate compliance with standardization.	Reporting structure developed to validate compliance with standardization.
					Communication loop developed to drive continuous improvement.

🟥 Current industry state of maturity.

🟦 Future industry state of maturity. Attained by addressing 2.3.1 Common Definition of Credentials

Audience: *Who are the primary, secondary, tertiary, etc. stakeholders?*
Many stakeholders participate in the credentialing marketplace and could be considered primary beneficiaries.

- **Learners and workers** could understand the unique focus of the di-fferent credentials available to them and see how best to get to where they want to go.
- **Credential providers** could more clearly describe the credentials they o-ffer and how they help meet the needs of individuals, businesses, and the community.
- **Employers** could discover and hire people who have the skills and competencies needed for the jobs of today while e-ffectively planning for and signaling the needs of tomorrow.
- **Policymakers and thought leaders** could better understand the credentials available, their connections, and can better support economic needs at scale.

Scope: *Where should the glossary apply, and where should it not apply?*
The scope of the larger project charter 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. This subteam focuses exclusively on 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”.

Development stages: *When should the common definition of credentials be considered entering or exiting threshold developmental phases–the characteristics that determine its readiness for the next cycle of development?*
Common definitions for credentials are particularly important for all public information that could be used by any stakeholder. A minimal-level of credential information should be consistently available to the public in order to support the most common and important use cases across the cybersecurity workforce, such as credential marketing materials, website metadata, career navigation applications, regulatory reports, and accreditation reviews. Additional credential information should be supported in a consistent manner so that credential providers may enrich the description of their credentials.

A regular business process should also be used to update or extend the common definition of credentials according to an explicit namespace policy for any changes.

Frameworks: *How should the ‘common definition of credentials’ content be framed–grounding the scope within accepted or discussed structures?*
At a high-level, any common definition of cybersecurity credentials needs to be well contextualized with existing definitions of credentials in order to facilitate and promote a broad set of career pathways. In the United States of America, state policymakers and agencies play a vital role in ensuring their residents and employers have the information they need to make well-

informed decisions about credential offerings. **States are tasked with meeting multiple, often competing, goals to efficiently and effectively identify, fund, and deliver education and training services. However, the data used to inform credential policy and practice are often insufficient and kept in silos, leading to confusion, duplication, and frustration.** There are almost one million education and training opportunities in the U.S., and transparency about credentials and their competencies and efficient data practices are essential to many of the key decisions states must make.

With Credential Engine's infrastructure—including the Credential Transparency Description Language (CTDL) schema and open-source Credential Registry—states can provide short-term solutions to meet the challenges of a rapidly changing economy—and make key contributions to long-term structural change and innovation. State policymakers can take the inefficiencies out of the labor marketplace and provide more efficient and equitable access to actionable information through the prioritization of credential transparency. As of April 2022, this work is already underway in 28 states and regions, and across 2 regional consortia of states. The CTDL schema has also been explicitly required and/or referenced in multiple state procurement solicitations and competitive federal grants. Based on these considerations, the project team recommends endorsing use of the CTDL schema as a common definition of credentials. **Because the CTDL schema is a living language that is already used by over one thousand credential providers, the team also recommends using Credential Engine's GitHub repositories to raise issues and their processes for significant updates.** Credential Engine maintains a minimum data policy that can be extended by partners and benchment data models based on types of credentials.

Content: *What should be the form and function of the 'common definition of credentials'?*
Credential information should be explicitly articulated by the credential provider in forms that promote broad and equitable use by all stakeholders. Today, many stakeholders use, and increasingly expect, data-intensive applications for all kinds of purposes, such as navigation, shopping, and social networking. These applications rely on common definitions to function, specifically they utilize open schemas that enable both humans and machines to decode semantic meanings across multiple contexts. Schemas include definitions of specific terms and rules concerning the potential relationships amongst these terms (analogous to a grammar).

This form of a common definition enables the communication patterns that promote transparency of information and positive market dynamics amongst stakeholders. Website developers regularly use schemas to describe key information about the content of their webpages. This information is regularly used by search engines to recommend links based on a user's search behavior. For example, the NICE website uses multiple schemas in the webpage's header to communicate important information, such as the website's name, title, creator, modified date, and description. Users of search engines are provided with links to the NICE website based, in part, upon the degree to which the user's search request matches the website's meta data header.

Cybersecurity credentials could be described similarly using a robust credential-specific schema so that users could discover credential offerings relevant to their career pathway. In particular, credential offerings could describe alignments to components of the NICE Framework using a schema so that users can more easily identify relevant credentials via search engines. This approach will entail significant coordination within NICE and segmented external communications for multiple audiences considering the many different cybersecurity career pathways and the significant number of cybersecurity credentials currently offered (see ‘Career Pathways and Credentials’ subteam draft report). We encourage NIST/NICE to actively pursue use of these schema-based practices for its common definition of credentials.

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

Introduction

Credentials have an important role to play in closing the Cyber Security skills gap. A perfectly functioning credentialing system would support decisions of both individuals and businesses. First, learners would be able to identify which credentials would support their job aspirations in specific job roles. Second, hiring managers would have confidence that individuals with specific credentials would have specific skills.

The challenge today is that neither learners nor employers have any measure of certainty from the credentialing structure. Many people feel they do not achieve their desired outcomes after obtaining a credential, and many organizations do not feel that the credentials are more than a rough guide in helping them hire.

We believe that the solution is to provide:

- More information to people investigating Cyber Security careers on how to get started and how to process the labyrinth of different credentials e.g. a “Getting started in Cyber Security - What you need to know” pdf.
- More transparency on 1) what is required to obtain a credential 2) the skills and knowledge that the credential provides and 3) the outcomes of people who have gained a credential.
- Understanding of how different credentials connect to one another and can work together to drive a career journey.
- Improved process in the creation and management of credentialing programs to ensure that credentials are well designed and appropriately administered.

There should be no delusions that any system will solve all individual and business challenges. It is imperative to recognize that there are multiple pathways to a career in cybersecurity. Building a career takes time, continual learning and a measure of good fortune. Under no circumstances should any work on Credential Quality lead people to believe that a credential is all that stands between them and success. No talent development pathway works for everyone. Neither can any one credential. No matter how successful the Cyber Security industry is at implementing the ideas above, employers will never view credentials as a perfect forcaster of job success. That means that credentials are ultimately helpful but not determinative.

Definition of Quality

What is quality or rather, what do we mean when we use the term in our context? Does a quality credential:

- Allow someone to get a job using the specific skills they have been taught?
- Allow someone to get a job because the credential marks them as someone who has the talent to learn what is needed to do the job?
- Offer psychometric validity that knowledge has been gained?
- Act as proof of a hands on capability?

There have been many attempts to define quality in higher education. Many of those efforts have focused on service quality and tend to integrate educational outcomes for students with other university missions e.g. research and societal impact. An additional set of research focuses on learning outcomes e.g. Using Student Learning as a Measure of Quality in Higher Education. Given the strength of the NICE framework and the work done by NIST, we think it makes sense to use the NIST definition with its focus on utility, objectivity, and integrity. The full NIST outline can be found here: https://www.nist.gov/nist-information-quality-standards.

The critical part of the NIST definition is as follows:

> **Quality** is an encompassing term comprising utility, objectivity, and integrity. Therefore, the OMB Guidelines sometimes refer to these four statutory terms, collectively, as "quality."
>
> **Utility** refers to the usefulness of the information to its intended users, including the public. In assessing the usefulness of information that the agency disseminates to the public, NIST considers the uses of the information not only from its own perspective but also from the perspective of the public. As a result, when transparency of information is relevant for assessing the information's usefulness from the public's perspective, NIST takes care to ensure that transparency has been addressed in its review of the information.
>
> **Objectivity** consists of two distinct elements: presentation and substance. The presentation element includes whether disseminated information is presented in an accurate, clear, complete, and unbiased manner and in a proper context. The substance element involves a focus on ensuring accurate, reliable, and unbiased information. In a scientific, financial, or statistical context, the original and supporting data will be generated, and the analytic results will be developed, using sound statistical and research methods.
>
> **Integrity** refers to security – the protection of information from unauthorized access or revision, to ensure that the information is not compromised through corruption or falsification.

NOTE: We believe that outcomes have an important role to play in understanding the quality of a credential. The NIST definition was created for information (usefulness, presentation, substance, and protection) and not credentialing outcomes, but we believe the definition still works: as long as outcomes are part of what is measured as utility, learners should find that they can identify the right credential for them.

Standardizing language

Any attempt to measure credential quality is going to require a consistent nomenclature. Different types of credentials ought to be measured in different ways and we can make no progress unless we agree on terminology and language. Fortunately, the NICE working group has created a helpful starting point for a *common definition of credentials.*

Measuring Utility

How might we measure the ability of a cyber credential to provide learners with specific skills and competencies that are desired in the workplace? Three approaches come to mind:

1. Open source reviews: these reviews might be broken into learner reviews and business reviews. Practically however, business reviews might be difficult to source but learners can easily provide information on their ability to obtain jobs, promotions, higher salaries, or increased job competence. Open source reviews might look much like product reviews on Amazon.com. Given the frequent gaming of these reviews by bots and bad actors there would likely need to be a mechanism for certifying the reviewer had gained the associated credential which necessitates support and involvement of the credential providers.
2. Specialist evaluation - akin to Consumer Reports: Specialized reviewers can take different credentials and evaluate them for a set of quality metrics e.g. how well is information communicated? Is the information practical? Do they believe people with the credential can engage successfully in a set of tasks? The challenge here is that the content behind credentials is continually evolving and credential programs are often lengthy. Whatever specialist evaluation systems are devised must deal with an unusually rapid pace of change.
3. Third party review of open source content: Paul Morgan has put together an interesting starting point at www.pauljerimy.com. His approach essentially scours comments on certifications across a suite of social media type websites and creates a representative aggregate view. Currently, pauljerimy.com focuses on the difficulty and topical areas of certifications in particular but the scope might be expanded to include other cyber credentials and information on workplace receptivity to the credential.

Tying Credentials to Work Roles

As a way of helping learners understand which credentials might work for them, it would be helpful if credentials were tied to specific work roles in the NICE framework. There are a few challenges to making this happen:

- Credential organizations usually map the credential to work roles and there is no third party oversight under usual circumstances.
- The US Department of Defense does, in some circumstances, provide review of credentials and associated work roles. The challenge is that the DoD tends to look primarily at ANSI accredited certifications and not the broader credentialing market. This can leave great education programs on the outside looking in. Furthermore, DoD review can take quite some time. That makes it an approach that is likely to have difficulty keeping pace with the rapid change in the cybersecurity market.

The challenges listed should not deter us from finding a way to tie credentials to Work Roles. It might be that the methods listed in the above section on “Measuring Utility” will work for Job Role mapping.

Conclusion

The discussion above tends to emphasize the challenges of different approaches to measuring quality. Ultimately, it seems like the best approach is to use some version of open source information to let the market dictate what it perceives as quality. Whether the system is curated or not there is tremendous value for learners and employers alike in a large sample set approach to determining which credentials can successfully lead down which pathways. It’s our hope that industry groups including NICE, employers, credential providers, and cyber professionals can come together in a manner that helps learners understand the right path for them and can guide employers as they seek job applicants with relevant skills.

Strategy 2.3.2:
Seek evidence to document and communicate the value of credentials for cybersecurity careers.
Strategy 2.3.3:
Increase the accessibility and affordability of credentials for cybersecurity

The Value of Certifications

There are multiple pathways to a career in cybersecurity. Building a career takes time, continual learning and a measure of good fortune. Under no circumstances should people believe that a certification is all that stands between them and success. No talent development pathway works for everyone. Ultimately, credentials in general and certifications in particular, are helpful but not determinative.

Employers have shifted their focus towards **competencies**. That is to say, job applicants are being tested on their timed ability to solve real world problems. Is the candidate workforce ready for the specific role? This shift toward competency-based hiring and promotion ensures that the individuals most capable of performing the roles and responsibilities required of a specific position are those selected for that position. Competencies were re-introduced to the NICE Framework in 2020 and their importance is only growing. (See: NISTIR 8355, NICE Framework Competencies: Assessing Learners for Cybersecurity Work. *Final version pending.*)

The new hiring and promotion emphasis on work-role ready competencies, combined with the unregulated explosion of often-costly certifications offered to the public presents a confusing landscape for those seeking to pursue or advance in a cybersecurity career. So, what is the ROI of a certification in 2022 and looking ahead? **Are certifications a legacy paradigm as the market shifts to a new paradigm based on skills and competencies demonstrated, for example, in a portfolio?** Statistics on job postings requesting specific certifications are not a useful metric, especially for entry-level positions; certifications will not translate to a job offer unless the certification outcome is also backed up by specific hands-on competencies that will be tested in real time during the interview process. It is no longer enough to remember or understand;

one must also move to the next level of Bloom's Revised Taxonomy and demonstrate applied learning. Until more employers are willing to take on motivated (but not-role-ready) job applicants, it is up to the learner to show up for a new job role or job interview with role-ready competencies. ***What is the value of a certification in this scenario? What market innovations can support a new paradigm centered on competencies?***

It Takes a Village. Certifications can be an appropriate way to gain new knowledge, build specific skills and have this validated by a third-party. A certification exam might be scenario-based or it might be an old-fashioned multiple choice test that assesses book-learned knowledge. The exams cost money and work is underway to bring consumers more transparency about the certification industry. By themselves, certifications can be milestones, building blocks, an employer-mandated compliance requirement, a good or bad investment, and in some cases, a form of gate-keeping.

Certifications are most valuable when leveraged into the next step of applied skills development within a mentoring community that can offer ongoing appropriate challenges and timely feedback. This community of practice experiential learning step might take the form of on-the-job training, an apprenticeship, or the demonstration of competencies with a portfolio of successfully completed hands-on challenge projects.[1] It might be via capture the flag competitions or other gamified platforms that help learners build confidence exercising their new skills in a mentoring community. These competencies are going to supplement certifications and further validate work-role readiness.

Certifications may appear to be an end goal, but it is more helpful to think of them as a means to an end - part of the multi-step process of developing work-role ready competencies to contribute to a team.

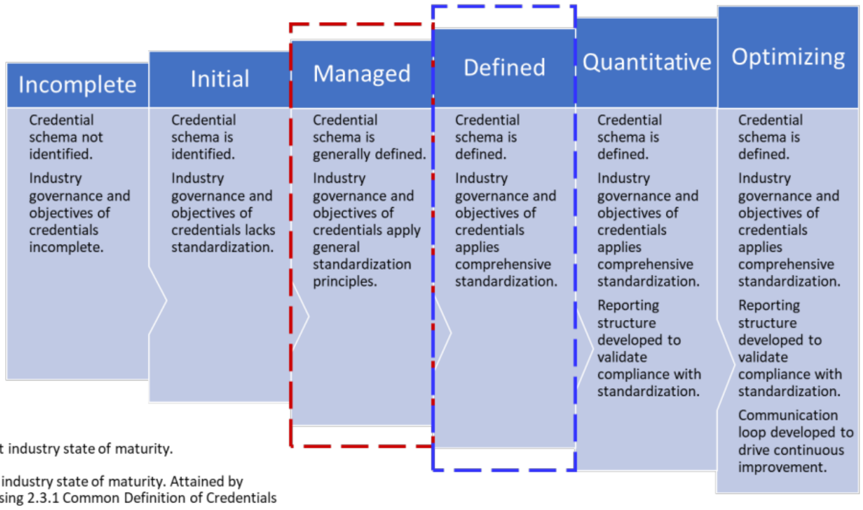
[1] Since at least 1945, a successful model for distributed, civic-minded citizen, low-cost community mentoring after an FCC credential step has existed in Amateur Radio. The ARRL club model supports competency development for everyone in electronics, sensors, space, and spectrum. Cybersecurity is bigger than IT.

What is the Value of Certification in 2022 and forward?

- Certifications are a means to an end, but do not guarantee employment;
- Certification training and exams can be costly and a barrier;
- Competencies are crucial and more important than knowledge tests;
- Cybersecurity is a team sport. Join a welcoming, mentoring community that can offer appropriate hands-on challenges and timely feedback to put those certification skills to work with confidence;
- It's possible to start learning cybersecurity for free, or at a very low cost, and demonstrate competency with a portfolio.
- **Be mindful of a new employer-driven paradigm shift that values competencies over certifications because the legacy certification paradigm failed to meet employer needs.** This is an opportunity for market innovation in the certification industry. NICE supports this transformation through emerging transparency standards, such as Credential Engine's Credential Transparency Description Language (CTDL), and a common definition of credentials.[2]

[2] See above: Strategy 2.3.1 - Articulate a common definition of credentials.

Maturity Levels for Credentials



Incomplete	Initial	Managed	Defined	Quantitative	Optimizing
Credential schema not identified. Industry governance and objectives of credentials incomplete.	Credential schema is identified. Industry governance and objectives of credentials lacks standardization.	Credential schema is generally defined. Industry governance and objectives of credentials apply general standardization principles.	Credential schema is defined. Industry governance and objectives of credentials applies comprehensive standardization.	Credential schema is defined. Industry governance and objectives of credentials applies comprehensive standardization. Reporting structure developed to validate compliance with standardization.	Credential schema is defined. Industry governance and objectives of credentials applies comprehensive standardization. Reporting structure developed to validate compliance with standardization. Communication loop developed to drive continuous improvement.

🟥 Current industry state of maturity.

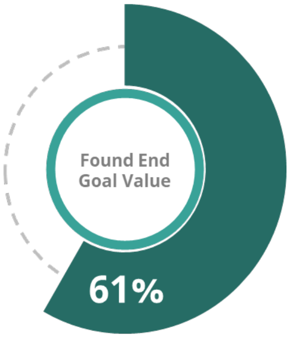
🟦 Future industry state of maturity. Attained by addressing 2.3.1 Common Definition of Credentials

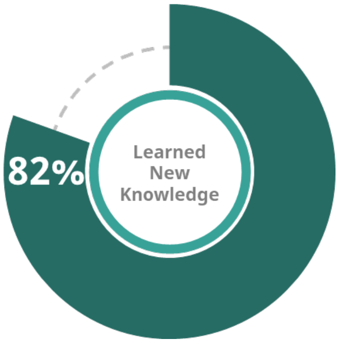
The Value of Certifications (one-pager)

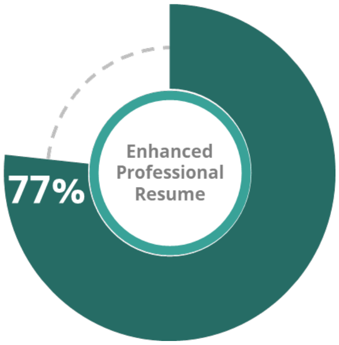
Of the 29,000 candidates surveyed in the 2021 Value of IT Certification Report, the **top motivation behind IT certification is a desire to upskill at 73%.**[3]

61% found end-goal value in certifications.[4]

- IF you are employed and want to advance in your current job. 61% (+)
- IF you are desiring to obtain a specific IT role 61% (+)
- Certifications helped 82% of learners learn new knowledge, and 77% felt certifications enhanced their professional resume.
- Between 2019 to 2021, employers stepped back from paying for certification exams and training, putting the burden on the individual upskilling.[5]

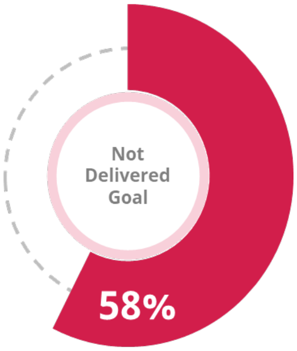


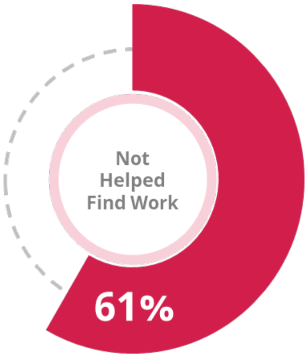




Certifications do not guarantee employment[6]

- 58% reported the earned certification had not yet delivered on the learner's goal of a job change
- 61% of the unemployed or underemployed reported the certification had not yet helped them find work.





Competencies are crucial & more important than knowledge tests.[7]

- Employers have shifted toward competency-based hiring and promotions in what amounts to a paradigm shift.[8]

[3] PearsonVue, *2021 Value of IT Certification Report*, 3. See: 2021-09-IT-VoC-Report-FINAL_update.pdf

[4] Ibid, 16.

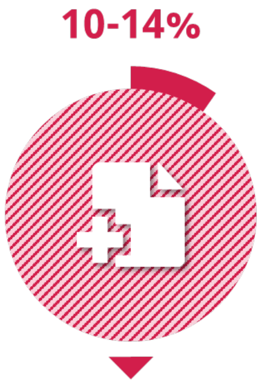
[5] Ibid, 18.

[6] Ibid, 16.

[7] NIST-NICE Project Charter Team for *Improve the Quality and Availability of Credentials* (2022).

[8] Demand has shifted toward demonstrated competencies that some updated certifications may effectively test, but many legacy certifications do not. For example, the Cyberseek data updated for June 2022 shows that there are over 2x as many *Security+* certification holders as job posting requests for that certification. [213,775 : 94,175 = 2.3] Further, only 13% of job postings request that certification per Cyberseek's own data. [94,175 / 714,548 = 13%] The

- Buyer beware: Certifications do not always validate competencies to perform work roles. Look for certifications that provide hands-on learning and performance-based assessments.



Cyberseek data shows certifications with the greatest numbers of holders does not result in the greatest job posting demand

It's possible to start learning IT and cybersecurity for free, or at a very low cost.[9]

- The most common Certification exam prep methods in North America were:
  - Free Materials 58%
  - Practice Tests 52%
  - Purchased self-directed materials 37%
  - Practice Labs 30%[10]

- Globally, **all exam prep methods** scored as **above average effectiveness**. [From 1 (most effective) to 5 (least effective). Scores ranged from 1.66 for *Commercial Training Center* prep to 2.5 for *Practice Labs.*]

Want to learn more? Visit the NIST-NICE Free and Low Cost Online Cybersecurity Learning Content and Learner Resources.

- **NICE - Free and Low Cost Online Cybersecurity Learning Content**
  - An important website that validates market innovators who are providing business insights into the new paradigm shift from credentials to competencies.
  - Request for NICE standards around transparency as a form of consumer protection.

- **NICE - Learner Resources**
  - Attention needed. Request for NICE standards around transparency as a form of consumer protection.
  - *Transparency standards needed.* Cyberseek infographics and links prioritize a sponsor narrative that is not helpful in the new workforce ready paradigm valuing competency.
  - Make this the hub for diverse candidates seeking a way into a career in cybersecurity.

reason for this is not due to market demand for this expensive certification but a legacy compliance requirement set by the DoD. What will motivate Legacy Certifications to stay relevant going forward and deliver to the nation's defenders? Innovation is mission critical.

[9] PearsonVue, *2021 Value of IT Certification Report*, 24.

[10] A metric to watch is **% Practice Tests vs Practice Labs**. Seek more evidence to understand this finding.

Appendices

Next Step Considerations

To support learners as they orient themselves in the rapidly changing field of cyber security, the **National Initiative for Cybersecurity Education (NICE)** may consider the following interaction model when mapping user journeys:

- What are the individual's learning goals:
    - (Develop interactive infographic on various learning goals (career/ further education/ to improve certain skill set etc.) expanding on current resource page):
        - https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/learner-resources

- What are the competencies individuals are required to demonstrate:
    - (Formalize and finalize competencies mapping. Develop interactive infographic to support user filtering of categorized competency schema):
        - https://csrc.nist.gov/publications/detail/nistir/8355/draft

- Which resources on the NICE website (free/ low cost) will support this directive:
    - (Validate existing list and support both open source and specialist reviews of vendors on the website, this will enable external user feedback to be captured in a centralized repository. Where issues exist, identify organizations that have been flagged for providing lower quality or misrepresenting credentials):
        - https://www.nist.gov/itl/applied-cybersecurity/nice/resources/online-learning-content

- Which community of interest may individuals join to put into practice their understanding:
    - (Grow the community through connections with established forums/ blogs/ communities including github/ reddit etc.)
        - https://www.nist.gov/itl/applied-cybersecurity/nice/community/community-coordinating-council#Workinggroups

Project Team Member Contact Information

Nancy Austin, PhD | KC1NEK
Career Coach, Leonardo Coaching
ResilientNancy@gmail.com [Newport, RI]

Jeremy Rabson, MBA, SANS | GIAC
General Manager, GIAC Certifications
JRabson@sans.org [Boston, MA]

Jeff Grann, PhD
Credential Solutions Lead
Credential Engine
jgrann@credentialengine.org [MN]

Kane Porter, MPAcc, CPA, CA, CBV, ABV/CFF/CITP, CIPP/C, CISA, PMP
Vice President, Compliance
Peoples Group
kanep@peoplestrust.com [Canada]

Benjamin Mossé
Founder and CEO
Mossé Security
https://www.mosse-institute.com/
benmosse@mosse-security.com [Tampa, FL and Australia]

Charmaine Sheeler-Mitchell, MS
Still working as a ParaLegal - with an underutilized Masters in Cybersecurity
csheeler-mitchell@oshrc.gov [DC/MD]