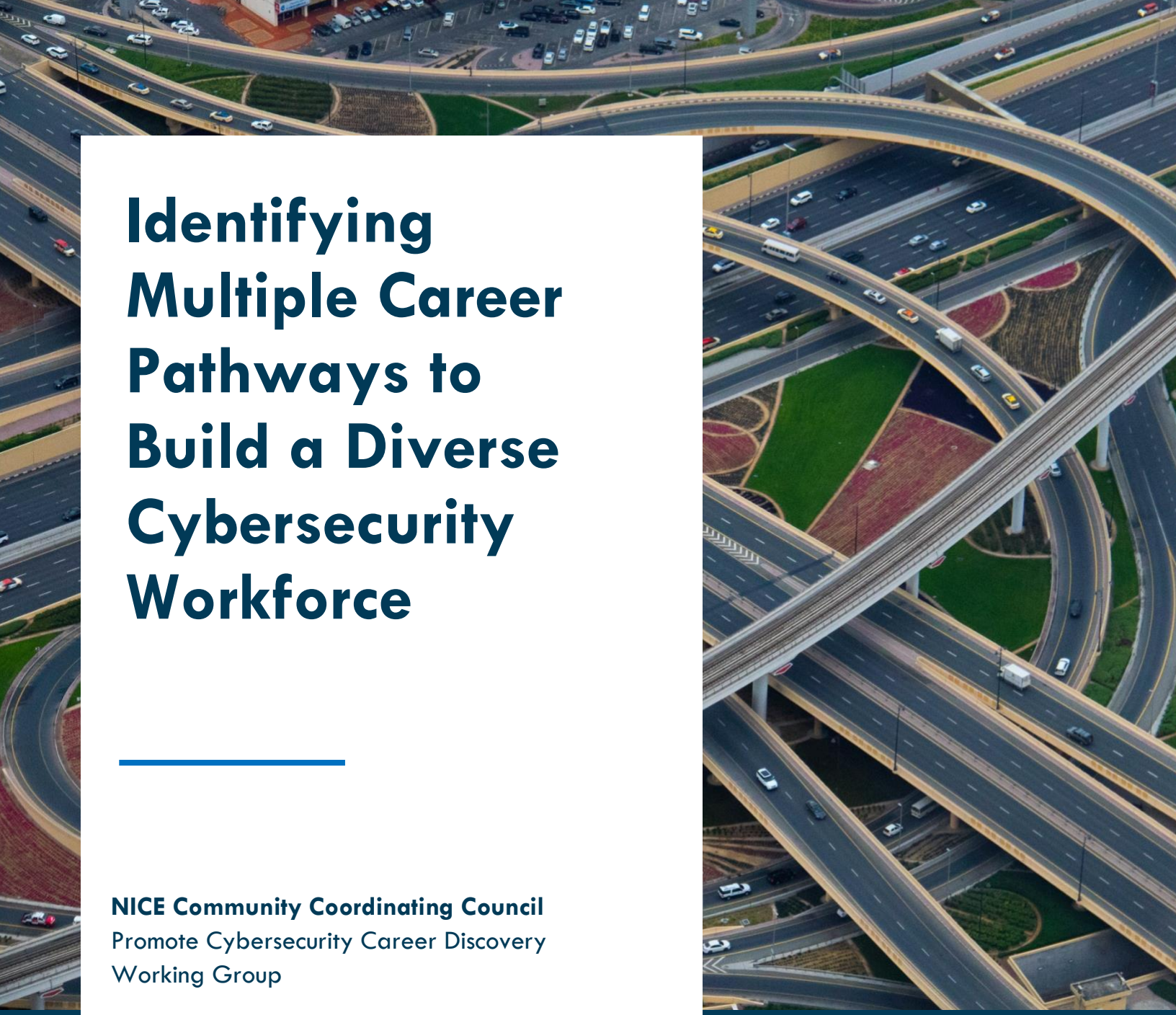


Identifying Multiple Career Pathways to Build a Diverse Cybersecurity Workforce

NICE Community Coordinating Council
Promote Cybersecurity Career Discovery Working Group

MAY 2023

Email: nice@nist.gov
Website: nist.gov/nice

NICE | community coordinating council

Authors & Acknowledgements

Identifying Multiple Career Pathways to Build a Diverse Cybersecurity Workforce was developed by an authoring team that includes representatives from the NICE Community Coordinating Council. NICE wishes to acknowledge and thank these authors, whose dedicated efforts contributed significantly to the publication:

Mark Beaudry

Worcester State University

Connie Bragg

AT&T

Jeff Grann

Credential Engine

Davina Pruitt-Mentle

National Institute of Standards and Technology

Additionally, the document authors gratefully acknowledge and appreciate the contributions of members of the NICE Community Coordinating Council for their contributions. In particular, the authors thank the co-chairs and members from:

The Promote Career Discovery Working Group, led by co-chairs James "Jimmy" Baker, Arrow Electronics; Keith Davis, Koinonia Family Life, Inc.; and Roland Varriale II, Argonne National Laboratory.

The Multiple Career Pathways for Cybersecurity Project Team, led by Jeff Grann, Credential Engine and Mark Beaudry, Worcester State University.

Table of Contents

INTRODUCTION

Report Charge and Approach

In response to a 2017 Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, the 2018 Department of Commerce and Department of Homeland Security Report to the President made recommendations that were incorporated into the FY21 National Defense Authorization Act (NDAA) as:

CYBERSECURITY CAREER PATHWAYS

Pub. L. 116–283, div. H, title XCIV, §9401(d), Jan. 1, 2021, 134 Stat. 4806 , provided that: "Not later than 540 days after the date of the enactment of this Act [Jan. 1, 2021], the Director of the National Institute of Standards and Technology shall, in coordination with the Secretary of Defense, the Secretary of Homeland Security, the Directory of the Office of Personnel Management, and the heads of other appropriate agencies, use a consultative process with other Federal agencies, academia, and industry to identify multiple career pathways for cybersecurity work roles that can be used in the private and public sector" that

> "(A) align with employers' cybersecurity skill needs, including proficiency level requirements, for its workforce; and
> "(B) prepare an individual to be successful in entering or advancing in a cybersecurity career."

This report identifies multiple career pathways aligned with the NICE Workforce Framework for Cybersecurity (NICE Framework) (NIST Special Publication 800-181 Rev. 1) work roles and further discusses career pathways through indices based on the Workforce Innovation and Opportunity Act's (WIOA) career pathway definition. This report provides overall context and clarity, discusses a wide range of existing cybersecurity pathways, summarizes findings regarding current efforts to identify multiple career pathways for cybersecurity work roles aligned to the NICE Framework that can be used in the private and public sector, and provides recommendations for recognizing and promoting cybersecurity career pathway models. The NICE Career Discovery Working Group prepared this report to address objective 1.2 of the first goal of the NICE Strategic Plan 2021-2025 which specifically calls out multiple pathways:

Goal 1, Promote the Discovery of Cybersecurity Careers and Multiple Pathways
Objective 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).

This report will be useful to state and local stakeholders, including education and training providers, workforce and economic development leaders, and employers who are interested in identifying and developing career pathways systems that help students, job seekers, and workers attain knowledge, skills, and credentials that are needed for the wide range of cybersecurity careers. The results provide employers with the skilled workers needed for cybersecurity work roles in high demand.

Report Structure

This report provides context for identifying multiple career pathways in cybersecurity as aligned with the NICE Framework work roles in response to America's continuing need for a knowledgeable and skilled cybersecurity workforce. This report builds on the previous Federal Career Pathways work that identifies strategies and program components that have proven to be effective in helping individuals to persist in education and training that provide learners with credentials that can help in obtaining in-demand jobs.

A broad number of education, training, and workforce and economic development efforts exist in both the public and private sectors. Career pathway approaches to workforce enhancement provide a proven method to extend articulated education and training opportunities between industry sector occupations and accompanying support services, "to enable individuals to enter and exit at various levels and to advance over time to higher skills, recognized credentials, and better jobs with higher pay."[i] The career pathway approach is designed to prepare individuals to progress in their lifelong career journey.

The strategies and processes to identify and develop cybersecurity career pathways highlighted in this report, build on best practices from federal research on career pathway approaches and will be particularly useful to stakeholders as they work to develop and implement career pathway systems that move students, job seekers, and workers most effectively and efficiently to valued credentials and careers.[ii] Alignment with employers' cybersecurity skill needs, is maintained through the NICE Framework, and proficiency level requirements are addressed in the separate report titled, "Measuring Cybersecurity Workforce Capabilities: Defining a Proficiency Scale for the NICE Framework."[iii]

This document consists of four main components:

1. **An introduction** that provides a background of the intent behind this work as well as the research and literature review that details the components of a career pathway as outlined in the Workforce Innovation and Opportunity Act (WIOA) (Pub. L. 113-128) definition.
2. **A common grounding** of definitions and elements related to Career Pathways and cybersecurity work used within this report.
3. **Discussion**
4. **Recommendations**

CAREER PATHWAY ECOSYSTEM

Identification of multiple career pathways to build a skilled and diverse cybersecurity workforce requires a partnership between multiple stakeholders from government, industry, and academia. Often the race to deliver a product in this case identifying career pathways to fast-track individuals into cybersecurity work is undertaken without the full understanding of the complexity of the integrated ecosystem of education, training, and workforce development landscape. This section provides a short synopsis for stakeholders not familiar with the intricacies of the cybersecurity workforce as aligned with the NICE Framework work roles, nor the purpose and requirements for a formal Workforce Innovation and Opportunity Act (WIOA) (Pub. L. 113-128) defined career pathway. Terms are defined and multiple cybersecurity career pathway approaches and development constructs are also discussed in greater detail.

What are Career Pathways?

The widespread deployment of digital technologies throughout the Nation and the ongoing shift to a knowledge-based economy have created strong demand for cybersecurity workers who are capable of building, securing, operating, defending, and protecting defensive and offensive cyber strategies. Cybersecurity work is among the fastest growing and well-paying opportunities in our economy, and the demand for highly skilled cybersecurity workers continues to grow.[iv] Despite these facts, there is a significant shortage of cybersecurity workers.[v] This deficit is a significant risk to America's overall national security and economic prosperity.

There is a growing need to equip America's current and future workforce with the education, training, and credentials required by in-demand businesses and industries—so workers can achieve and maintain economic prosperity, employers can find qualified candidates, and the U.S. economy can remain competitive and continue to grow. The U.S. labor market research indicates that individuals with a high school education or less have experienced low and stagnating wages and high unemployment, whereas those with postsecondary credentials experienced economic gains.[vi] Hendra et al., found that stand-alone instruction and quick job placement training have neither increased employment or earnings over the long run nor helped individuals overcome poverty.[vii] The career pathway approach addresses labor market changes by focusing on postsecondary competencies determined by employee regional needs. In addition, the career pathway approach involves a wide range of wrap-around services needed to enable individuals to enter the workforce and to continue to progress over time in their lifelong learning journey.

Over the years, policymakers and workforce development entities have defined "career pathways" in a wide variety of ways. Federal agencies have spent considerable years detailing best practices and strategies associated with building career pathways. After significant research, in 2012, the U.S. Departments of Education (ED), Labor (DOL), and Health and Human Services (HHS) issued a joint

commitment to promote the use of a career pathway approach as a promising strategy to help adults acquire marketable skills and industry-recognized credentials through better alignment of education, training, and employment, and human and social services among public agencies and with employers. At that time, the three Departments agreed upon a common definition and essential components of a career pathways approach, and outlined six key activities that state, local, and tribal policymakers should undertake to support the development of successful career pathways programs.[viii]

The joint federal definition and key elements to develop successful career pathways were built upon lessons learned over decades of work in carrying out successful workforce education and training programs.[ix] A comprehensive career pathways approach proved to be the most promising method for providing Americans with the knowledge, skills, and credentials needed for in-demand jobs and careers. The three departments defined career pathways as, "**a series of connected education and training strategies and support services that enable individuals to secure industry-relevant certification and obtain employment within an occupational area and advance to higher levels of future education and employment in that area**."[x] The approach connects the necessary adult basic education, occupational training, postsecondary education, career, and academic advising, and support services so that students and workers can successfully prepare for, obtain, and progress in their careers.

The WIOA Definition of Career Pathway

The importance and potential impact of the career pathway structure were acknowledged in 2014 when the United States Congress passed, and President Obama signed into law the bipartisan Workforce Innovation and Opportunity Act (WIOA) (Pub. L. 113-128).[xi] WIOA is designed to strengthen our Nation's public workforce system, helping job seekers access the education, training, and support services they need to obtain and advance in quality jobs and careers and to help businesses hire and retain the skilled workers they need to succeed in a global and digital economy. WIOA contributes to economic growth and business expansion by ensuring the workforce system is job-driven, which supports matching employers with skilled individuals.

The 2014-enacted WIOA included an update to the earlier definition for the implementation of career pathways at Federal, State, local, and tribal levels. The WIOA career pathway approach emphasizes a combination of rigorous and high-quality education, training, and other services that is focused on the needs of high-demand industry sectors and occupations; regional collaboration focused on the skill needs of regional economies; and the establishment of career pathways systems that make it easier for all Americans to attain the skills and credentials needed for family-supporting jobs and careers.[xii] Within these systems, the career pathways program promotes the sequence or pathway of education coursework and/or training credentials aligned with employer-validated work readiness standards and competencies.

The WIOA enables the workforce system to have the flexibility to engage employers in developing the workforce for an economic region.[xiii] From preparing entry-level workers to reskilling transitioning workers, including veterans and their spouses and upskilling incumbent workers, the career pathways approach promotes stronger coordination of services and programs, including greater business involvement in developing and delivering training, and encourages support for job seekers with disabilities and unemployed youth not in school.

Specifically, the WIOA defines the term "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 apprenticeships registered under the Act of August 16, 1937;
(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.

Often a "career pathway" is associated only with items (F) and (G) – credentials and career entry and career advancement. However, (A) thru (E) support a "career pathway system" that is much more comprehensive, so that learning pathways into careers are also considered in this systemic approach. Importantly, career pathways in this definition extend beyond education and training to include supporting services that align both vertically and horizontally across secondary education, postsecondary education, adult education, workforce training and development, career and technical education systems, pathways, and programs. Collaborative partnerships with businesses, and industries along with human service agencies, and other community stakeholders, serve as the foundational structure for proven high-quality and sustainable career pathways.

Key Elements of Career Pathways

The WIOA definition expanded upon the 2012 Federal partners joint commitment letter to promote the use of career pathways to assist youth through adults with acquiring marketable skills and industry-recognized credentials through better alignment of education, training and employment, and social services. In addition to the federal definition, the Federal agencies outlined,

"six key elements that state, local and tribal policy-makers can undertake to support the development of successful career pathways programs. One of the hallmarks of career pathways is that it provides a systemic strategy for integrating educational instruction, workforce development, and human services and linking them to labor market trends and employer needs. Connecting the traditional "silos" of education, labor, and human services to form a coherent system facilitates the development of programs that provide a holistic, comprehensive, and coordinated set of educational and employment services for individuals. These career pathways programs blend elements from different parts of the workforce, education, and human services systems enabling an individual to move seamlessly between school and work. The more the systems are aligned at the state and local levels, the easier it is to create a level of integration necessary to develop comprehensive programs and ensure an individual's success.[xiv]

The Federal department's six key principles (Figure 1) outline how to develop a comprehensive career pathway system. These principles represent the "how-to" of building rigorous and sustainable career pathways and are based on best practices and strategies from the Departments of Education and Labor research. These include:

1. **Build Cross-Agency Partnerships**: Key cross-agency partners at the local and state levels are engaged to participate in the initiative. For example, state and local partners, including, but not limited to employers, workforce investment boards, K12 education, and higher education institutions, adult basic education providers, human services, economic development and community-based organizations, and workforce intermediaries. A holistic approach is

FIGURE 1: CAREER PATHWAYS SIX KEY ELEMENTS

needed in lieu of a siloed perspective to fast-track individuals into and throughout their journey allowing for no duplication of efforts and enabling employees' needs to be met.

2. **Identify Industry Sector and Engage Employers:** Sectors and industries are selected, gap analysis is conducted, and employers are engaged in the development of the career pathways. Sector-based training strategies that include employers in the design of curricula and instruction have demonstrated better employment and earnings outcomes for participants than more traditional approaches.[xv] Career pathways systems are designed using real-time labor market information and active employer involvement to ensure that training and education programs meet the skill and competency needs of local employers.
3. **Design Education and Training Programs:** Career pathways provide potential education and training options and credentials that meet the skill needs of high-demand industries. Key program design features include contextualized curricula, integrated basic education and occupational training, career counseling, support services, assessments, and credit transfer agreements that ease entry and exit and promote credential attainment.
4. **Identify Funding Needs and Strategies:** Career pathways approaches blend and align services from different government, academic, and industry entities to support an individual's successful completion, innovative funding strategies that braid funds from a variety of public and private sources are essential.
5. **Align Policies and Programs:** Federal, state, and local legislation or administrative policies promote career pathway development and implementation. Career pathways programs require significant alignment among workforce, education, and human services to ensure that an individual can move seamlessly throughout their learning journey and earn in-demand credentials. Because of the wide variety of state and local area policy infrastructure, there is no single approach to creating the public policy necessary for career pathways approaches. States, localities, and tribal entities need to examine whether administrative or legislative policy changes are necessary to help individuals participate in programs, enable blended funding, or support the professional development of staff necessary to support career pathway approaches.
6. **Measure System Change and Performance:** Career pathways should ensure measures are used to assess and determine system change and performance including policy changes for system-wide change.

On the same day that WIOA was signed into law, then Vice President Biden issued the *Ready to Work: Job-Driven Training and American Opportunity Report*, laying out a vision for measuring the effectiveness of job-training programs and announcing an array of actions that can be taken, in combination with the new workforce law, to achieve the skilling of America's workforce. What followed was a dramatic increase at the state, regional, and institutional levels in the development of career pathways designed to bring greater efficiency and transparency to the routes from adult education programs, non-credit training, or other starting points to credentials recognized by industry and postsecondary educational institutions. In response, the original Federal partnership on career pathways grew to comprise the White House National Economic Council, the Office of

Management and Budget, and thirteen Federal agencies, including the U.S. Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Housing and Urban Development, Interior, Justice, Labor, the Social Security Administration, Transportation, and Veterans Affairs. An updated letter of commitment highlighted the WIOA definition of "career pathways," emphasized the need for the inclusion of the six key elements in developing a career pathway, demonstrated the continued commitment to collectively promote career pathways, and provided updated information and resources from the expanded Federal partnership to help States, regions, local entities, and tribal communities integrate service delivery across Federal and State funding streams.

Career Pathways Systems vs. Career Pathways Individual Programs

A central assumption that underlies the career pathways approach is that the whole is larger than its parts; that is, it is the combined effect of different career pathways elements working in concert that makes career pathways a success rather than any single career pathways element. Unfortunately, many efforts focus on individual career initiatives rather than the proven holistic approach.

The U.S. Department of Labor in 2020 contracted with Abt Associates to conduct the Career Pathways Descriptive and Analytical Project, a meta-analysis on the impacts of career pathways program approaches. Results draw attention to the vast array of ways programs are designed and implemented and highlight the difference between systems and individual-level career pathway approaches.

System-level career pathways meet the components of the WIOA definition by addressing the six career pathway elements to reduce barriers and create opportunities for individuals to advance within specific fields or areas of concentration, for example, cybersecurity. Individual-level career pathways efforts are initiatives that provide specific approaches to one or more, but not all, of the WIOA-defined career pathway elements. For example, an individual-level career program might include an intervention that makes it easier for a targeted stakeholder group to earn industry-recognized credentials. However, other components that are defined by the WIOA definition (i.e., helping that same individual to enter or advance into the workforce) may not be addressed.

Each step on a pathway prepares the individual to progress to the next level of employment and/or education, enabling an individual to gain new skills or achieve higher-level skills that are evidenced through recognized credentials, which in turn can help the individual to achieve better jobs, often with higher pay. Figure 2 provides the Department of Labor Career Pathways commissioned schematic (AQCP, 2014). It should be emphasized that there are numerous opportunities for individuals to enter and exit a career pathway system, including offering both horizontal and lateral movement within the system, to and from other disciplines, among numerous other possibilities.

> ***A career pathway is not a linear progression; but includes multiple entry and exit points at various levels enabling individuals to build their skills as they progress along a continuum of education, training, and advance in sector-specific employment.***

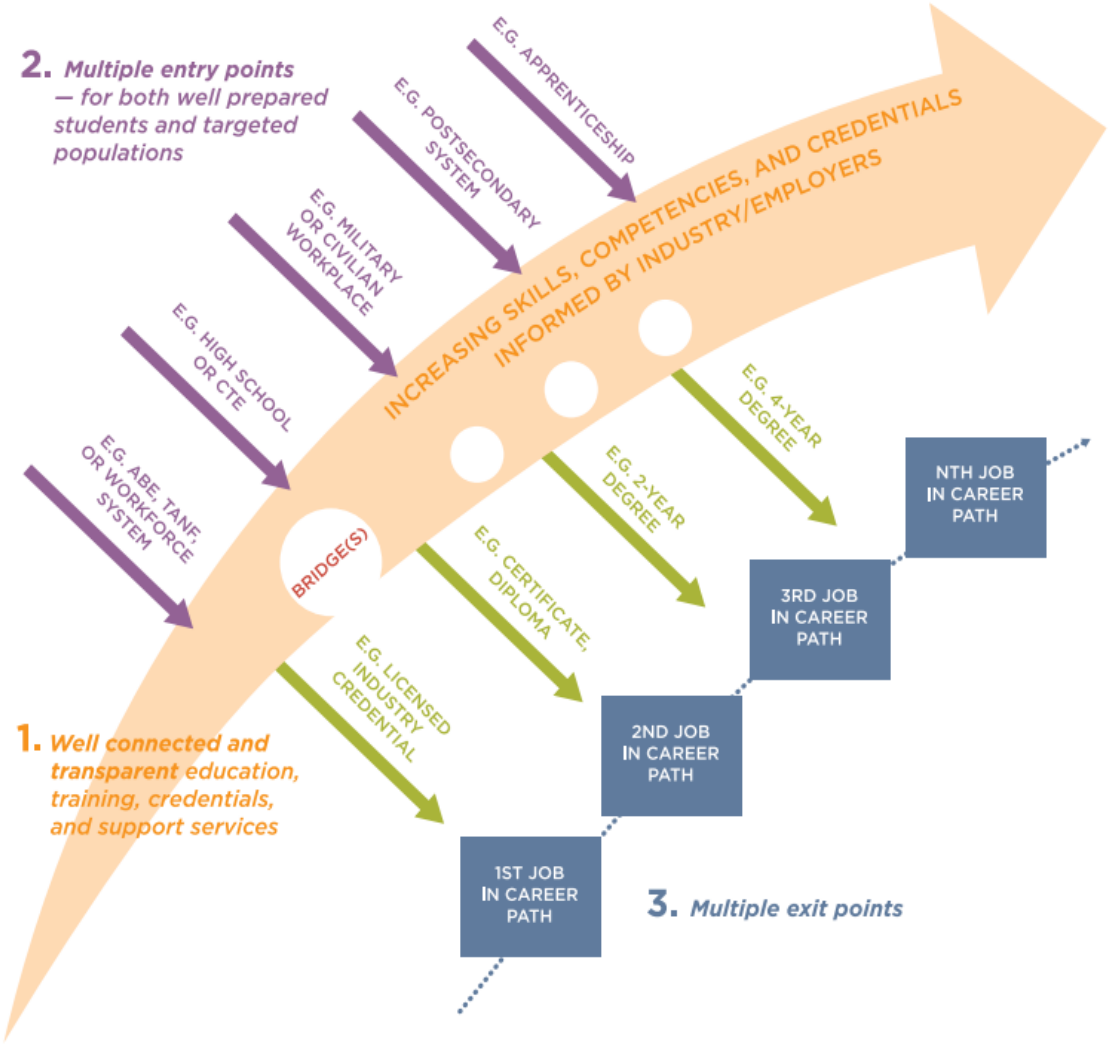


FIGURE 2: SHARED VISION, STRONG SYSTEMS: THE ALLIANCE FOR QUALITY CAREER PATHWAYS FRAMEWORK VERSION 1.0. CENTER FOR LAW AND CENTER FOR LAW AND SOCIAL POLICY, JUNE 2014 FOR DEPARTMENT OF LABOR

One steadfast rule is that Career Pathways target jobs important to local industries and aim to develop strong relationships with employers.

What is Cybersecurity Work?

General Definition

Digital technologies have grown exponentially. The acceleration of technical progress in the digital era has made the use of devices and applications employing cloud computing, big data analysis, blockchains, and artificial intelligence routine. The adoption and integration of advanced digital technologies such as 5G mobile networks, the Internet of things (IoT), cloud computing, quantum, robotics, etc., have created a strong demand for workers who are capable of designing, developing, implementing, and maintaining defensive and offensive cybersecurity strategies. However, the convergence of dynamic and interconnected technologies can be complex. Both this complexity and the varying and at times conflicting language often makes it difficult to clearly describe the work needed in this quickly evolving field.

> **Cybersecurity work is not a monolithic entity. Convergence of technologies has made describing cybersecurity work and those who perform it a challenge.**

The term "cyber," usually refers to or is appended onto things that have a relationship with modern technology, "referring to both information and communications networks."[xvi] The term "cyberspace," for example, refers to a virtual space denoting connections between computers and the networks, devices, data, control systems, etc. that reside or can be reached in that space.[xvii] Cybersecurity refers to protecting cyberspace and physical items that have a computational component that could be affected adversely, such as defense systems, cars, medical devices, and manufacturing systems.[xviii] The cybersecurity workforce includes not only technically focused staff or those who are fully embedded in the cybersecurity domain, but all those who have cybersecurity responsibility when preparing their organization to successfully implement its mission.

The NICE Framework provides a common language that describes cybersecurity work and the individuals who carry out that work. It can be applied during education, training, recruitment, hiring, development, and retention processes. As such, it supports the development of a rigorous cybersecurity career pathways based on industry needs.

Throughout the NICE Framework, those performing cybersecurity work—including students, job seekers, and employees—are referenced as Learners. This approach supports the cybersecurity career pathway approach, which emphasizes continually learning and achieving objectives

throughout. NICE recognizes that those performing cybersecurity work are lifelong learners who address cybersecurity implications across many domains. The standard structure and language it provides helps learners to explore cybersecurity work and to engage in appropriate learning activities to develop their knowledge and skills.

Figure 3 depicts a high-level view of the NICE Framework. The main building blocks of the NICE Framework are *Tasks*, *Knowledge*, and *Skills* (TKS) statements. The *Task* statements describe the cybersecurity work to be performed, and the Knowledge and Skill statements describe what an individual or team needs to know or be able to do to complete that work.

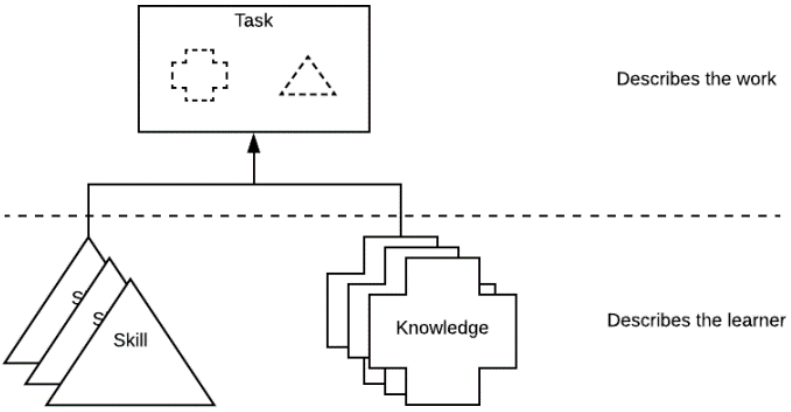


FIGURE 3: NICE FRAMEWORK BUILDING BLOCKS APPROACH

Work is what an organization needs to achieve cybersecurity risk management objectives. Every organization executes common tasks as well as some context-unique tasks. For example, every organization has some form of management tasks, whereas only some organizations have tasks to "deploy bulk energy systems securely." The NICE Framework provides organizations a way to describe their work through *Task* statements that group supporting *Knowledge* and *Skill* statements.

The *learner* can be a student, job seeker, employee, or other person within the workforce, who is acquiring or has knowledge and skills. In an organizational context, learners execute tasks. In an educational context, learners acquire new knowledge and skills. All individuals are considered learners due to education or training they received prior to entering the workforce and ongoing training or self-learning done throughout their lifelong career pathway journey.

Task statements describe the work to be completed; they represent a collection of associated concepts and actions defined by *Knowledge* and *Skill* statements. A *Task* can be defined as an activity that is directed toward the achievement of organizational objectives, including business objectives, technology objectives, or mission objectives. i.e., troubleshoot system hardware and software.

Knowledge statements are defined as a retrievable set of concepts within a learner's memory- that is, what a learner knows. *Knowledge* statements may describe either foundational (i.e., knowledge of cyber threats and vulnerabilities) or specific concepts (i.e., Knowledge of vulnerability information

dissemination sources, e.g., alerts, advisories, errata, and bulletins). Multiple *Knowledge* statements may be needed to complete a given *Task*, or one *Knowledge* statement may be used to complete many different *Tasks*.

Skill statements describe what the learner can do. *Skills* are defined as the capacity to perform an observable action. A learner who is not able to demonstrate the described skill would not be able to complete the *Task* that relies on that skill (i.e, Skill in integrating black box security testing tools into quality assurance process of software releases). Multiple *Skill* statements may be needed to complete a given *Task.* Likewise, exercising a *Skill* may be used to complete more than one *Task*.

NICE Framework *Competency Areas* are clusters of related *Knowledge* and *Skill* statements that correlates with one's capability to perform *Tasks* in a particular domain. *Competency Areas* (Figure 4) can help learners discover areas of interest, inform career planning and development, identify gaps for knowledge and skills development, and provide a means of assessing or demonstrating a learner's capabilities in the domain. *Competency Areas* are employer-driven and therefore enable education and training providers to be responsive to employer or sector needs by developing learning experiences that help learners develop and demonstrate the capability in the defined competency areas.

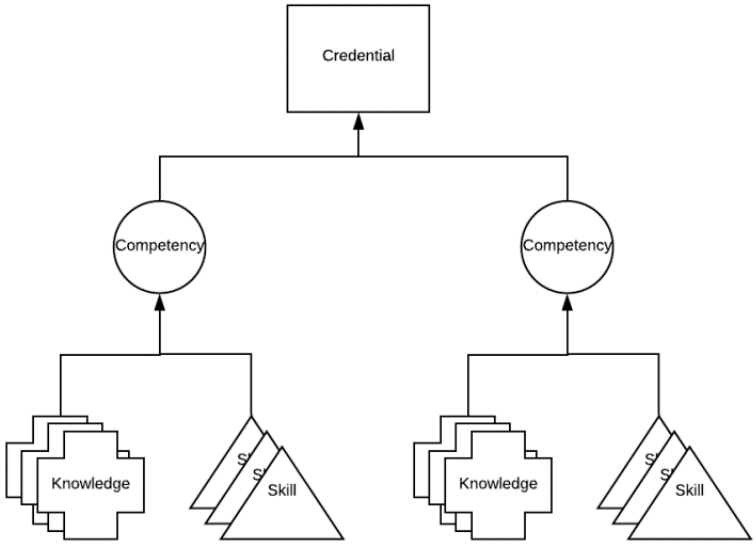


FIGURE 4: USING COMPETENCIES TO ASSESS LEARNERS THROUGH A CREDENTIAL

Work Roles are a way of describing a grouping of work for which an individual or team is responsible or accountable. *Work Roles* are not synonymous with "jobs" or "job titles." A *Work Role* is defined by a group of *Tasks,* whereas a job is a specific instance of employment, characterized by a set of responsibilities based on *Work Roles* within an occupation as defined by an employer. However, some *Work Roles* may coincide with a job title depending on an organization's use of job titles (e.g., Program Manager, Enterprise Architect, Software Developer, or Data Analyst). Additionally, *Work Roles* are not synonymous with "occupations," which may also be known as professions, trades, or career fields (e.g., Chemical Engineer or Database Architects).[xix] A single *Work Role* (e.g., Software Development or Cyber Policy and Strategy Planning) may apply to a variety of job titles (e.g., software engineer, coder, application developer). Conversely, multiple *Work Roles* could be combined to create a particular job. Indeed, a person in a large business may be asked to perform one or two

cybersecurity *Work Roles,* while another person, with the same job title at a small business could be responsible for three or more *Work Roles*. Employers in the state, regional, and local economies should determine the NICE Framework *Competency Areas* and *Work Roles* they need and what cybersecurity career pathways can help meet those employee's needs.

Multiple Opportunities

Cybersecurity is dynamic in nature and integrates and applies concepts from a wide variety of disciplines and draws on a broad and expanding portfolio of technical, as well as professional skills such as oral and written communication, teamwork, problem-solving, leadership, and business acumen and entrepreneurship. Cybersecurity workers use their knowledge and skills in a wide variety of occupations and across multiple industry sectors.

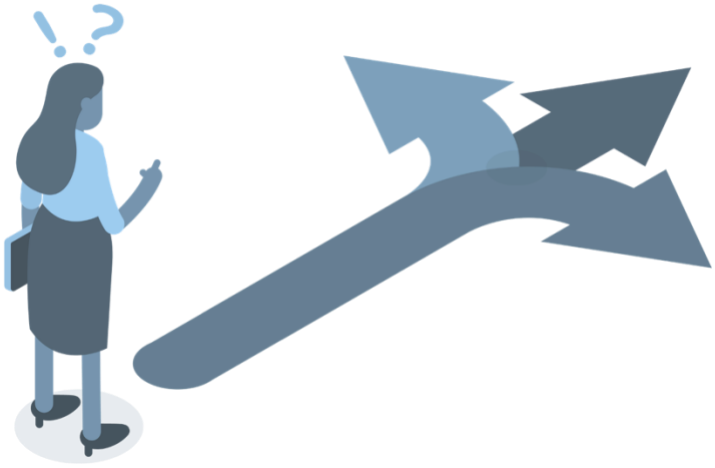
As additional businesses and households connect more devices to the Internet, more data will be gathered, which will need to be secured. This will drive the need for more developers, technicians, network specialists, and data analysts with cybersecurity skills. This is true across multiple industries, as well, in areas such as health care and the financial sector. There will also be a growing need for "cybersecurity-proximate" or "cybersecurity-hybrid" expertise in areas such as cybersecurity policy and legal services, project and program managers, and instructors, all of which require capabilities in one or more NICE Framework *Work Roles*.

As the demand for workers in all fields and industry sectors requiring varying degrees of cybersecurity expertise, it is critical to not think of career pathways as a linear progression to a specific work role or job as an end project. Instead, cybersecurity career pathways highlight the multiple opportunities available that connect with cybersecurity at various stages.

Multiple Entry and Exit Points

The perception of cybersecurity work often focuses on the predominance of the technical perspective. Even if the cybersecurity workforce seems monolithic and impenetrable for an outsider, there are countless opportunities for a multitude of talents and numerous ways for individuals to gain knowledge, skills, and experience that will help them enter and grow within the cybersecurity workforce. Fortunately, there is an increasing acknowledgment of the importance of both technical and non-technical activities and human interactions in cybersecurity. There are many ways individuals enter into the cybersecurity workforce and many ways to gain experience and demonstrate competencies within it. This is often referred to as the cybersecurity career "superhighway," with "multiple on and off-ramps." Some people are exposed to cybersecurity curriculum and instruction at an early age and pursue programs and jobs within the cybersecurity industry directly. Other people follow a more idiosyncratic path that is responsive to specific opportunities they encounter with a variety of twists, pauses, and turns. Still, others may pursue careers outside of cybersecurity and later discover that many of the capabilities they have developed transfer back into a cybersecurity career. Many people get started in a cybersecurity career serendipitously based on informal suggestions

from others in their social network. These examples illustrate some of the challenges of identifying the plethora of ways that individuals' cybersecurity learning and career pathways could align with the NICE Framework *Work Roles* and *Competencies.*



A recent project by the NICE Career Pathways Working Group curated a sample of Career Pathway "entry points."[xx] The discussion that follows highlights some of the working group's findings. It is not meant to be exhaustive, but to illustrate the wide range of possibilities and variations.

Entry Options from Secondary School

Authority to regulate education resides constitutionally with individual states, with limited direct authority of the U.S. Congress and the federal U.S. Department of Education. Recent widespread adoption of the Common Core state standards, Next Generation Science Standards are designed to set high expectations for critical thinking, problem-solving, and collaborative skills across a range of academic subjects - and other similar standards in English language arts and mathematics has sparked a rigorous conversation about how to identify the knowledge, skills, and discipline dispositions of high school graduates who are prepared for postsecondary success -whether directly into a career or pursuing additional educational endeavors. In addition, most states have created a set of academic expectations for college and career readiness to reinforce these goals. All combined, high school learners in the U.S. have access to multiple diploma options: general diplomas, specialized diplomas, 2+2 and 2+2+2 diplomas, and GEDs.

The general diploma usually found in a comprehensive high school setting[xxi] is the most common type, but even with this type of diploma there are different options available to students. A student within a comprehensive track may select STEM-related coursework or more advanced classes. At times these are recognized in the diploma, with some local school districts designating honors or specialty area (STEM) diplomas. School districts may also offer career and technical education (CTE), at times including specialization in cybersecurity or in one of the other Information Technology career cluster possibilities (e.g., web design, networking, support IT services). Some school districts also offer alternative routes including Career Academies,[xxii] P-TECH[xxiii], and Early College Programs.[xxiv] There are also a growing number of Youth Apprenticeship programs.[xxv] As found in footnotes, there are many that have centered around cybersecurity. One size does not fit all. Collectively the variety of programs represents a broad range of options. Some of the programs are described as "2 + 2." These can lead to a student graduating with both a high school diploma and an associate degree credential.

Another pathway option is described as a "2+2+2." This pathway includes the last two years of high school coordinated with two years at the Community or Technical College level and further coordinated with the final two years of bachelor's degree program. Some 2+2+2 programs are local or regional while others are statewide. These alternative programs focus on providing opportunities for high school students to take college-level coursework to get a head start on earning college credits while continuing to fulfill high school graduation requirements. Some offer articulated college credit while others might offer dual or transcripted credit.[xxvi]

A graduate equivalency degree (GED) is yet another point of entry into a cybersecurity career pathway. Credentials in the form of high school diplomas and college credit vary greatly from state to state and school district to school district.

In addition to courses of study at the secondary level, industry has recognized the need for developing its own workforce early and has designed a wide range of work-based options for high school students. For example, Northrop Grumman Corporation offers internship opportunities starting in high school and continuing through college. Successful students return each summer and begin full-time after graduation from college. Their experience often translates to higher entry pay or level, as well as counting toward their seniority for benefits.

Traditional Postsecondary Educational Entry Options

Providing all the postsecondary experiences that provide the backdrop for entry points in a cybersecurity career pathway is beyond the scope of this report. Previously, the commonly held belief was for a cybersecurity worker candidate to hold a bachelor's degree, preferably in computer science, engineering, or a cybersecurity-related or STEM program area. However, successful cybersecurity professionals have come from a wide range of backgrounds, both technical and non-technical and STEM and liberal arts related associate and bachelor's degrees. Some baccalaureate options come with minors or specializations in cybersecurity or cybersecurity-related credentials.

In addition, there is an increasing number of associate degree possibilities from community and technical colleges. Options include cybersecurity associate degrees, cybersecurity-related or STEM associate degrees, and non-STEM-related associate degrees. These can be either an Associate of Science (AS) or an Associate of Applied Science (AAS) degree.[xxvii] There are also a growing number of Bachelor of Applied Science (BAS) degrees offered by both two[xxviii] and four-year institutions.[xxix]

Some newer approaches, beyond the traditional degree program, also exist. An increasing number of higher education entities are providing stackable certificates, what the U.S. Department of Labor calls a "sequence of credentials that can be accumulated over time to build up an individual's qualifications."[xxx] Horizontal, vertical, and value-added are the three most recognized ways of

stacking credentials. Vertical stacking is the traditional method of adding one degree onto another in a hierarchy.

Horizontal stacking of credentials deepens knowledge in a specific field. Instead of attending a degree program that may take years to complete, students can complete a series of stackable certificates horizontally across their area of interest to broaden their skills. Merging vertical and horizontal stacking, known as "value-added stacking", combines a degree with a certification to qualify for a specific job. For example, adding a certificate in project management to a baccalaureate degree can help a person move into a more managerial role.

Once an associate or bachelor's degree is earned, a learner may also decide to continue their formal learning in post-graduate degree programs. Master's and doctoral degree programs are available from a wide range of departments and can be valuable way to increase knowledge in skills relevant to cybersecurity in areas such as computer science, engineering, business, public policy, information sciences, communication, criminal justice, psychology, and an increasing number of interdisplinary opportunities.[xxxi]

Finally, another effective post-secondary approach into cybersecurity is via the military. Individuals who choose to serve in the military have many opportunities in cybersecurity, not all of which require previous experience. Many corporations have programs recognizing the value of military training and have partnerships with the military to help these individuals transition from military to contractor when they separate from the service.

Alternative Entry and Re-Entry Options

There are a wide variety of alternative opportunities to enter or advance in cybersecurity. There are pre-apprenticeship programs that have a documented partnership with an employer and are designed to prepare individuals to enter and succeed in a registered apprenticeship or non-registered apprenticeship program that is not listed with the U.S. Department of Labor but meet some or all registered apprenticeship criteria other than the official application. There are a range of apprenticeship models that can be part of a cybersecurity career pathway. There are the Registered Apprenticeship Programs (RAP) with the U.S. Department of Labor that meet the standards and components defined by USDOL. There are also Industry-Recognized Apprenticeship Programs (IRAP) that are high-quality, customizable models of apprenticeship that adhere to recognized standards and have been validated by the Department of Labor.[1]

Additional entry and re-entry points in the career pathway journey provide opportunities for those that are already in the workforce and have decided to gain technical skills to reskill or upskill. These

[1] See https://www.apprenticeship.gov for more information and details.

options are also helpful for previous incarcerated individuals and justice-impacted, reentry, and recovery populations. There are both non-technical reskilling and upskilling options. Someone might be in a technical role but not involved with cybersecurity. Through technical upskilling they may create an entry way into the cybersecurity workforce. Others, through reskilling, might transfer or move into the cybersecurity workforce. Still, others who are already in the cybersecurity workforce might select technical or non- technical upskilling options through self-learning MOOCs, certificate, or boot camp training, or take advantage of the wide range of industry certification options to get additional skills that will allow them to advance in their career.

The NICE Career Discovery and Transform Learning working groups and the Midwest Credential Transparency Alliance (MCTA) conducted an environmental scan of existing cybersecurity credentials, using the NICE Transform Learning working group's definition of credentials and the Credential Transparency Description Language (CTDL) schema. Overall, the team identified an estimated 2,251 cybersecurity-focused credentials (Table 1). This estimate is primarily composed of enumerated lists of different types of cybersecurity credentials, including certifications, associate degrees, bachelor's degrees, master's degrees and doctoral degrees, certificates, micro-credentials, apprenticeship certificates, and led with an estimate using prior national research. Specific credentials were identified from multiple public data sources and nominations from project team members.

TABLE 1: OVERALL 2022 COUNT OF CYBERSECURITY CREDENTIALS

Credential Type	Method	Data Source	Count
Certification	Enumeration	Midwest state lists + DoD Approved 8570 Baseline Certifications + PaulJerimy.com	613
Associate degree	Enumeration	Cyberseek	251
Bachelor's degree	Enumeration	Cyberseek	260
Master's degree and Doctoral degree	Enumeration	Cyberseek	190
Certificate (Career Training)	Enumeration	Cyberseek	373
Micro-Credential (Grad cert)	Enumeration	Cyberseek	12
Apprenticeship Certificate	Enumeration	RAPIDS	88
License	Enumeration	CareerOneStop	0

Badge	Estimation	% based on Counting Credentials 2021	464
Total			2,251

Certifications had the greatest number of credentials identified corresponding to the importance of a highly qualified cybersecurity workforce and the pace of significant changes. A small number of certifications were referenced by multiple state agencies and/or education providers (See Appendix A). Conversely, many certifications (n=430) were referenced by only one organization. The project team also found that 38 of the certifications referenced by state agencies or credentials organizations were now deprecated. Additional information about the alignment of these certifications to the workforce needs would provide a more useful evaluation relative to the nation's cybersecurity workforce needs.

Some companies are providing in-house training, and both permanent and temporary rotation programs to help their employees negotiate the reskilling and upskilling landscape internally and grow their skills and take on new challenges without having to leave the company.[xxxii] IBM cultivates talent through a "new collar" approach that involves tapping professionals who may not have a traditional college degree but do have the needed technical skills and aptitudes.

Another industry approach is to offer on the job training to employees. This could range from required annual training for all employees to targeted training to expand the number employees knowledgeable on a specific skill. Technical mentorships provide a way to have senior employees give career advice and help more junior employees identify the training they need to advance their own career, and what opportunities might be available for them to grow. Another way to find opportunities is through internal job boards. Alternatively, short-term needs are often posted to a target community. For example, AT&T's The Opportunity Marketplace (TOM) application enables all management employees at AT&T to post "classifieds" offering or requesting help. This facilitates employees connecting with each other to find mentors, job shadowing, expert advice, or project help with over 70% of opportunities posted (not all cyber postings) receiving at least one interested candidate. This is an excellent tool for connecting beginners to experts, no matter where they are in the company. The platform has been successful and is now in staging with plans to launch a private community specifically for Cybersecurity@Work (an Employee Network) that focuses on professional growth, growing the talent pipeline, and encourages and facilitates the recruitment, development, advancement, and retention in cybersecurity by providing mentoring, education, and networking opportunities.

Building a stronger cybersecurity workforce can be supported by these activities as the skills of people in these work roles can be shared with other employees who are looking for new challenges. These employer practices can help individuals gain work experience and opportunities in cybersecurity without having to look externally. This company-supported and directed training can

help funnel their employees to their area of greatest need, increase employee satisfaction, and reduce attrition. More research is needed to understand the prevalence of these practices and the success of meeting their goals. For example, do employees once they have these new skills remain in their current company, or do they take their new skills to obtain employment elsewhere?

As described in this section, there are a large number of different ways to move into cybersecurity; straight from high school or college, through certificates, the military, and up-skilling and re-skilling to name just a few. The journey is not a linear one; having multiple entry exit, reentry, and even internal learning options to advance a career. Given the growth in the need for cybersecurity professionals, all these paths are necessary as one single path is insufficient. In fact, throughout their career, individuals usually take advantage of multiple training opportunities as they traverse the opportunities that are presented to them.

DISCUSSION

The following discussion is meant to clarify how a successful cybersecurity career pathway—often comprised of one or more career pathway programs—should operate. This guidance also addresses the career pathway system, which sets the policies and procedures that shape career pathways and can assist with strong pathway development and sustainability. A-G represent elements of the WIOA Career Pathways definition, with added guidance to clarify and provide additional detail for each element.

(A) Aligns with the skill needs of industries in the economy of the State or regional economy involved; Cybersecurity career pathways should:

- Use labor market data, informed by state, regional, and local employers, to design sector-focused programs that meet the needs of the employers in the state, regional, and local economies. The Cyberseek.org interactive heat map provides a granular snapshot of demand and supply data for cybersecurity jobs at the state and metro area levels and can be used to grasp the challenges and opportunities facing the local cybersecurity workforce. One size does not fit all.[xxxiii] Industry sector cybersecurity needs vary throughout the U.S.[xxxiv]
- Engage employers regularly and meaningfully at every stage of pathway development in an interactive, ongoing relationship and encourage employers to assume leadership roles.[xxxv]
- Identify the certifications, licenses, and industry-recognized credentials that state, regional, and local employers value or require and craft programs leading to them. The Cyberseek.org interactive heat map provides job opening certification requests.[xxxvi] However, local employers might have particular needs which should be taken into consideration.

(B) Prepares an individual to be successful in any of a full range of secondary or postsecondary education options, including apprenticeships registered under the National Apprenticeship Act;[xxxvii] Cybersecurity career pathways should:

- Enable lifelong learning that ensures youth and adult participants can gain entry to and advance, as desired, through successive education and training programs, leading to stackable credentials relevant to the specific occupation. [xxxviii] Options for multiple on and off ramps are needed. The NICE Framework *Competencies* and *Work Roles* can serve as a guide for employers, educators, and individual learners.
- Offer a range of education and training strategies to reach a wide range and more diverse set of individuals. These could include apprenticeships, contextualized instruction, integrated education and training, career ladders/lattices/roadmaps, curriculum built on industry competency strategies, stackable credentials, career navigation and support services.
- Ensure access and appropriate services for the targeted populations to widen the diversity of the workforce.

(C) Includes counseling or mentoring to support an individual in achieving the individual's education and career goals; Cybersecurity career pathways should:

- Ensure participants have access to career exploration, academic advising, support with transitions through the pathway, and comprehensive individualized support services, such as, but not limited to, childcare, transportation, and financial aid (where appropriate).
- Involve partnerships among K-12, postsecondary educational institutions, workforce training, development agencies, public and private employers, workforce boards, human services providers, and other partners to ensure participant access to the above services.
- Develop resources and offer training for career counselors and career navigators.
- Develop resources for learners and parents.
- Promote mentoring opportunities. A number of existing and successful cybersecurity mentoring programs should be highlighted.[xxxix]

(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.[xl] Cybersecurity career pathways should:

- Include cybersecurity career-focused instruction that integrates academic and technical content with foundational professional skills, considered necessary for success in education, training, career, and life.[xli] The NICE Framework can be used with the Federal Employability Skills which has been folded into the Department of Labor Competency Model.[xlii] [xliii]
- Offer opportunities for work-based learning experiences.[xliv] Examples include internships, job shadowing, service learning, paid work experience, project-based learning, on-the-job training, incumbent worker training, transitional jobs, and apprenticeships.
- Offer job placement assistant services that are tailored to participant needs at different points along the pathway.

(E) Organizes education, training, and other services to meet the needs of an individual in a manner that accelerates the educational and career advancement of the individual to the extent practicable; Cybersecurity career pathways should:

- Offer quality, non-duplicative training, coursework, assignments, and assessments to accelerate progress, maximize credit and credential attainment, and increase student success.[xlv] Align subject matter and curriculum to the NICE Framework *Competencies* to allow for greater vertical and horizontal content alignment.
- Promote strategies that allow learners to simultaneously pursue multiple steps along their career pathway to accelerate their progress while maintaining the quality and integrity of required learning. Successful proven strategies include flexible program design, workplace learning, credit for prior learning, and dual enrollment.

- Encourage concurrent enrollment, early college credit opportunities, and dual and transcripted credit that support progression through the cybersecurity career pathway.
- Offer participant-focused education and training that incorporates flexible class formats, locations, and times that make learning accessible and achievable for all populations.[xlvi] Strategies include, but are not limited to, modularized curriculum[xlvii], contextualized curriculum and instruction[xlviii], and virtual learning. Low and no-tech options or options for communities with limited internet access should also be explored.
- Encourage flexible and accessible education, training, and support services to forge advancement. Competency-based learning that is skills-based, self-paced, and personalized has proven to be a successful strategy.

(F) Enables an individual to attain a secondary school diploma or its recognized equivalent, and at least one recognized postsecondary credential; Cybersecurity career pathways should:

- Create partnerships between programs that serve youth and adults of all skill levels to ensure that participants can, in time, earn a recognized postsecondary credential, as desired.[xlix]
- Enable participants to gain entry to or advance within a given sector or occupational cluster, facilitate efficient transitions to continuing education, and incorporate stackable and portable industry-recognized credentials.
- Facilitate co-enrollment in programs administered by the core[l] and required[li] partners (as defined by WIOA), in addition to Supplemental Nutrition Assistance Program Employment & Training (SNAP E&T).

(G) Helps an individual enter or advance within a specific occupation or occupational cluster; Cybersecurity career pathways should:

- Involve partnerships with employers to support participants' educational and career advancement through on-the-job training, customized training, corporate training, incumbent worker training[lii], and other work-based training strategies.
- Reduce barriers to entry to ensure that participants with diverse backgrounds and experience can enroll and succeed in a pathway.
- Provide individuals with multiple entry points to accommodate academic readiness and multiple exit points to allow individuals to obtain employment and return to the program when they are ready to progress to the next level of credential attainment.

Career pathways enable those even without a high school diploma or its equivalent to attain one and give access to additional training and education opportunities that lead to additional credentials. Credentials, both academic and work-related, are important milestones for career pathways. Students can earn credentials that verify educational attainment and mastery of skills and

competency. For employers, credentials allow them to readily determine their competency needs and the competencies of a job applicant.

An effective and efficient cybersecurity career pathway will also commit to diversity, equity, inclusion, and accessibility for all participants. Collecting, sharing, and using evidence to identify and eliminate barriers to participant access and success is needed throughout the cybersecurity career pathway lifecycle. In addition, qualitative and quantitative evaluation of effectiveness in serving employers (the business community) should be shared to inform strategies for improvement.

RECOMMENDATIONS

All successful career pathways create a series of structured and connected education programs and support services that enable students, often while they are working, to advance over time to better jobs and higher levels of career advancement.[liii] Each step on a career pathway is designed explicitly to prepare students to progress to the next level of employment and/or education. Career pathways target jobs in industries of importance like cybersecurity, to local and regional economies. They are designed to create avenues of advancement for the underemployed, the unemployed, incumbent workers, new and future labor market entrants, and to produce a steady supply of qualified workers for employers. Career pathway certificates and degrees are carefully aligned to skill sets needed in a given industry or occupational sector and have relevance, credence, and currency with employers. Ideally, career pathways are designed to maximize student flow and accomplishment—so that credits are portable; credentials are stackable; and students who need to are able to step in and out of college, as well as employment, building as they go.

The following actions, to be led by the NICE Program Office in coordination with the NICE community, are recommended:

- **Curation and maintenance of cybersecurity career pathways tools, programs, and systems:** The NICE Career Discovery Working Group will establish a Project Team for NICE Strategic Plan Goal 1: Promote the Discovery of Cybersecurity Careers and Multiple Pathways, Objective 2: Increase understanding of multiple learning pathways and credentials that lead to careers that are identified in the Workforce Framework for Cybersecurity (NICE Framework). Specifically, curation and maintenance of cybersecurity career pathways tools, programs, and systems (see sample in Appendix B) will address Strategy 2.1: Identify and track multiple learning pathways and credentials aligned to NICE Framework Work Roles and Competencies and Strategy 2.2: Identify and develop tools and resources that promote learning pathways and credentials aligned to NICE Framework *Work Roles* and *Competencies.* This will provide the needed scaffolding to address Strategy 2.4: Collaborate and support the alignment of the NICE Framework *Work Roles* and *Competencies* with career tools and resources.
- **Develop Cybersecurity Career Pathway graphic or infographic and interactive tool:** The NICE Career Discovery Working Group will establish a Project Team in coordination with the other NICE Community Coordinating Council members for NICE Strategic Plan Goal 1: Promote the Discovery of Cybersecurity Careers and Multiple Pathways, Objective 2: Increase understanding of multiple learning pathways and credentials that lead to careers that are identified in the Workforce Framework for Cybersecurity (NICE Framework) to develop a Cybersecurity Career Pathway graphic or infographic (Phase 1) and an interactive tool (Phase 2) that highlights the multiple entry, exit, and reentry possibilities, the multiple opportunities across numerous industry sectors, the multiple credentials, and highlights the focus on *Competencies* which make up the NICE Cybersecurity *Work Roles*.

- **Encourage the NICE Framework OLIR and JSON Application:** The Online Informative Reference (OLIR) Program, managed by NIST, provides a process for aligning references to NIST documents. Additionally, the program provides a catalog of those references. NICE should continue to work with the Online Informative Reference (OLIR) Program to develop templates and other resources for NICE Framework mappings. NICE should continue to work on cross alignment of the NICE Framework with other Frameworks (e.g., Privacy, NIST Cybersecurity Framework, AI, Quantum) through the proposed JSON format allowing easier cross collaboration to highlight synergy between multiple career pathways.
- **Provide Cybersecurity Career Pathways Examples:** In partnership with the Federal Career Pathways IWG develop or highlight existing Cybersecurity Career Pathways that can be added to the Career Pathways Resource Center. All Cybersecurity Career Pathways should follow the WIOA Career Pathway definition, align to the NICE Framework, and provide possible cross mapping or connections with the Bureau of Labor Statistics, U.S. Department of Labor, Outlook Handbook, and 2021 Edition and the U.S. Office of Personnel Management's Handbook of Occupational Groups and Families.
- **Support Regional Career Pathway Partnerships:** Encourage effective local or regional multistakeholder workforce partnerships to develop cybersecurity career pathways to support local economic development to stimulate job growth. Cybersecurity Career Pathways should align with the WIOA definition of Career Pathways, address the key elements, and align with the NICE Framework.
- **Promote Coordination:** Informed by the proven career pathway systems perspective, stakeholders in the nation's cybersecurity education and workforce ecosystem should work together to develop, research, evaluate, and coordinate mutually reinforcing initiatives that produce a significant, positive, and collective impact on the cybersecurity workforce challenge rather than pursuing numerous individual, discrete, largely disconnected, and low-impact initiatives.
- **Increase Research Data:** NICE working with researchers and policy stakeholders should establish a better empirical foundation for research on the educational and career paths of cybersecurity workers for the purpose of building a robust evidence base to inform policy. For example, identifying resources to collect and integrate longitudinal administrative records from university transcript data and data from statistical agencies, using data for characterizing student educational pathways (including student retention in higher education and workforce), employment choices, earnings and employment dynamics would provide valuable information to help address the state of the cybersecurity workforce.

REFERENCES

Alliance for Quality Career Pathways (2014). Shared vision, strong systems: The alliance for quality career pathways framework version 1.0. Washington, D.C.: The Center for Law and Social Policy.

Burning Glass Technologies, (2020). Protecting the future: The fastest-growing cybersecurity skills. Boston, MA: Burning Glass Technologies. https://www.burning-glass.com/wp-content/uploads/2020/10/Fastest_Growing_Cybersecurity_Skills_Report.pdf

Carnevale, A., Jayasundera, T., & Gulish, A. (2016). America's divided recovery: College haves and have-nots. Washington, D.C: Georgetown University Center on Education and the Workforce. https://files.eric.ed.gov/fulltext/ED574377.pdf

Cyberseek. Hack the gap: Close the cybersecurity talent gap with interactive tools and data. Retrieved May 1, 2022, from https://www.cyberseek.org/heatmap.html

Dann-Messier, B., Oates. J., & Sheldon, G. (2012). Joint commitment letter from U.S. Departments of Education, Health and Human Services, and Labor. Available at: http://cte.ed.gov/docs/RPOS_2012/Joint_Letter_Career_Pathways.pdf

Hendra, R., Greenberg, D. H., Hamilton, G., Oppenheim, A. Pennington, A. Schaberg, K., and Tessler, B. L. (2016). Encouraging evidence on a sector-focused advancement strategy. New York: MDRC. https://clear.dol.gov/Study/Encouraging-evidence-sector-focused-advancement-strategy-Hendra-et-al-2016-2

Sarna, M., Schwartz, D., Strawn J., (2018). Career pathways research and evaluation synthesis: Career pathways design study (U.S. Department of Labor Report DOLQ129633231). Bethesda, MD: Abt Associates.

APPENDICES

Appendix A: Cybersecurity Certifications Referenced by Five or More Organizations

Organization	Certification	URL
(ISC)²	(ISC)2 Certified Information Systems Security Professional (CISSP)	https://www.isc2.org/Certifications/CISSP
Cisco	Cisco Certified Network Associate (CCNA)	https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna.html
Cisco	Cisco Certified Network Associate Cybersecurity Operations (CCNA Cyber Ops)	https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/cyberops-associate.html
CompTIA	CompTIA Security+	https://www.comptia.org/certifications/security
ISACA	ISACA Certified Information Security Manager (CISM)	https://www.isaca.org/credentialing/cism
CompTIA	CompTIA A+	https://www.comptia.org/training/by-certification/a
Cisco	Cisco Certified Internetwork Expert Security (CCIE Security)	https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/expert/ccie-security-v2.html
Cisco	Cisco Certified Professional Security (CCNP Security)	https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/professional/ccnp-security-v2.html
EC-Council	Certified Ethical Hacker (CEH)	https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/
GIAC	GIAC Certified Incident Handler	https://www.giac.org/certification/gcih
ISACA	ISACA Certified Information Systems Auditor (CISA)	https://www.isaca.org/credentialing/cisa
CompTIA	CompTIA Cloud+	https://www.comptia.org/certifications/cloud
CompTIA	CompTIA Advanced Security Practitioner + (CASP+)	https://www.comptia.org/certifications/comptia-advanced-security-practitioner
CompTIA	CompTIA CySA+	https://www.comptia.org/certifications/cybersecurity-analyst
CompTIA	CompTIA Network+	https://www.comptia.org/certifications/network
CompTIA	CompTIA Server +	https://www.comptia.org/certifications/server

The NICE Career Pathways project team searched for detailed information about the alignment of identified credentials with the NICE Framework. Overall, few organizations provide detailed alignment information for their offered credentials to the public. The few examples discovered came from certification providers and were communicated to the public via pdf documents or formatted websites. CompTIA provides recommendations on their website for particular CompTIA certifications aligned to the NICE Framework's Specialty Areas. The EC-Council provides a detailed mapping document for the EC-Council certifications to the NICE Framework's categories, specialty areas, work roles, knowledge, skills, abilities, and tasks. In 2020, (ISC)² offered a request form to download (ISC)² Certification NICE Framework Map that claimed to contain alignments with the NICE Framework's Specialty Areas; Work Roles; Knowledge, Skills and Abilities; and Tasks, but this request form and the resource has been removed from their website.

Appendix B: Cybersecurity Career Pathway Tools, Programs, and Systems Examples

There are a wide range of cybersecurity career pathway resources developed to provide conceptual guidance on career pathways and credentials, all applicable to cybersecurity, some aligned to the NICE Framework and others that are not. Some would be defined as individual program initiative while others would meet the formal cybersecurity career pathway definition. Below provides a small sample of the resources discussed with public and private sector partners.

Federal Government Career Pathway Tools

Department of Labor Career Pathways Toolkit

The U.S. Department of Labor, Employment, and Training Administration of the U.S. Department of Labor, sponsors WorkforceGPS which hosts an online technical assistance website created to help build the capacity of America's public workforce investment system.[liv] The Careers Pathways Community resources are found on this website. The original Career Pathways Toolkit: A Guide for System Development has been updated and includes a wide variety of resources. Toolkit resources and templates continue to be updated to provide the workforce system with a framework, resources, and tools for States and local partners to develop, implement, and sustain career pathway systems. The toolkit acknowledges the WIOA definition and key components needed to create and sustain a demand-driven employment and training system as part of a larger national effort. It references the Department of Labor Career One Stop and the Department of Labor Competency Model as a building block for creating career pathway programs.[lv] [lvi] It references the Career One Stop credentials toolkit as an easy way to search existing industry-recognized credentials. Toolkit supplements are maintained to reflect new knowledge and lesson learned from career pathway research and address new focus areas such as sector strategies and Registered Apprenticeship.

Department of Education Programs of Study Design

The Department of Education Career Pathways Systems national initiative provides information about career pathways generally and strategies to support career and technical education students in acquiring the academic, employability, and technical skills that employers demand.[lvii] One entry point in the career pathway system is driven by the Carl D. Perkins Career and Technical Education Act (Perkins V) to promote career and technical education (CTE) programs of study (POS). The Perkins POS ten components' requirements include incorporating and aligning secondary and postsecondary education elements, including academic and career and technical education content in a coordinated, nonduplicative progression of courses, offering the opportunity for secondary students to acquire postsecondary credits, and leading to an industry-recognized credential or certificate at the post-secondary level, or an associate or baccalaureate degree. Formal CTE POS must address the ten components of the Department of Education Programs of Study Framework.[lviii]

The Federal Cyber Career Pathways Tool

The Cyber Career Pathways Tool is developed and maintained by the Federal Cyber Workforce Management and Coordination Working Group, tri-chaired by the Department of Defense, the Department of Veterans Affairs, and Cybersecurity and Infrastructure Security Agency (CISA).[lix] This tool presents an interactive way to explore an interpretation of the Workforce Framework for Cybersecurity (NICE Framework). It depicts the Federal "Cyber" Workforce according to five distinct skill communities. These are IT, Cybersecurity, Cyber Effects, Intel (Cyber) and Cross Functional. Intelligence is a separate and sixth community. The classification scheme differs from the seven NICE Framework Categories.[lx] The interface is comprehensive and allows drill down and comparison between the various work roles. An explanation of the classification scheme is found in a technical report. There is not an obvious mapping between the seven NICE Framework Categories and the distinct skill communities. In fact, defining one of the skill communities as cybersecurity has proven to be confusing to some, as all the work roles are defined by the NICE Framework to be supportive of cybersecurity work. In addition, NICE Framework Specialty Areas and Ability statements are used which are no longer in use. The updated NICE Framework and formatting will allow cross alignment with other NIST Frameworks (i.e., Privacy, NIST Cybersecurity Framework, AI, Quantum, etc) through the Online Informative Reference (OLIR) Program, managed by NIST. This update will include JSON format allowing easier cross collaboration with other frameworks following the NICE Framework structure. The Cyber Career Pathways Tool team should collaborate closer with the NIST NICE team to ensure future compatibility and accuracy, highlighting competencies and how an individual may be responsible for multiple work roles. This combination allows work to identify the totality of Knowledge, Skills, and Tasks, that combined define the work to be completed. The current version of the Cyber Career Pathways Tool allows quick access to the information for a specific work role. However, it is difficult to combine Tasks statements that help determine position descriptions that guide individuals on their career pathway journey.

The DoD Cyber Workforce Framework

Warfare has shifted its focus to cyberspace and the battlefield is becoming more important by the day. To keep up with this reality, DoD revamped DoD cybersecurity by issuing the DoD Cyber Workforce Framework (DCWF). This framework shifts the focus of DoD cybersecurity away from solely information assurance and more towards the personnel end of the DoD cyber workforce. The DoD Cyber Workforce Framework (DCWF), similar to the NICE Framework, establishes the DoD's lexicon based on the work an individual is performing, not their position titles, occupational series, or designator.[lxi] The DCWF describes the DoD work performed by the full spectrum of the "cyber" workforce as defined in DoD Directive (DoDD) 8140.01.[lxii] The DCWF leverages the original National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF) and the DoD Joint Cyberspace Training and Certification Standards (JCT&CS).[lxiii] To increase understanding and use of the DCWF, the DoD collaborated with DISA to create the DCWF Tool,[lxiv] an interactive online tool for stakeholders to identify, organize, and manage the tasks and KSAs of the cyberspace workforce in accordance with the DoD policy. The scheme presents each work role with the corresponding NICE Category and Specialty Area through five "Workforce Elements." These are IT

(Cyberspace), Cybersecurity, Cyberspace Effects, Intelligence (Cyberspace) and Cyberspace Enablers. The tool allows one to search by categories, the five workforce elements, work roles, and/or KSAT's. It is noted that updates to the tool need to occur to account to for the refresh of NICE Framework to ensure future compatibility and accuracy; highlighting competencies and how an individual may be responsible for multiple work roles. This combination allows work to identify the totality of Knowledge, Skills, and Tasks that combined define the work to be completed. The current version of the tool allows quick access to the information for a specific work role. However, the ability to combine Tasks statements or competencies that help determine position descriptions that guide individuals on their career pathway journey will be necessary moving forward.

MILGears Cyberspace IT/Cybersecurity Workforce Tool (CSWF)

The Cyberspace IT/Cybersecurity Workforce Tool (CSWF), part of the MILGears series, is based on the qualification matrices found on Navy COOL, which were developed to ensure that Sailors working in Cyber IT and Cybersecurity meet defined qualification requirements to serve in those roles.[lxv] The Department of Navy (DON) model is consistent with the DOD Cyber Workforce Framework (DCWF), both based on cybersecurity work roles outlined in the NICE Framework. There are two ways to explore. A person can view by work roles or through inputting unique credentials and exploring recommended Cyber IT/CSWF roles and their required qualifications.

Private Sector Career Pathway Tools

Cyberseek Cybersecurity Career Pathway

CyberSeek is an interactive tool that provides visualization of the need for and the supply of cybersecurity workers across the country.[lxvi] CyberSeek has been developed by Burning Glass Technologies and CompTIA in partnership with NICE. CyberSeek's interactive heat map provides data at the national, state, and local levels, in both the private and public sectors in nineteen different industries. The site also includes an interactive Cybersecurity Career Pathway tool that helps identify key jobs within cybersecurity; detailing information about the salaries, common transition opportunities, credentials, and skillsets associated with each role; and common career advancement opportunities. CyberSeek's career information is aligned with the NICE Framework. The tool provides data to help employers, job seekers, policy makers, training providers, and educators and guidance counselors meet today's increasing demand.

ISSA Cybersecurity Career Lifecycle (CSCL)

The Information Systems Security Association (ISSA) has developed a Cybersecurity Career Lifecycle Tool based on a cumulative knowledge model, where individuals establish a foundational knowledge that is demonstrated by a degree and/or a security certification.[lxvii] The Career Lifecycle is divided into five stages with the opportunity for a variety of paths when within each level. The five stages are: Pre-professional (an individual who has not yet obtained a cybersecurity position), Entry level (1-5 years of experience), mid-level (5-7 years in an identified field), Senior level (7+ years in a respective

field), and Security leader (12+ years). The tool provides ISSA resources for each level and provides access to a search feature for job options aligned to each Lifecycle Level.

CompTIA Cybersecurity Career Pathway

CompTIA cybersecurity career pathway graphical tool and interactive option indicates the CompTIA certification options along a learning continuum depending on IT experience, existing certifications, or course of study.[lxviii] [lxix] The certification pathways include five options: Core, Infrastructure, Cybersecurity, Data and Analytics, and Professional. Core skills include the foundation for a career in IT with our core skills certification that covers a broad spectrum of topics, including operating systems, networking, security and more. Certification core skills are covered in CompTIA ITF+, A+, Network+, and Security+. From the Core, an Infrastructure pathway could be added on with Server+, Linux+, and Cloud+ certifications. The Cybersecurity pathway pairs the Core and Instructure series with cybersecurity certifications to gain the hands-on ability to protect organizations from cyberattacks and threats. These include PENTEST+, CYSA+, and CASP+. The Data and Analytics pathway includes the DATA+ CompTIA certification. The Professional pathway supports areas like project management and training and includes the PROJECT+, Cloud Essentials+, and CTT+ certifications.

EDUCAUSE Information Security Pathway Toolkit

The EDUCAUSE Information Security Pathway Toolkit provides a way for individuals to identify strengths and gaps in skills, then select activities to leverage those areas and develop in select capacities.lxx The toolkit supports the development of an action to improve immediate performance and foster readiness for long-term professional goals. The tool was designed to help individuals identify and navigate an Information Security (IT) career by increasing their understanding of the knowledge, skills, and experiences needed to begin, transition, and advance in an IT career. Depending on the career stage of an individual (early career, mid-career, or late career), they select from five levels: Early (0-7 years), Mid-level (3-11 years), Advanced Level (7-19 years), Unit Executive Level (11-27 years), and Institutional Executive Level (19-50 years). The lexicon is based on a person's years of experience in information technology, provides sample job titles associated with each level, and organizes the "skills for success" in five areas: Lifelong Learning, Project Management and Strategy, Communication, Leadership, People, and Change Management, and Finance. Recommended education at all levels relies on degrees with additional certifications depending on career goals and institutional expectations.

SANS Cyber Security Skills Roadmap

The SANS Cyber Security Skills Roadmap presents both a graphic and interactive tool aligning "needed skills" with SANS course offerings.[lxxi] More than 60 SANS courses are offered to deliver critical skills in the cyber defense operations, digital forensics, cloud security, penetration testing, and management practice areas of cybersecurity. The roadmap begins with baseline skills or core techniques that

"every security professional should know," and continues to develop skills that focus on specific job roles (monitoring and detection, penetration testing, and incident response and threat hunting), and finally specificized roles (cyber defense operations, specialized penetration testing, threat intel and forensics, cloud security, industrial control systems, and advanced management).[lxxii]

SA2020 Talent Pipeline Task Force

SA2020 convened the Talent Pipeline Task Force to develop a plan to better connect education and training to the San Antonio workforce in targeted industries such as cybersecurity.[lxxiii] With support from Lumina Foundation, they partnered with the Chicago-based Council on Adult and Experiential Learning (CAEL) to develop a cybersecurity career pathway.[lxxiv] By matching education supply data and labor market needs supported by Community Information Now (CI:Now), CAEL and SA2020, a cybersecurity career pathway was designed from the ground up, with attention to foundational and essential skills at the entry level or "in the early stages of the ladder." They also offered multiple entry and exit points, with the intent being that those who seek skills and a job in a pathway can do so while intentionally climbing an explicit career ladder. Developer, Engineer/Architect, Consultant/Manager, and Industrial Networks/Control Systems Job Family schemes were created. All but Industrial Networks indicate a bachelor's degree was a required entry point.

Sample of State Examples

CTE State Options

AL: 2015 – 2016 Career Cluster Programs for Education and Training, Hospitality and Tourism, Human Services and FACS Middle School Program (alabamaachieves.org)
AR: ADE Announces Cyber Security Course Pathway (arkansas.gov)
GA: PowerPoint Presentation (gadoe.org) and GA Tech
VA: Search | Virginia Department of Education and VDOE :: Career & Technical Education - Program Administration and Management (virginia.gov) and Cyber Security Education (virginia.gov)
Program of Studies 2022-23 (yorkcountyschools.org)

Workforce Development State Pathways

AR: AR Career Pathways (arpathways.com)
CO: https://www.mycoloradojourney.com/journey/tools/careers
DE: Pathways Programs | Delaware Pathways
GA: Georgia Cyber Center WorkForces Program | GACC WorkForces | Home
MO: Missouri Career Pathways | Missouri Department of Elementary and Secondary Education (mo.gov)
PA: What does PAsmart mean to you?
TX: Statewide Program of Study: Cybersecurity; STEM Career Cluster (texas.gov)
VT: Vermont: Cybersecurity Career Pathway Framework | Agency of Education
WVA: MURC_WVCybersecurityWorkforce_Book_FINAL.pdf (techconnectwv.org)

Appendix C: Cybersecurity Guidance Regarding WIOA Career Pathways

The richness of the NICE Framework can be used to support multiple components of a cybersecurity career pathway definition.

WIOA Career Pathways Definition	
The term "career pathway'' means a combination of rigorous and high-quality education, training, and other services that–	• Explicit criteria for including components in a pathway • Pathway components are intentionally sequenced
WIOA Career Pathways	**NICE Guidance**
A. *aligns with the skill needs of industries in the economy of the State or regional economy involved;*	• The NICE Framework can help guide alignment to education, training, workforce development and credentials and industry sector alignment analysis
B. *prepares an individual to be successful in any of a full range of secondary or postsecondary education options, including apprenticeships registered under the Act of August 16, 1937 (commonly known as the ``National Apprenticeship Act''; 50 Stat. 664, chapter 663; 29 U.S.C. 50 et seq.) (referred to individually in this Act as an "apprenticeship'', except in section 171);*	• Career pathways and components should articulate alignment to the NICE Framework and with additional frameworks for transferability of skills (such as, the Connecting Credentials Framework, or the Degree Qualifications Profile) • Options for multiple on and off ramps are needed. The NICE Framework *Competencies* and *Work Roles* can serve as a guide for employers, educators, and individual learners. • The NICE Framework allows employers to determine or develop the competencies they need which can drive the development of an internal program. • The NICE Apprenticeship community of Interest hosts the cybersecurity apprenticeship tracker.[lxxv] • NICE supports and continues to advance the Cyberseek.org cybersecurity career pathway tool.[lxxvi] • The NICE Career Discovery Working group continues to promote the multiple career options and multiple entries to entering the workforce. • NICE hosts the National Cybersecurity Career Week that promotes awareness of the multiple career options.[lxxvii] • The components of a career pathways can articulate alignments to the NICE Framework to analyze the sufficiency of pathways for individuals.
C. *includes counseling to support an individual in achieving the individual's education and career goals; 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;*	• Resources developed for assessing, documenting, and appropriately sharing individuals' education and career goals should align with the NICE Framework. • Pathways include learning opportunities and work experience components aligned with explicit

	occupations and SOC codes which connect with NICE Framework. • NICE has and continues to develop resources for career counselors, hosts the National School Counselor Winners each year at the NICE K12 Cybersecurity Education Conference, and hosts a number of workshops to learn about the needs of school counselors and college navigators. • NICE working groups and Communities of Interest have recently launched a focus on development of a National Cybersecurity Apprenticeship Program and Cybersecurity Mentoring opportunities.
D. *includes, as appropriate, education offered concurrently with and in the same context as workforce preparation activities and training for a specific occupation or occupation cluster;*	• Advocate for work-based learning experiences. • Articulation agreements and transfer value profiles are consistently documented based on earned credentials and the NICE Framework competencies. • The NICE Framework can help guide alignment to education, training, workforce development and credentials and industry sector alignment analysis and reduce duplication.
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;*	• Support services for learner success are sufficiently documented and described. • The NICE "Transform Learning" working group project team is analyzing different schemas for representing the full range of credential offerings. • NICE Strategic Plan promotes research-based strategies that allow learners to accelerate their career advancement. • Competency-based learning that is skills-based, self-paced, and personalized has proven to be a successful strategy and is the underpinning of the NICE Framework.
F. *enables an individual to attain a secondary school diploma or its recognized equivalent, and at least 1 recognized postsecondary credential; and*	• Specific cybersecurity credentials or sets of credentials are included as pathway destinations. • Career pathway components can be explicit about their "on ramps" and "off ramps", such as admissions requirements and alignment with particular occupational frameworks. • Competencies are key elements with the NICE Framework which can drive the development of credentials, both academic and work-related, which are important milestones for career pathways.
G. helps an individual enter or advance within a specific occupation or occupational cluster.	• Career pathway components can be explicit about their "on ramps" and "off ramps", such as admissions requirements and alignment with particular occupational frameworks permitting

	interruptions without causing an individual to veer from an education or career path. This results in increased access to family-sustaining careers and career advancement over time.

Endnotes

i Sarna, M., Schwartz, D., Strawn J., (2018). Career pathways research and evaluation synthesis: Career pathways design study (U.S. Department of Labor Report DOLQ129633231). Bethesda, MD: Abt Associates.
ii Career Pathways Descriptive and Analytical Project | U.S. Department of Labor (dol.gov) https://www.dol.gov/agencies/oasp/evaluation/completedstudies/career-pathways-descriptive-and-analytical-project
iii NIST Measuring Cybersecurity Workforce Capabilities 7-25-22 https://www.nist.gov/system/files/documents/2022/08/03/NIST%20Measuring%20Cybersecurity%20Workforce%20Capabilities%207-25-22.pdf
iv Burning Glass Technologies, (2020). Protecting the future: The fastest-growing cybersecurity skills. Boston, MA: Burning Glass Technologies. https://www.burning-glass.com/wp-content/uploads/2020/10/Fastest_Growing_Cybersecurity_Skills_Report.pdf
v Cyberseek. Hack the gap: Close the cybersecurity talent gap with interactive tools and data. https://www.cyberseek.org/heatmap.html
vi Carnevale, A., Jayasundera, T., & Gulish, A. (2016). America's divided recovery: College haves and have-nots. Washington, D.C: Georgetown University Center on Education and the Workforce. https://files.eric.ed.gov/fulltext/ED574377.pdf
vii Hendra, R., Greenberg, D. H., Hamilton, G., Oppenheim, A. Pennington, A. Schaberg, K., and Tessler, B. L. (2016). Encouraging evidence on a sector-focused advancement strategy. New York: MDRC. https://clear.dol.gov/Study/Encouraging-evidence-sector-focused-advancement-strategy-Hendra-et-al-2016-2
viii See 2012 Dear Colleague memo defining Career Pathways and detailing the critical components Six Key Elements https://www2.ed.gov/about/offices/list/ovae/ten-attachment.pdf
ix Additional research findings can be found at Search, DRE, Employment & Training Administration (ETA) - U.S. Department of Labor (doleta.gov) https://wdr.doleta.gov/research/details.cfm?q=&id=2695 and Workforce GPA https://wdr.doleta.gov/research/details.cfm?q=&id=2695 and DOL EPA WIOA Workforce Innovation and Opportunity Act | U.S. Department of Labor (dol.gov) https://www.dol.gov/agencies/eta/wioa
x Dann-Messier, B., Oates. J., & Sheldon, G. (2012). Joint commitment letter from U.S. Departments of Education, Health and Human Services, and Labor. Available at: http://cte.ed.gov/docs/RPOS_2012/Joint_Letter_Career_Pathways.pdf
xi The 2014 WIOA replaced the Workforce Investment Act of 1998 and amended the Adult Educational and Family Literacy Act, the Wagner-Peyser Act, and the Rehabilitation Act of 1973.
xii See U.S. Department of Labor Employment and Training Administration Workforce Innovation and Opportunity Act website https://www.dol.gov/agencies/eta/wioa/
xiii The Workforce Innovation Technical Assistance Center (WINTAC) worked together with state agencies and partners to develop resources to effectively implement the requirements of WIOA. Workforce System | U.S. Department of Labor (dol.gov) https://www.dol.gov/agencies/odep/program-areas/workforce-system
xiv See https://www2.ed.gov/about/offices/list/ovae/ten-attachment.pdf, https://careerpathways.workforcegps.org/resources/2016/10/20/10/11/Enhanced_Career_Pathways_Toolkit, https://lincs.ed.gov/professional-development/resource-collections/profile-556, and https://cte.ed.gov/initiatives/career-pathways-systems%E2%80%8B
xv See Maguire, S., Freely, J., Clymer, C., Conway, M., and Schwartz, D. 2010. Tuning in to local labor markets: Findings from the sectoral employment impact study. Public/Private Ventures: New York.
xvi See NIST ITL Computer Resource Center https://csrc.nist.gov/glossary
xvii The Department of Defense (DOD) defines cyberspace as a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers. https://sgp.fas.org/crs/natsec/IF10537.pdf
xviii NIST ITL Computer Resource Center defines cybersecurity as the ability to protect or defend the use of cyberspace from cyberattacks https://csrc.nist.gov/glossary
xix The U.S. Bureau of Labor Statistics Standard Occupational Classification (SOC) system is a federal statistical standard used to classify the nation's workforce into occupational categories for the purpose of collecting, calculating, or

disseminating data. All workers are classified into one of 867 detailed occupations according to their occupational definition. To facilitate classification, detailed occupations are combined to form 459 broad occupations, 98 minor groups, and 23 major groups. Detailed occupations in the SOC with similar job duties, and in some cases skills, education, and/or training, are grouped together. See https://www.bls.gov/soc/2018/major_groups.htm

[xx] Entry point refers to any entrance to the career pathway journey and not just the "first." An individual could initially enter into a pathway, exit, and later enter again creating a different entry point.

[xxi] Comprehensive high schools are the most popular form of public high schools, as compared to practice in which examinations are often used to sort students into different high schools for different populations. Some high schools specialize in university-preparatory school academic preparation, some in remedial instruction, and some in vocational instruction. The average comprehensive high school offers more than one course of specialization in its program. Comprehensive high schools generally offer a college preparatory course and one or more scientific or vocational courses.

[xxii] For example, Moreno Valley Unified School District in Moreno Valley, CA offers a highly successful cyber academic program.

[xxiii] For example, Horizontal High School, an independent charter school in El Paso, TX, offers a P-TECH Cyber security Academy.

[xxiv] For example, Howard County Public School System, in Howard County, MD, in partnership with Howard Community College, offers an Early College Cybersecurity Program.

[xxv] For example, Charleston County School District and Triton Technical College in South Carolina offer a Cybersecurity Youth Apprenticeship Program.

[xxvi] See https://www.nacep.org/about-nacep/what-is-concurrent-enrollment/ to learn more about the difference between articulated and dual or transcripted credit.

[xxvii] An AS degree is a two-year degree offered by most community colleges and some four-year colleges. An AAS degree prepares graduates to enter a career immediately after graduation.

[xxviii] See the St. Petersburg College in St. Petersburg, FL, Cybersecurity BAS degree.

[xxix] See George Mason University in Fairfax, VA, Applied Science in Cybersecurity concentration degree.

xxx See https://wdr.doleta.gov/directives/attach/TEGL15-10.pdf

[xxxi] For example, the M.S. in Cybersecurity Risk and Strategy, offered jointly by the NYU School of Law and NYU Tandon School of Engineering, is designed to create managers with the integrated expertise needed to play a leadership role in cybersecurity..

[xxxii] See https://www.aihr.com/blog/job-rotation/

[xxxiii] See https://www.cyberseek.org/heatmap.html

[xxxiv] The DC metro region might have a higher need for defense industry or policy, NY might have a higher need for financial sector cybersecurity work roles, and the Mid-west might have a higher concentration of manufacturing cybersecurity sector.

[xxxv] "Meaningful employer engagement" is the process by which State and/or local stakeholders (e.g., training providers, colleges, workforce boards) convene with local and regional industry employers to discuss the skill and credential needs of their workforce and ways in which education and training programs can best prepare individuals.

[xxxvi] See https://www.cyberseek.org/heatmap.html

[xxxvii] The Act of August 16, 1937 (commonly known as the ''National Apprenticeship Act''; 50 Stat. 664, chapter 663; 29 U.S.C. 50 et seq.).

[xxxviii] A stackable credential is part of a sequence of credentials that can be accumulated over time and move an individual along a career pathway or up a career ladder.

[xxxix] See Cyversity https://www.cyversity.org/, Women in Cybersecurity https://www.wicys.org/, Cyberjutsu https://womenscyberjutsu.org/, and MENTOR https://www.mentoring.org/

[xl] "Workforce preparation activities" means activities, programs, or services designed to help an individual acquire a combination of basic academic skills, critical thinking skills, digital literacy skills, and self-management skills, including competencies in utilizing resources, using information, working with others, understanding systems, and obtaining skills necessary for a successful transition into and completion of postsecondary education or training, or employment. WIOA HR 803, SEC. 203. DEFINITIONS (17)

[xli] "Foundational professional skills" (often also called "soft skills" or "essential skills") are the skills needed for success in college, career, and life, such as, but not limited to, punctuality, communication, collaboration, and problem-solving.

[xlii] See https://cte.ed.gov/initiatives/employability-skills-framework

[xliii] See https://www.careeronestop.org/CompetencyModel/competency-models/cybersecurity.aspx

[xliv] Work-based learning provides participants with work-based opportunities to practice and enhance the skills and knowledge gained in their program of study or industry training program, as well as to develop employability.

[xlv] Non-duplicative (across education and training partners) assessments of participants' education, skills, competencies, assets, and support service needs as they move through a career pathway and its programs.
[xlvi] Flexible format could include online, hybrid, in-person, weekend, after hours, or other options that meet the needs of a particular target group.
[xlvii] "Modularized curriculum" is a curriculum that is divided into shorter, 'self-contained' segments or chunks of instruction. The common module length can vary depending upon content, format, and schedule of the course.
[xlviii] "Contextualized curriculum and instruction" is the practice of systematically connecting basic skills and academic instruction to industry or occupational content.
[xlix] "Recognized post-secondary credential", as defined by the Workforce Innovation and Opportunity Act, means a credential consisting of an industry-recognized certificate or certification, a certificate of completion of an apprenticeship, a license recognized by the State involved or Federal Government, or an associate or baccalaureate degree. https://www.doleta.gov/wioa/Docs/wioa-regs-labor-final-rule.pdf WIOA sec. 3(52)
[l] Core programs within WIOA are: WIOA Title I (Adult, Dislocated Worker and Youth formula programs) administered by Department of Labor (DOL); Adult Education and Literacy Act programs administered by the Department of Education (DoED); Wagner-Peyser Act employment services administered by DOL; and Rehabilitation Act Title I programs administered by DoED.
[li] Required programs within WIOA are: Career and Technical Education (Perkins), Community Services Block Grant, Indian and Native American Programs, HUD Employment and Training Programs, Job Corps, Local Veterans' Employment Representatives and Disabled Veterans' Outreach Programs, National Farmworker Jobs Program, Senior Community Service Employment Program, Temporary Assistance for Needy Families (TANF), Trade Adjustment Assistance Programs, Unemployment Compensation Programs, and YouthBuild.
[lii] "Incumbent worker training" is training that is developed with an employer or employer association (group of employers) to retain a skilled workforce or avert the need to lay off employees by assisting the workers in obtaining the skills necessary to retain employment.
[liii] See https://www.careerladdersproject.org/
[liv] See https://www.workforcegps.org/ and Career Pathway Community resources https://careerpathways.workforcegps.org/
[lv] See https://www.careeronestop.org/. Career One Stop is a career, training, and job search website maintained by DOL.
[lvi] See https://www.careeronestop.org/CompetencyModel/Competency-Models/cybersecurity.aspx which includes a Technical Assistance Guide https://www.careeronestop.org/CompetencyModel/BuildaModel/TAG.pdf and access to a Competency Model Clearinghouse (CMC) https://www.careeronestop.org/CompetencyModel/ that serves as resources for the creation of customized competency models tailored to a local region or specific sector in the industry.
[lvii] See Perkins Collaborative Resource Network https://cte.ed.gov/initiatives/career-pathways-systems
[lviii] See Perkins Collaborative Resource Network Programs of Study Design https://cte.ed.gov/initiatives/career-pathways-systems
[lix] See https://niccs.cisa.gov/workforce-development/cyber-career-pathways
[lx] The NICE Framework Categories currently include Securely Provision, Operate and Maintain, Oversee and Govern, Protect and Defend, Analyze, Collect and Operate, and Investigate, however, updates are planned in 2023. To learn more visit https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center
[lxi] See https://public.cyber.mil/cw/dcwf and https://www.dodemergingtech.com/dod-cyber-workforce-framework-dcwf
[lxii] See https://www.gao.gov/assets/700/697523.pdf to learn more about the roles and responsibilities of Cyber Mission Force Training
[lxiii] See https://www.jcs.mil/Doctrine/. The objective of the JCT&CS initiative is to have forces trained and ready to meet the challenges of cyberspace. The training program calls for creating common, arduous standards for both individuals and collectives, administering first-rate training, and accurately evaluating the forces' capabilities to perform missions. Standards developed by the JCT&CS are in the operational context and mission requirements of CYBERCOM and its components. Training standards are defined for each job role and for collective audiences. The joint procedures and guidelines for implementing the initiative are patterned after the Joint Training System's (JTS's) four phases: requirements, planning, execution, and assessment. The JTS framework provides commanders with integrated processes used to evaluate the command's missions and to determine the tasks essential to accomplishing those missions. These processes are designed to improve the commander's joint readiness by linking plans, training, and assessment to mission requirements.
[lxiv] See https://public.cyber.mil/cw/dcwf/
[lxv] See https://milgears.osd.mil/CSWF
[lxvi] See https://www.cyberseek.org/

[lxvii] See https://www.issa.org/cyber-security-career-lifecycle/
[lxviii] See https://www.comptia.org/certifications/which-certification
[lxix] See https://www.comptia.org/content/lp/it-certifications-job-match
[lxx] See https://pathways.educause.edu/pathways/information-security
[lxxi] See https://www.sans.org/cyber-security-skills-roadmap/
[lxxii] See https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt7f56517b3622c96b/2022_Roadmap_Web.pdf
[lxxiii] See report https://sa2020.org/resources/talent-pipeline-task-force-report
[lxxiv] See https://www.sa2020.org/wp-content/uploads/2015/07/CareerPathway_Cybersecurity-FINAL.pdf
[lxxv] See https://www.nist.gov/nice/apprenticeship-finder
[lxxvi] See https://www.cyberseek.org/pathway.html
[lxxvii] See https://www.nist.gov/itl/applied-cybersecurity/nice/events/cybersecurity-career-awareness-week