
# Cybersecurity Workforce Definitions Report

April 2024
Final Report

Contractor Awardee: RTI International

Contract Number: 49100421D0019

Disclaimer: This contract deliverable is intended to report exploratory results of research and analysis undertaken by the National Center for Science and Engineering Statistics (NCSES) within the U.S. National Science Foundation (NSF). Any opinions, findings, conclusions, or recommendations expressed in this contract deliverable do not necessarily reflect the views of NSF. This contract deliverable has been released by the NCSES Cybersecurity Workforce Data Initiative (CWDI) Working Group to inform interested parties of ongoing research or activities and to encourage further discussion of the topic. Please send questions to NCSES-CWDI@nsf.gov.

# NCSES Cybersecurity Workforce Data Initiative:

# Cybersecurity Workforce Definitions Report

April 2024


## Abstract

This report reviews the federal, private sector, and international definitions of the cybersecurity workforce. We find that there is no comprehensive definition of who composes the cybersecurity workforce in the United States. Rather than a definition, frameworks focused on work roles, tasks, knowledge, and skills that can cut across job titles and industries are common. The lack of a standardized definition of the workforce is a limiting factor in addressing the national cybersecurity challenges and workforce gaps cited by employers and industry research. Leading taxonomies, including the NICE Framework from the National Institutes for Standards and Technology (NIST), consider the cybersecurity workforce to include both core workers and those who engage in cybersecurity activities in their role, providing an expansive definition of cybersecurity workers.

Based on this review of frameworks and definitions, we propose a definition of the cybersecurity workforce for the Cybersecurity Workforce Data Initiative (CWDI). This proposed definition balances the tension between a broad set of cybersecurity work roles and skills like those emphasized by federal government agencies and a narrow, concise definition from organizations like the European Union, United Kingdom, and professional organizations. Our proposed definition establishes a core workforce and adjacent workforce based on the percentage of work activities that align with the NICE Framework work roles and aligning them with traditional metrics in labor market research.


## Suggested Citation


Hogan M, Bean de Hernandez A, McHugh P, Arbeit CA, Sullivan P; National Center for Science and Engineering Statistics (NCSES). 2024. *Cybersecurity Workforce Data Initiative: Cybersecurity Workforce Definitions Report*. Alexandria, VA: National Science Foundation. Available at https://ncses.nsf.gov/about/cybersecurity-workforce-data-initiative.


## Contact


Kelly Phou
CWDI Project Lead and Contracting Officer's Representative
Science Technology, and Innovation – Public Information
National Center for Science and Engineering Statistics

## Contents

## Acknowledgements

*Report Authors:*

Michael Hogan
Alison Bean de Hernandez
Patrick McHugh
Caren A. Arbeit and
Pearl Sullivan
RTI International, under contract to the National Center for Science and Engineering Statistics (NCSES)
cwdi@rti.org

Thank you to the NCSES Cybersecurity Workforce Data Initiative working group members Amber Levanon Seligson, Kelly Phou, Gigi Jones, Shelley Feuer, Julia Milton, Vrinda Nair, Daniela Oliveira, and Danielle Taylor and RTI editors Virginia Ferguson, August Gering, and Cat Olenick for content and editorial feedback on earlier versions of this report. Findings, conclusions, and recommendations in this report are those of the authors and do not necessarily reflect the views of the National Science Foundation.

# Executive Summary

As part of the CHIPS and Science Act of 2022, the National Center for Science and Engineering Statistics (NCSES) within the National Science Foundation (NSF) established the Cybersecurity Workforce Data Initiative (CWDI) to address the growing demand for a skilled workforce in cybersecurity and address existing data gaps. This report, on the definitions of the cybersecurity workforce, is the first in a series of reports that will inform NSF and future government data collections on the cybersecurity workforce. RTI International (RTI) is the research lead on this report with the support of NSF and its cybersecurity workforce working group.

## Background

Federal and non-federal efforts to understand the cybersecurity workforce have been driven by rapidly evolving technology demands. While initial federal workforce efforts focused on government and defense jobs, recent demands for cybersecurity span industry sectors. The White House 2023 National Cyber Workforce and Education Strategy emphasizes the need for cyber skills and education across the entire workforce.[1] New and changing cybersecurity technologies have expanded the cybersecurity skillset, which complicates creating a clear definition of who counts as a cybersecurity worker.

## Existing Workforce Frameworks

In the U.S., the most frequently cited taxonomy for cybersecurity work is the NICE Framework, released by NIST. The NICE Framework is built around knowledge, skills, and work roles and is not limited by occupation. The knowledge, skills, and work roles include those associated with core cybersecurity workers and those whose work roles have a direct or indirect impact on the cybersecurity risks of an organization. It reflects that cybersecurity activities and work cut across occupations and industries.

The NICE Framework is highly flexible and has been adopted and adapted in federal employment from organizations like the Office of Personnel Management (OPM) and the Department of Homeland Security (DHS) but has not easily translated to private sector work or traditional labor market data sources. Programs like CyberSeek translate the NICE Framework into labor market data using web scraping and Lightcast data. Its flexibility is a strength but has drawbacks, most notably, it creates a tension between defining a narrow, clearly defined set of cybersecurity work roles and a broad set of cybersecurity and cyber skills across the workforce and society.

Other workforce frameworks cited by private sector and industry leaders include the European Cybersecurity Skills Framework (ECSF) and United Kingdom Cybersecurity Careers Framework. These delineate a narrower set of job titles. Professional organizations such as ISC2 and CompTIA retain their own definitions and taxonomies of the workforce, including both those who hold professional certifications and traditional credentials.

Importantly, federal data providers such as the BLS, Census Bureau, Department of Education, and O*NET do not have a single, concise definition of cybersecurity work that translates into traditional labor market data using categories like standard occupation classification (SOC). Experts in the academic and private sector cite the lack of a concise definition of the workforce and consistent data as key obstacles to addressing cybersecurity challenges.

## Proposed Definition of the Cybersecurity Workforce

The definition of the cybersecurity workforce we propose includes cybersecurity as both an occupation and as a work activity. This reflects the complexity of this workforce and work roles.

The cybersecurity workforce includes a core set of cybersecurity occupations focused on cybersecurity. Workers in other occupations where their primary, or secondary work activities include cybersecurity are also part of the core cybersecurity workforce. Cybersecurity-involved workers engage in cybersecurity work as a work activity that is not their primary or secondary work activity. Finally, workers not already identified as core or cybersecurity-involved workers whose tasks, skills, knowledge and/or jobs functions are related to cybersecurity are part of the cybersecurity adjacent workforce.

Thus, our definition includes both a core set of cybersecurity occupations, as well as cybersecurity-involved and cybersecurity-adjacent workers whose activities include various tasks, knowledge, skills, and functions related to cybersecurity. The definition is based on skills and work activities and follows the existing frameworks from organizations like NIST, ISC2, CompTIA, and the ECSF. Additionally, it parallels other NCSES research on work activities by considering workers' primary and secondary work responsibilities. This multilayered approach thus remains consistent with the NICE Framework and other comprehensive flexible definitions, while also addressing the primary challenges of the NICE Framework.

## Key Takeaways and Next Steps

In 2024, cybersecurity activities cut across work roles, occupations, and industries making it difficult to delineate or place a border around the cybersecurity workforce using existing data. Recognizing that cybersecurity is a component of a range of occupations, we will refine this definition through a series of stakeholder workshops to delineate specific factors around a cybersecurity job. In these workshops we will ask participants to give feedback on this proposed definition, which will help guide any necessary revisions.

Additionally, we are conducting an analysis of existing estimates of the workforce and are reviewing federal and administrative data to prioritize existing data and surveys and understand existing gaps. Together, these analyses are intended to guide future data collection efforts by NCSES either through a new survey or augmenting existing surveys to produce national estimates on the cybersecurity workforce, addressing a key gap in filling the nation's cybersecurity needs.

# Cybersecurity Workforce Definitions Report

## Introduction

As mandated by the Creating Helpful Incentives to Produce Semiconductors (CHIPS) and Science Act of 2022, the National Center for Science and Engineering Statistics (NCSES) is establishing a Cybersecurity Workforce Data Initiative (CWDI) that seeks to bridge the gap between the rapidly shifting demands for cybersecurity and the skills and knowledge of the current and future workforce. The CWDI is led by NCSES, a principal federal statistical agency at the National Science Foundation (NSF). The goal of the CWDI is to assess the feasibility of producing nationally representative estimates and statistics on the cybersecurity workforce in the United States.

This report provides a review of the existing definitions, frameworks, and taxonomies of the cybersecurity workforce in the United States and proposes a working definition for the CWDI. The working definition will identify those currently working in cybersecurity in the public and private sectors, as well as the pipeline for new workers through cybersecurity degree programs and credentials. Currently, the NICE Workforce Framework for Cybersecurity (NICE Framework), a program of the National Institutes for Standards and Technology (NIST), is the most frequently cited framework for understanding the current workforce. The NICE Framework uses knowledge, skills, and work roles to define cybersecurity work and provides a strong guiding framework.

As this report will show, cybersecurity work is not limited to a single definition, job title, or set of job titles, but by activities and work roles that relate to protecting information technology (IT) and operational technology. Changing technology demands has created an understanding of the cybersecurity workforce and requires an expansive definition covering both jobs that are core cybersecurity jobs and jobs with cybersecurity functions or where cybersecurity skills are critical but not central to the position. The definition proposed in this report reflects the crosscutting nature of cybersecurity work, aligns with the NICE Framework, and addresses the need to *understand both core and adjacent cybersecurity occupations*.

### *Background*

This first CWDI report outlines existing definitions, frameworks, and taxonomies of the cybersecurity workforce and proposes a working definition for the initiative, to be refined with additional input from workshops with experts in the field. This report will introduce definitions and provide a baseline for the analyses which will follow:

- Supply and demand analysis, including in-depth analysis of data sources
- Workshops with stakeholders and subject matter experts to refine the definitions and needs
- Evaluation of existing federal data sources with data relevant to the cybersecurity workforce
- Evaluation of private, commercial, and other nonfederal data sources for cybersecurity workforce

Together these reports will provide the background information should NCSES conduct a pilot survey to capture the cybersecurity workforce in the United States using the definitions and criteria defined in this work.

## Federal Efforts to Define the Cybersecurity Workforce

Cybersecurity, with its origins in cryptography during World War II, evolved through the birth of the early internet, the growth of information security, personal computers, mobile and cloud computing, and artificial intelligence. Today, as digital technology is incorporated into every facet of business, government, defense, and everyday life, the role of cybersecurity skills and workers is evolving quickly.[2]

In the 21st century, efforts to define the cybersecurity workforce have focused on a set of cybersecurity job functions, and the federal government has maintained an expansive framework for the cybersecurity workforce, defining it as all workers who perform cybersecurity job functions and have the skills needed to do so. As this section will show, federal workforce initiatives and frameworks have not focused on a single job title or credential, but on the workplace skills and responsibilities of workers in protecting and securing information. By defining the workforce through job roles and skills, federal workforce frameworks allow for flexibility and can adapt to the rapidly evolving needs of cybersecurity.

This approach has drawbacks, most notably that this flexibility creates a tension between a narrow, clearly defined set of cybersecurity work roles and a broad set of cybersecurity and cyber skills across the workforce and society. The White House 2023 National Cyber Workforce and Education Strategy emphasizes the need for cyber skills and education across the entire workforce.[3] New and changing cybersecurity technologies have expanded the cybersecurity skillset, which further complicates creating a clear definition of who counts as a cybersecurity worker.

### *History of Federal Government Cybersecurity Workforce Initiatives*

The federal government has been instrumental in the development of the cybersecurity field. Federal entities led the development of foundational technologies for both cyber defense and attack, and federal agencies were early adopters of the developed cybersecurity tools. In addition to being on the forefront of the cybersecurity field, the federal government has led the development of definitions for the cybersecurity field and cybersecurity workforce. The White House, Congress, and various agencies have published both strategic cybersecurity strategies and cybersecurity workforce strategies since 2000, outlined in table 1.

Table 1
Selected recent federal government cybersecurity workforce initiatives
(Initiatives)

| Year | Agency | Initiative |
|---|---|---|
| 2001 | NSF/OPM/DHS | CyberCorps Scholarship for Services first cohort |
| 2007 | NSA | NSA IT Security Essential Body of Knowledge |
| 2008 | White House | The National Comprehensive Cybersecurity Initiative |
| 2009 | White House | White House Cyberspace Policy Review |
| 2010 | White House | National Security Presidential Directive 54 creates process to establish National Initiative for Cybersecurity Education (NICE) Framework |
| 2011 | OPM | Office of Personnel Management Competency Model for Cybersecurity |
| 2012 | NIST | First version of the NICE Framework released |
| 2014 | Congress | Cybersecurity Enhancement Act |
| 2014 | NIST | Second version of the NICE Framework released |
| 2015 | Congress | Federal Cybersecurity Workforce Assessment Act |
| 2016 | White House | Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure |
| 2017 | NIST | Third version of the NICE Framework released |
| 2018 | NSA | Supporting the Growth and Sustainment of Nation's Cybersecurity Workforce |
| 2019 | White House | Executive Order 13870: America's Cybersecurity Workforce |
| 2020 | NIST | Revised NICE Framework released |
| 2020 | NSA | CISA Growth and Sustainment of Nation's Cybersecurity Workforce |
| 2021 | White House | Executive Order on Improving the Nation's Cybersecurity |
| 2022 | Congress | CHIPS and Science Act mandates CWDI |
| 2023 | White House | National Cyber Workforce and Education Strategy |
| 2024 | NIST | Revisions to NICE Framework |

CHIPS = Creating Helpful Incentives to Produce Semiconductors; CISA = Cybersecurity and Infrastructure Security Agency; CWDI = Cybersecurity Workforce Data Initiative; DHS = Department of Homeland Security; IT = information technology; NICE = National Initiative for Cybersecurity Education; NIST = National Institute of Standards and Technology; NSA = National Security Agency; NSF = National Science Foundation; OPM = Office of Personnel Management.

Source(s):
National Center for Science and Engineering Statistics, Cybersecurity Workforce Data Initiative (CWDI).

Strategies include a mix of national cyber defense and cybersecurity, alongside efforts to strengthen the cybersecurity skills of the federal and nonfederal workforce. Early federal efforts to define the cybersecurity workforce focused on federal employees in defense and national security roles. Since then, federal work has expanded to reflect the increasing importance of cybersecurity for private companies, organizations, and individuals. Notably, the 2023 White House Strategy emphasizes that the responsibility of protecting software and systems from vulnerabilities must shift from end users to developers and large vendors, reflecting the expansion of cybersecurity work into software and product development to protect users such as individuals, businesses, and public sector agencies.[4]

Federal initiatives and workforce efforts do not rely on a concise definition of the cybersecurity workforce. Federal efforts and many nongovernmental organizations reference the NICE Framework[5] when discussing cybersecurity work roles, which stands as the most comprehensive existing effort to capture cybersecurity work roles, functions, and skills.[6] The NICE Framework evolved from the 2008 National Comprehensive Cybersecurity Initiative, initially created to address federal workforce needs. It expanded to the private sector in 2009 and released its first framework in 2012, with updates in 2014, 2017, 2020, and 2024.[7]

### *The NICE Framework and its Uses*

The NICE Framework is a national framework to categorize and describe cybersecurity work. It is the most exhaustive taxonomy from a government agency for defining the tasks, skills, and knowledge entailed in cybersecurity work in the United States. The NICE Framework is an effort to create shared baseline definitions of cybersecurity functions and worker capabilities, and intentionally does not define the cybersecurity workforce. NIST has refined the NICE Framework through several iterations since it was originally developed, with the most recent revision in 2024.

The NICE Framework is a useful and impactful theoretical framework for understanding cybersecurity work and work roles. NIST emphasizes that the framework is not intended to be a comprehensive definition of the workforce but a way to understand cybersecurity work and job roles. As such, only some documents include a succinct statement describing the cybersecurity workforce. The NICE Framework describes the cybersecurity workforce as:

> *Those whose primary focus is on cybersecurity as well as those in the workforce who need specific cybersecurity-related knowledge and skills in order to perform their work in a way that enables organizations to properly manage the cybersecurity-related risks to the enterprise.*[8]

The framework purposely takes a broad approach to understanding the cybersecurity workforce. It includes detailed information regarding cybersecurity work roles and is intended to be flexible and align its tasks, knowledge, and skills in varying degrees to different work roles. Currently, it contains 993 proposed tasks and 214 knowledge and skills statements. This complexity reflects the growing and changing nature of cybersecurity work.

The NICE Framework is flexible, but it has drawbacks. The knowledge, tasks, and skills statements in the NICE Framework encompass a large number of occupations, yet do not differentiate the centrality of these tasks, knowledge, and skills to the work performed in the occupation. Because of this, it is not aligned with traditional occupational or workforce data. While it can be used theoretically across many applications, it is not currently aligned with the federal Standard Occupational Classification (SOC) taxonomy of codes or other metrics used to traditionally define and measure the workforce. While the NICE Framework is commonly cited by federal agencies to define their internal workforce, there are others, including federal survey data providers, who acknowledge that the NICE Framework does not easily translate to their data structures or occupation titles. The succinct description of the cybersecurity workforce (cited above) is not presented as central to the framework itself and is thus rarely used.

With its strengths and gaps, we identified four core types of relationships between the NICE Framework and cybersecurity workforce initiatives. The NICE Framework serves, for different organizations, as:

- A foundational management framework: Federal agencies use the NICE Framework as the foundation for organizing and managing their cybersecurity workforce, including creating job titles, establishing pay scales and increased pay for certifications, identifying workforce needs, developing career pathways, and targeting workforce recruitment and retention efforts. These are most common in management of the federal workforce.
- A basis for developing training coursework: Some universities organize coursework based on the NICE Framework to secure federal funding and scholarships through programs like CyberCorps Scholarship for Service. Designation from the National Security Agency (NSA) as one of the National Centers of Academic Excellence in Cybersecurity (NCAE-C) requires utilizing the NICE Framework.

- A basis to identify cybersecurity jobs: CyberSeek is a special case in the private sector because it uses task, skill, and knowledge statements from the NICE Framework in searches of job listings using data from Lightcast. CyberSeek is funded by and supported by NIST.

*Strengths of the NICE Framework*

The NICE Framework is the most refined and widely used taxonomy for understanding cybersecurity work in the United States, and its strengths reflect its flexibility and the crosscutting nature of cybersecurity work. Its adaptability gives it several strengths:

- Establishes the core competencies and work functions common to most cybersecurity positions: The NICE Framework helps to identify the knowledge and skills shared across work roles and competency areas. This helps to establish the foundational knowledge and abilities that are required to be part of the cybersecurity workforce. The work role categories provide seven critical role types that focus on the function of a position. This is a succinct, approachable, and easy-to-understand portion of the framework.

- Reflects the lack of a clear boundary around the periphery of the cybersecurity workforce: Definitions based in skills, knowledge, and tasks reflect the fact that many employees without cybersecurity in their job titles nevertheless perform vital cybersecurity functions. Particularly among IT professionals, many of the core competencies and tasks that are part of cybersecurity work are held and performed by professionals that work in adjacent occupations.

- Permits flexible and scalable use: Skill- and knowledge-based definitions can be scaled up or down to meet the specific needs of companies and organizations. Smaller organizations can limit the types of work roles that are considered part of their cybersecurity workforce, while larger organizations with more complex information systems can create more granularity in how their cybersecurity workforce is organized and defined.

- Facilitates workforce planning for federal agencies: Associating cybersecurity workforce roles with key skills and knowledge currently helps federal agencies assess where gaps exist between the skills and knowledge possessed by their existing workforce and their current or projected cybersecurity needs.

*Federal Agencies Using the NICE Framework to Define their Cybersecurity Workforce*

Federal cybersecurity workforce initiatives, including those from the Department of Defense (DOD), Cybersecurity & Infrastructure Security Agency (CISA), White House, National Initiative for Cybersecurity Careers and Studies (NICCS), and Office of Personnel Management (OPM), all reference the NICE Framework. What these organizations have in common is that they employ cybersecurity workers and support national cybersecurity defense functions. For these agencies, the NICE Framework is foundational to their management, definitions, and job titles and roles. (For more information on the agencies' definitions of the cybersecurity workforce, see appendix A.)

Other federal employers work with the NICE Framework, adapting its components to create classifications that broadly identify their cybersecurity workforce. For example, the OPM definition cites the NICCS glossary and the White House Cyberspace Policy Review (May 2009), in addition to the NICE Framework. The NICCS glossary cites the NICE Framework and the same White House Cyberspace Policy Review (May 2009). The NICE Framework is mapped to 52 OPM codes that define cybersecurity workers in the federal workforce,[9] CISA and NICCS define the cyber workforce using skill

communities and work roles, and the Cyber Career Pathways Tool[10] breaks out the workforce into 52 work roles, which are the same ones identified by OPM.

OPM provides a direct definition of cybersecurity:

> Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.[11]

The cybersecurity workforce classifications adopted by federal agencies that use the NICE Framework capture the complexity and expansiveness of the federal cybersecurity workforce. Yet they also suffer from many of the same drawbacks—the definitions cannot identify which portions of and positions within the workforce are focused primarily on cybersecurity.

*Function of Federal Cybersecurity Workforce Frameworks*

Agencies that use the NICE Framework for management of the federal workforce in cybersecurity (e.g., OPM, DOD, CISA, NICCS, and NCAE-C) draw on the framework to create a common language for cybersecurity work and to identify job titles, specialty areas, and work roles. OPM and DOD make the most extensive use of the NICE Framework to manage the cybersecurity workforce across agencies and departments. Both use the task, knowledge, and skill statements in the NICE Framework to standardize job descriptions, identify cybersecurity workforce needs, develop targeted recruitment and retention efforts to fill those needs, identify training needs, develop career pathways, and organize compliance reporting.

- In addition to these functions, OPM uses the NICE Framework to standardize occupational series and grade levels, identify private credentials that qualify federal workers for pay increases, and provide data on the federal cybersecurity workforce.

- DOD also uses the NICE Framework to enhance interoperability through establishing core skills and knowledge needed across force units and missions.

Given their role in setting training standards, both NICCS and NCAE-C use the NICE Framework to establish curriculum requirements for educational institutions. NICCS also uses the framework to identify career pathways. The uses of the NICE Framework are outlined in table 2.

Table 2

Use of the NICE Framework across federal cybersecurity workforce frameworks

(Use)

| Use | OPM | DOD | CISA | NICCS | NCAE |
|---|---|---|---|---|---|
| Create a shared lexicon | X | X | X | X | X |
| Identify categories, specialty areas, and work roles | X | X | X | X | X |
| Standardize job descriptions and titles | X | X | | | |
| Facilitate supply, demand, and gaps analysis | X | X | | | |
| Target recruitment and retention | X | X | | | |
| Identify training needs | X | X | | X | X |
| Develop career paths | X | X | | X | |
| Support compliance reporting | X | X | | | |
| Standardize occupational series and grade levels | X | | | | |
| Identify credentials for pay increases | X | | | | |
| Measure size of the cybersecurity workforce | X | | | | |
| Enhance interoperability across missions | | X | | | |

CISA = Cybersecurity and Infrastructure Security Agency; DOD = Department of Defense; NCAE = National Centers of Academic Excellence; NICCS = National Initiative for Cybersecurity Careers and Studies; OPM =Office of Personnel Management.

Note(s):

While practical utilization of the NICE Framework continues to evolve and not all uses cases are clearly documented for public consumption, a number of resources speak to how different federal agencies build on the NICE Framework. For details on OPM uses, see United States Office of Personnel Management. 2018. *Interpretive Guidance for Cybersecurity Positions: Attracting, Hiring, and Retaining a Federal Cybersecurity Workforce*. Available at https://www.opm.gov/policy-data-oversight/classification-qualifications/reference-materials/interpretive-guidance-for-cybersecurity-positions.pdf. For information on DOD uses, see DEFENSESSCOOP. 2023. *DOD Issues Long-Awaited Cyber Workforce Framework.* Available at https://defensescoop.com/2023/02/16/dod-issues-long-awaited-cyber-workforce-framework/; Department of Defense. *DOD Cyber Workforce Framework.* Available at https://www.dodemergingtech.com/dod-programs/dod-cyber-workforce-framework-dcwf/. For details on how CISA references the NICE Framework, see Cybersecurity & Infrastructure Security Agency. N.d. *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.* Available at https://www.cisa.gov/national-initiative-cybersecurity-education-nice-cybersecurity-workforce-framework. For information on how NICCS uses the NICE Framework to establish career pathways, see National Initiative for Cybersecurity Careers and Studies. 2024. *Cyber Career Pathway Tool.* Available at https://niccs.cisa.gov/workforce-development/cyber-career-pathways-tool. For information on how NCAE uses the NICE Framework to set curriculum requirements for National Centers of Academic Excellence in Cybersecurity, see National Centers of Academic Excellence in Cybersecurity. 2024. *National Centers of Academic Excellence in Cybersecurity (NCAE-C 2024): Designation Requirements and Application Process.* Available at https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/20240103_CAE2024_CAE-CD_Designation_Requirements_Ver1-16_Clean.pdf.

Source(s):

National Center for Science and Engineering Statistics, Cybersecurity Workforce Data Initiative (CWDI).

## *Federal Agencies Not Using the NICE Framework*

The NICE Framework accurately describes the complexity of cybersecurity work, noting that cybersecurity skills and job roles cut across job titles. It also allows for flexibility as the field evolves. However, the framework does not provide a comprehensive definition. As the White House 2023 National Cyber Workforce Strategy notes, the data needed to guide economic development, workforce development, and education programming for cybersecurity is lacking. The NICE Framework serves as a strong theoretical framework for understanding the workforce, but several gaps exist in connecting it to labor market data, specifically from federal survey data providers. The NICE Framework:

- Does not translate to labor market data from federal survey providers: Classifications from DOD and OPM that rely on the NICE Framework are well-documented, but the use of the NICE Framework by federal statistical providers and private labor market analysis is limited.

- Is too flexible and complex for some uses: While the flexibility, complexity, and expansiveness of the NICE Framework are strengths, they have some distinct drawbacks. The framework lacks a sense of centrality of tasks, knowledge, skills, and work roles to positions. Thus, positions where cybersecurity is a central or primary focus are difficult to differentiate from those where cybersecurity tasks, knowledge, skills, and work roles are secondary, tertiary, or minor components of a position.

Because of these limitations, some federal agencies do not reference the NICE Framework in their work, most notably major providers of nationally representative labor market and education data, including the Census Bureau, Bureau of Labor Statistics (BLS), Department of Labor's Occupational Information Network (O*NET), and Department of Education. Thus, critical federal labor market survey data does not sufficiently capture the cybersecurity workforce. Interviewees across the public, private, and academic sectors cited a lack of reliable secondary federal data as a critical gap in addressing cybersecurity workforce challenges, noting that the NICE Framework did not translate to traditional federal labor market data sources.

Federal agencies using the SOC and Classification of Institutional Programs (CIP) for national surveys acknowledge that their current classifications and definitions do not capture cybersecurity. Surveys from the Census Bureau, Department of Education, BLS, and O*NET do not have strong links to the NICE Framework, showing a gap between the theoretical framework and labor market data needed from federal surveys.

The 2023 White House National Cyber Workforce and Education Strategy emphasized that federal longitudinal data did not fully describe the national cybersecurity workforce in ways that can inform workforce and economic development and that agencies need better data to understand demands and needs.[12] Interviewees from outside of the federal sector noted that because of the complexity of the NICE Framework and the lack of reliable labor market data, industry leaders rely heavily on data from private or internal surveys, certificate providers, or other administrative data sources such as web scraping which they cite as unreliable or reflective of only a portion of the population.

### *Synthesis of Federal Cybersecurity Workforce Frameworks*

Across the various federal cybersecurity workforce initiatives, several themes emerge around the definition of the workforce, making it unique from other professions, industries, and occupations.

- Based on job functions and skills: Across governmental agencies and nongovernmental organizations, the definition of the cybersecurity workforce draws from the job functions performed and from the requisite skills and knowledge required. Classifications vary in the amount of cybersecurity-specific work performed that is required for someone to be considered part of the cybersecurity workforce but share the feature of defining the cybersecurity space in terms of the functions performed.

- Made up of a large number of job titles or occupation codes: The cybersecurity workforce cannot be limited to professionals with specific job titles, occupation codes, or credentials that indicate expertise in cybersecurity work. Government and industry experts note that different workers have varying degrees of cybersecurity work roles and that many workers who are not immediately in cybersecurity occupations play important roles in protecting their organizations' information.

- Tied to many industries: The workforce is not limited to a single North American Industry Classification System (NAICS) sector or industry definition and crosses multiple industries. Definitions for cybersecurity jobs in O*NET indicate a presence in Professional & Technical Services and Finance & Insurance, but occupations today span government and national security, healthcare, transportation and logistics, manufacturing, and other industries.

- Not defined by a specific educational program of study or credentialing background: Workers enter the cybersecurity workforce through many doors. While there are programs of study in higher education and professional certifications that can indicate proficiency in cybersecurity

capabilities, much of the workforce was trained in adjacent areas, such as engineering, IT, and computer science. In many job roles, a bachelor's degree plus experience is the minimum requirement. Interviewees and industry research emphasize that cybersecurity workers are more likely to enter the field later in their career and come from a variety of backgrounds, making it difficult to define the workforce pathway.

- Built on the recognition that technology is evolving faster than traditional workforce data: Traditional sources of labor market data, such as BLS, the Department of Education, and the Census Bureau, periodically revise their data structures, updating SOC and CIP codes to reflect new work and educational programs. However, technology and job skills are evolving faster than is feasible to maintain updates to these data structures.

- Do not clearly distinguish the terms cybersecurity and cyber: Public-facing reports frequently use the terms cybersecurity and cyber interchangeably when describing the workforce. In some cases, cyber workforce encompasses a broad definition of technology and other related jobs, while cybersecurity workforce defines the workforce more narrowly as core professions in cybersecurity. Federal- and state-level policies and initiatives use the term cyber to be all-encompassing, and organizations like NIST place a clear delineation between cyber and cybersecurity. Interviewees noted that in some cases, the swapping of terms is unintentional and reflects a misunderstanding of the field by elected officials and business leaders, emphasizing the need for a clearer definition.

## Private and International Cybersecurity Workforce Frameworks

Professional organizations, administrative data providers, and international agencies maintain their own frameworks or classifications for the cybersecurity workforce. When compared to the NICE Framework, their orientations tend to be narrower and more closely aligned to job titles rather than work roles. The most frequently cited data on the cybersecurity workforce in the United States relies on a combination of membership surveys from industry organizations, individuals with professional certifications, or Web scraping of job postings, and each method has its drawbacks. While each source views the cybersecurity workforce differently, they translate work roles to job titles to describe cybersecurity work in a way that business representatives can better understand.

The full list of cybersecurity workforce frameworks and definitions referenced is included in Appendix A.

### *U.S. Nongovernment and Private Sector use of the NICE Framework in Defining the Cybersecurity Workforce*

The NICE Framework has some applications in the private sector, but they are primarily tied to programs funded by the federal government or tied to federal government employment.

*CyberSeek*

CyberSeek defines the cybersecurity workforce through alignment with key job roles and tasks outlined in the framework and aligns them with publicly available data from job postings. CyberSeek is a partnership between NIST, the cybersecurity certification provider Computing Technology Industry Association (CompTIA), and workforce market intelligence company Lightcast. It is the most frequently cited source of data on the needs in the cybersecurity workforce.

*Professional Certifications*

Professional organizations in the United States, including CompTIA,[13] the International Information System Security Certification Consortium (ISC2),[14] Information Systems Security Association,[15] and N2K Networks,[16] provide training and certifications in cybersecurity and are among the nongovernmental organizations that use or reference the NICE Framework. As detailed in appendix A, they most frequently cite the NICE Framework as their definition of cybersecurity work and *acknowledge that the workforce contains a growing range of secondary and adjacent jobs that employ cybersecurity skills*.

*Academic and State-Level Programs*

The NICE Framework also informs a variety of state cybersecurity workforce efforts, including Virginia's Commonwealth Cybersecurity Initiative and the California Cybersecurity Institute at California Polytechnic Institute.[17] Adherence to the NICE Framework is a component of funding eligibility for scholarships at academic programs, including CyberCorps Scholarship for Service and NSA NCAE-C.

### *European Cybersecurity Skills Framework*

The European Cybersecurity Skills Framework (ECSF), released in 2022, outlines 12 work roles for cybersecurity professionals. The framework was designed by a multidisciplinary working group between 2020 and 2022 and is intended to reach both cybersecurity core professionals and non-cybersecurity experts to easily understand the field.[18] The ECSF includes profile titles and summaries, mission,

deliverables, main tasks, key skills and knowledge, and connections to the European Union e-Competence Framework for information and communications technology professionals.[19] Private sector representatives interviewed pointed out that the ECSF was simpler to understand than the NICE Framework and more easily applicable to private sector organizations.

The European Cybersecurity Skills Framework Role Profiles are available from the ENISA at https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles.

### *United Kingdom Cybersecurity Careers Framework*

The United Kingdom (UK) Cybersecurity Council publishes its Cyber Careers Framework, focusing on 16 pathways for specialisms in cybersecurity. Similar to the NICE Framework, it is based on responsibilities, tasks, skills, and knowledge and is intended to be a flexible definition that offers pathways into specific professions. The *Cyber Skills in the UK Labour Market 2023* report released in February 2023, conducted by the UK Department of Science, Innovation, & Technology and Ipsos, defines who works in cybersecurity roles using the 16 specialisms in the route map outlined on the website of the UK Cybersecurity Council at https://www.ukcybersecuritycouncil.org.uk/careers-and-learning/cyber-career-framework/.

### *Organisation for Economic Co-Operation and Development*

In the 2023 Organisation for Economic Co-operation and Development (OECD) report *Building a Skilled Cyber Security Workforce in Five Countries: Insights from Australia, Canada, New Zealand, United Kingdom, and United States*, the authors use natural language processing to identify the level of similarity between Lightcast codes and the five most relevant skills they defined for cybersecurity work: cyber security, information security, anti-malware software, NIST cybersecurity framework, and open Web application security project. Using these five terms, the OECD defined the cybersecurity workforce through five Lightcast codes and their subsequent skills and job descriptions that have the highest level of similarity to the five relevant skills, one of which is the NIST cybersecurity framework.

### *Professional Organizations and Administrative Data Providers*

Professional organizations and administrative data providers have frameworks and taxonomies linked to the reports they publish on the state of the workforce, with the two most prominent frameworks coming from professional organization ISC2 and private data provider Lightcast. Both provide similar estimates of the size of the workforce and define it through a set of occupation groups and occupations related to cybersecurity activities.

Additional professional organizations, workforce frameworks, and definitions are included in Appendix A.

#### *ISC2*

ISC2 is a professional organization that conducted its first workforce report in 2019 to estimate the size of the cybersecurity workforce and the skills needs in the industry. In 2023, it estimated over 1.3 million cybersecurity workers in the United States based on surveys asking respondents for the number of cybersecurity professionals employed in their organizations, estimates from third parties, and extrapolating previous years' estimates. ISC2 defines cybersecurity professionals as its members and those who respond to its survey which captures extensive data on the state of the workforce. In its survey, professionals emphasize that job titles, skills pathways, experience, and educational backgrounds into cybersecurity work are wide-ranging and changing and are not well defined.[20]

*Lightcast*

Lightcast is a private sector provider of labor market analytics, pulling from online job postings and publicly available data on labor markets to analyze the state of the labor market and generate its own taxonomies. The Lightcast Occupation Taxonomy is a hierarchical structure with career areas as the most general classification, then broken down into occupation groups, occupations, and specialized occupations. Lightcast details eight occupation groups under its "Information and Computer Science" career area and then a set of occupations related to cybersecurity under "Network and Systems Engineering," including cybersecurity analysts, architects, consultants, engineers, administrators, technicians, and others.[21]

Lightcast offers a definition of cybersecurity systems in its skills taxonomy as

> "Cyber security [*sic*] systems involve the use of specialized tools and techniques to protect computer networks, systems, and devices from unauthorized access, attacks, and theft. It requires a unique set of skills, including knowledge of computer networks, programming languages, and security protocols. Cyber security experts must be able to identify and mitigate potential threats and implement preventative measures to ensure the safety and integrity of digital assets." It highlights a set of job titles requiring cybersecurity skills, including both core cybersecurity positions and other software roles that require cybersecurity skills.[22]

### *Synthesis of Private and Non-U.S. Government Taxonomies*

Among private sector and non-U.S. government agencies, the common features of cybersecurity workforce frameworks fall into one of three categories:

- International government frameworks, including those from the European Union and United Kingdom, which create a taxonomy of between 12 and 16 specific occupation titles that can be used by businesses or labor market data providers.
- Applications of the NICE Framework for specific uses, including uses by certificate providers and academic programs that are tied to federal government employment or federal funding programs, such as CyberCorps Scholarship for Service or NSA NCAE-C.
- Professional organizations and administrative data providers that conduct their own work, notably ISC2 and Lightcast. ISC2 conducts a survey of its membership, connecting it with membership data and labor market data to get a global look at the cybersecurity workforce. Lightcast collects data from job postings and profiles based on keywords related to cybersecurity work.

## Proposed Definition of the Cybersecurity Workforce

Existing frameworks and taxonomies of the cybersecurity workforce reveal a tension between a broad understanding of cybersecurity skills as outlined by the NICE Framework and a narrow set of core cybersecurity occupations, as seen in European or private sector research on the workforce. The NICE Framework emphasizes the need for a flexible taxonomy of work roles that can adapt to changing technologies and workplace needs. These frameworks show the need for a definition of the cybersecurity workforce that is layered, allowing for a focus on core cybersecurity occupations and activities alongside additional occupations involved in cybersecurity.[1]

[1] The definition follows the structure of the O*NET Content Model for an occupation, noting that a single occupation requires a mix of knowledge, skills, and abilities and is performed using a variety of activities and tasks. For more information, see the O*NET Content Model at https://www.onetcenter.org/content.html.

We propose a multilayered definition of the cybersecurity workforce driven by cybersecurity activities that includes both a core set of occupations, as well as cybersecurity-involved and cybersecurity-adjacent workers with responsibilities, tasks, knowledge, skills, and functions related to cybersecurity. The definition includes cybersecurity as an occupation for a small set of workers, and also includes skills and work activities. This follows the existing frameworks from organizations like NIST, ISC2, CompTIA, and the ECSF. Additionally, it parallels other NCSES research on work activities by considering workers' primary and secondary work activities. This multilayered approach thus remains consistent with the NICE Framework and other comprehensive flexible definitions, while also addressing the primary challenges of the NICE Framework.

The White House National Cyber Workforce and Education Strategy emphasizes the need for cybersecurity to be integrated across all jobs connected to cyber. Our proposed definition also reflects a trend in business and organizational practice where cybersecurity is becoming more closely integrated into technology teams, rather than operating as an isolated group.

***Proposed Definition***

*The cybersecurity workforce includes a core set of cybersecurity occupations focused on cybersecurity. Workers in other occupations where their primary, or secondary work activities include cybersecurity are also part of the core cybersecurity workforce. Cybersecurity-involved workers engage in cybersecurity work as a work activity that is not their primary or secondary work activity. Finally, workers not already identified as core or cybersecurity-involved workers whose tasks, skills, knowledge and/or jobs functions are related to cybersecurity are part of the cybersecurity adjacent workforce.*

In our proposed definition, we view the cybersecurity workforce as having a core, where cybersecurity is an occupation itself, or a primary or secondary, work activity, as seen in figure 1. Surrounding the core are cybersecurity-involved workers, which are those where cybersecurity is one of many work activities but not a primary or secondary one. Finally, cybersecurity-adjacent occupations on the periphery are those that are not directly related to cybersecurity but have some cybersecurity implications or cybersecurity related tasks, knowledge, and/or skills. The core cybersecurity workforce consists of:

- **Cybersecurity Occupations**: These are work roles where cybersecurity is the primary work activity and is explicitly at the core of the position. Primary occupations require tasks, knowledge, and skills from the NICE Framework to be central components of the position. Examples of primary cybersecurity occupations may include cybersecurity analysts and engineers, penetration testers, chief information security officers, and other direct cybersecurity occupations.

- **Primary and Secondary Cybersecurity Workers**: These are work roles where cybersecurity is an explicit portion of the position and a primary or secondary work activity, but the worker is not in a cybersecurity occupation. In other words, cybersecurity is a critical component of the work role. These roles also require multiple tasks, knowledge, and skills central to cybersecurity. Examples of primary and secondary cybersecurity workers may include lawyers working on cybersecurity law and compliance, database architects and managers, web developers and programmers, and other roles on development and IT teams that are increasingly integrated with cybersecurity teams.

We consider cybersecurity occupations and primary and secondary cybersecurity workers to be the core cybersecurity workforce. As we move forward, if desired, we suggest identifying ways to identify the percentage share of cybersecurity work activities to better understand the workforce.

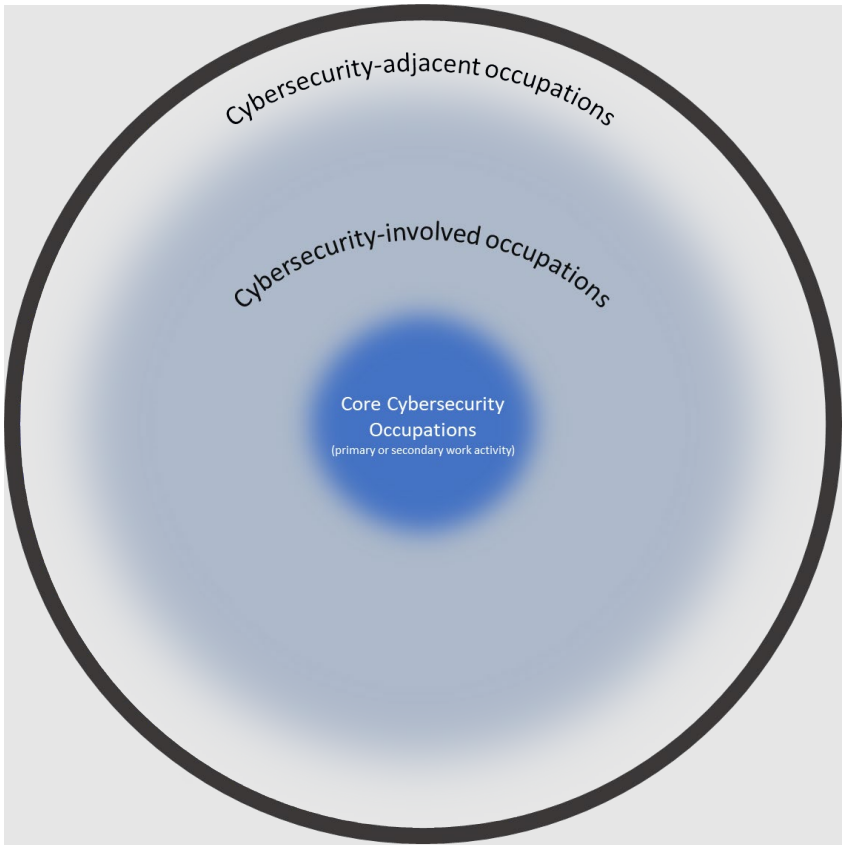
- **Cybersecurity-Involved Workers**: These are roles where cybersecurity is an explicit or other work activity, but where an employee may not rank it as a primary or secondary part of their regular work roles. Workers in these roles have a subset of tasks, knowledge, and skills from the NICE Framework. Examples of cybersecurity-involved occupations may include other computer and technology occupations, business and financial operations, legal and management roles, military and protective services, office and administrative support, and multiple types of engineers.

- **Cybersecurity-Adjacent Workforce**: These are roles where cybersecurity is not an explicit work activity but where there are cybersecurity implications or a small number of required tasks, knowledge, and/or skills from the NICE Framework central to the occupation. Workers in these roles incorporate cybersecurity into their jobs but are not directly involved in cybersecurity on a day-to-day basis.

These delineations between core (primary/secondary), involved, and adjacent occupations are a starting point, and are fuzzy. Identifying delineations is an area where more information is needed.

As noted in figure 1, we believe that under the current definition, the boundaries between core, involved and adjacent workers are blurry. Because cybersecurity activities span across occupations and current data does not fully capture the share of cybersecurity activities conducted by each occupation, we propose this as a framework to better refine our definition and identify opportunities for future data collection.

Figure 1. Proposed framework for cybersecurity occupations




Source(s):
National Center for Science and Engineering Statistics, Cybersecurity Workforce Data Initiative (CWDI).

The proposed definition serves to bridge the gap between the frameworks and taxonomies that focus on work roles, tasks, and skills and creates a definition to inform the next stages of the CWDI. Upcoming analysis of supply and demand, federal data sources, administrative data, and stakeholder workshops will inform, in greater detail, the data sources, classifications, and boundaries around the core, involved, and adjacent occupations.

## Key Takeaways and Conclusions

Based on our review of existing definitions of the cybersecurity workforce; examination of existing data; and interviews with public, private, and academic experts in cybersecurity, there is no comprehensive definition of who composes the cybersecurity workforce in the United States. Experts agree that cybersecurity jobs are defined by work roles, tasks, knowledge, and skills that can cut across job titles and industries. The nature of cybersecurity work is evolving quickly. This results in a landscape that includes frameworks and classifications rather than definitions. The lack of a standardized definition of the workforce is a limiting factor in addressing the national cybersecurity challenges and workforce gaps cited by employers and industry research.

In the United States, the NICE Framework is the industry standard for framing cybersecurity work roles in the public, private, and academic sectors, and its flexibility allows it to evolve, with a new revision in 2024. The NICE Framework reflects the crosscutting and skills-based nature of cybersecurity work. It contains nearly 1,000 tasks and over 200 knowledge and skill statements, allowing for a high level of detail about cybersecurity work. It translates directly to federal government employment through the 52 OPM codes for cybersecurity and is used to define the federal workforce. The NICE Framework has been directly applied to federal government employment through NICCS using the OPM codes from the NICE Framework.

While it is designed to be applied to the entire workforce, including the private sector, the highly complex taxonomy of the NICE Framework limits its application, and it is not directly linked to traditional labor market data from federal sources or industry providers. NIST emphasizes that the NICE Framework is a taxonomy for analysis, not a definition. Some existing definitions of the cybersecurity workforce, such as those cited by the OECD and by CyberSeek, rely on a crosswalk between the knowledge, skills, and tasks outlined in the NICE Framework and proprietary labor market data from Lightcast and online job postings. However, professional organizations and other administrative data providers do not rely on the NICE Framework and cite the lack of a clear definition and limited granular data from sources like BLS, O*NET, and the Census Bureau as a barrier to understanding the workforce and addressing immediate and long-term talent needs.

Our proposed definition of the cybersecurity workforce balances the tension between a broad set of cybersecurity work roles and skills like those emphasized by the NICE Framework and federal government agencies and a narrow, concise definition from the European Union, United Kingdom, and professional organizations. Our proposed definition establishes a core workforce and adjacent workforce, based on the work activities that align with the NICE Framework work roles and aligning them with traditional metrics in labor market research. We recognize that the threshold for the share of work activities in cybersecurity is preliminary and that additional research, including a survey, may be desired to set the boundaries between core, adjacent, and non-cybersecurity jobs, but more information is needed before such boundaries are practical. This will help to fill the need cited by public, private, and academic experts in the field for reliable, independent data from a secondary source like NCSES to understand the cybersecurity workforce.

## Glossary

This glossary provides definitions for agencies, organizations, statistical standards, and computing terms pertaining to the cybersecurity workforce.

**Artificial Intelligence (AI):** Technology that makes it possible for machines to learn from experience, adjust to new inputs, and perform human-like tasks.

**Bureau of Labor Statistics (BLS):** A federal statistical agency of the Department of Labor that collects and analyzes data to measure labor market activity, working conditions, price changes, and productivity in the economy to support public and private decision making.

**Chief Information Security Officer (CISO):** A senior-level executive who oversees an organization's information, cyber, and technology security and whose responsibilities include developing, implementing, and enforcing security policies to protect critical data.

**Classification of Instructional Programs (CIP):** A taxonomy developed by the Department of Education to support the accurate tracking and reporting of fields of study and program completion activity across postsecondary education institutions.

**Computing Technology Industry Association (CompTIA):** A professional organization that provides education, training, and certifications to computing technology professionals, as well as research and information on a variety of technology topics.

**Creating Helpful Incentives to Produce Semiconductors (CHIPS) and Science Act of 2022:** Legislation providing funding to carry out research and other activities to boost semiconductor production in the United States, including mandating NCSES to conduct a feasibility study on the collection of data on the cybersecurity workforce.

**Cybersecurity & Infrastructure Security Agency (CISA):** An agency within the Department of Homeland Security that leads and coordinates federal efforts to understand, manage, and reduce risk to cyber and physical infrastructure.

**Cybersecurity Workforce Data Initiative (CWDI):** A federal initiative mandated by the CHIPS and Science Act of 2022 to gather information about the cybersecurity workforce and to assess the feasibility of producing national estimates and statistical information on the cybersecurity workforce.

**CyberCorps Scholarship for Service (SFS):** A federal program supported by OPM, NSF, and DHS that provides scholarships for up to three years of cybersecurity undergraduate or graduate education in return for which recipients must agree to work after graduation for the government in a position related to cybersecurity for a period equal to the length of the scholarship.

**CyberSeek:** A collaboration effort between Lightcast, NIST's NICE Framework, and CompTIA, this set of interactive online tools showing data such as number of open cybersecurity jobs by region, average salaries, certifications, and career pathways using data scraped from government employment data, online job postings, and social media profiles.

**Department of Defense (DOD):** The government agency that provides the military forces needed to deter war and to protect the security of the United States.

**Department of Homeland Security (DHS):** The Department of Homeland Security (DHS) works to improve the security of the United States. The Department's work includes customs, border, and immigration enforcement, emergency response to natural and manmade disasters, antiterrorism work, and cybersecurity.

**European Cybersecurity Skills Framework (ECSF):** A practical tool to support the identification and articulation of tasks, competences, skills and knowledge associated with the roles of European cybersecurity professionals. It is the European Union’s reference point for defining and assessing relevant skills, as defined in the Cybersecurity Skills Academy, which was recently announced by the European Commission.

**Information Systems Security Association (ISSA):** A not-for-profit, international organization of information security professionals and practitioners that provides educational forums, publications, and peer interaction opportunities that enhance the knowledge, skill, and professional growth of its members.

**Information Technology (IT):** Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

**International Information System Security Certification Consortium (ISC2):** The world’s leading member association for cybersecurity professionals that provides training, education, certification, networking, and advocacy.

**Lightcast:** An organization specializing in the collection and big-data analysis of information on the labor market that collects real-time data to create a database with information about job postings, occupations, skills in demand, and career pathways.

**National Center for Academic Excellence in Cybersecurity (NCAE-C)** A program managed by NSA's National Cryptologic School. NCAE-C program aims to create and manage a collaborative cybersecurity educational program with community colleges, colleges, and universities.

**National Initiative for Cybersecurity Careers and Studies (NICCS):** A national online resource hub for cybersecurity training, education, and career information managed by CISA within the Department of Homeland Security.

**National Institute for Standards and Technology (NIST):** An agency whose purpose is to create a first-rate measurement infrastructure, advancements in measurement science, and equitable standards to enhance the industrial competitiveness and economic security of the United States. NIST developed and periodically updates the NICE Framework.

**National Security Agency (NSA):** A support agency of DOD that leads the government in cryptology, encompasses both signals intelligence insights and cybersecurity products and services, and enables computer network operations to gain a decisive advantage for the nation and our allies.

**NICE Framework:** A taxonomy created by NIST and formerly known as the National Initiative for Cybersecurity Education (NICE) Framework that describes cybersecurity work roles and the tasks, knowledge, and skills that are needed to perform cybersecurity work. The most recent NICE Framework updates were released in 2024.

**North American Industry Classification Systems (NAICS):** The standard used by federal statistical agencies in classifying business establishments for the purpose of collecting, analyzing, and publishing statistical data related to the business economy, allowing for comparability in business statistics among North American countries.

**Occupational Employment and Wage Statistics (OEWS):** A BLS project that produces annual employment and wage estimates for approximately 830 occupations at the national, state, and metropolitan levels.

**The Occupational Information Network (O*NET):** A hierarchical database maintained by the Department of Labor that describes occupational and worker characteristics, as well as knowledge, skills, abilities, and tasks for over 900 occupations.

**Office of Personnel Management (OPM):** The chief human resources agency and personnel policy manager for the federal government.

**Open Worldwide Application Security Project (OWASP):** A nonprofit foundation that provides education, training, free informational forums and documents, and community-led open-source projects dedicated to creating, operating, and maintaining secure software applications.

**Organisation for Economic Co-operation and Development (OECD):** An international organization that works to provide a knowledge hub for data; analysis; and exchange of experiences, best practices, and policy advice in order to find solutions to a range of social, economic, and environmental challenges.

**Personal Computer (PC):** a digital computer designed for use by only one person at a time.

**Standard Occupation Code (SOC):** A federal statistical standard taxonomy developed and maintained by the Department of Labor and used by federal agencies to classify all workers into one of 867 detailed occupational categories for the purpose of collecting, calculating, or disseminating data.

**Tasks, Knowledge, and Skills Statements (TKS statements):** Building blocks of the NICE Framework model that allow for describing work in a way that can assist with defining competencies, work roles, and teams; assessing a workforce; conducting learning and professional development; and recruiting and hiring.

# Appendix A: Existing Classifications of the Cybersecurity Workforce

This section catalogs examples of leading U.S. federal and nongovernment actors' classifications, taxonomies, frameworks and/or definitions of cybersecurity work and its workforce. While not universally comprehensive, this section captures the general approach to classifying the cybersecurity workforce through identifying cybersecurity functions and skills. As this section will show, there are several working classifications that capture components of the cybersecurity workforce focusing on information technology (IT) professionals and defense applications from agencies like the Department of Defense (DOD) and the Department of Homeland Security (DHS) but that do not capture the diverse cybersecurity roles in industries like health care, transportation, utilities, manufacturing, and others that require cybersecurity skills.

Of the existing frameworks, the NICE Workforce Framework for Cybersecurity (NICE Framework) from the National Institutes for Standards and Technology (NIST) is the most thoroughly developed and features prominently in all federal initiatives that address cybersecurity work. The definitions from organizations like DOD and the Cybersecurity & Infrastructure Security Agency (CISA) focus on workers directly employed in cyber defense work. Others (such as the 2023 White House definition) include cybersecurity as part of a broader definition of cyber work that includes workers who use cyber technologies across industries, reflecting the broad reach and demand for cyber skills in a range of industries.

## U.S. Government

### *NIST: NICE Framework*

First released in 2012, the NICE Framework is an effort to create shared baseline framework of cybersecurity functions and worker capabilities.[23] NIST has refined the NICE Framework through several iterations since 2012, and it is the most commonly cited framework among public- and private sector programs and reports related to the cybersecurity workforce. Federal cybersecurity workforce initiatives, including those from DOD, CISA, the White House, the National Initiative for Cybersecurity Careers and Studies (NICCS), and the Office of Personnel Management (OPM), all reference the NICE Framework. NIST emphasizes that the NICE Framework is a taxonomy for analysis but is not intended to be a comprehensive definition of the cybersecurity workforce.

Cybersecurity Workforce: "Shorthand for a workforce with work roles that have an impact on an organization's ability to protect its data, systems, and operations. Included are new work roles that have been known traditionally as IT security roles. Those roles have been added to this workforce framework to highlight their importance to the overall cybersecurity posture of an organization."[24]

### *NIST: CyberSeek*

A partnership of NIST, certification provider Computing Technology Industry Association (CompTIA), and workforce analysis company Lightcast, CyberSeek is an effort to measure the size of the cybersecurity workforce at different geographic levels of aggregation, capture the gap between supply and demand for cybersecurity workers, and identify career pathways (https://www.cyberseek.org/ ).

Cybersecurity: "Commonly refers to the tools and techniques used to protect technology devices, the data they contain, and the functions they perform from people who want to steal, damage, or misuse them. This includes normal features of modern life that you deal with every day, like the passwords that protect your phone, your computer, and your various online accounts, as well as the practices and defenses to keep everything safe."[25]

### *National Science Foundation: CyberCorps*

The CyberCorps Scholarship for Service provides financial support to undergraduate and graduate students who agree to work for the federal government upon completion of their degrees. The first cohort graduated in 2001, and enrollment for the last several years has surpassed 1,000 students annually.

Cybersecurity: "Achieving a truly secure cyberspace requires addressing both challenging scientific and engineering problems involving many components of a system, and vulnerabilities that stem from human behaviors and choices. Examining the fundamentals of security and privacy as a multidisciplinary subject can lead to fundamentally new ways to design, build, and operate cyber systems; protect existing infrastructure; and motivate individuals to learn about cybersecurity."[26]

### *DHS: CISA*

DHS's CISA supports NICCS, which includes online resources for training, careers, and education. NICCS supports education, workforce development, and career readiness for education, federal, nonfederal government, private sector, and individuals in the cybersecurity sector.[27]

Cybersecurity: "Members of the workforce with roles and responsibilities that have an impact on an organization's ability to protect its data, systems, and operations."[28]

The DHS CISA definition is based on the NICE Framework but takes an expansive view. "Cybersecurity knowledge, skills, and abilities are applied not only by individuals operating and defending complex technical systems vital to organizations, but also by anyone in the organization who has a role that can reduce the organization's cybersecurity risk."[29]

### *OPM: Guidance for Cybersecurity Positions*

The OPM guidance for cybersecurity was defined in 2018 and is based on the NICE Framework and references the 2009 White House Cyberspace Policy Review. OPM guidance has evolved since the December 2015 Federal Cybersecurity Workforce Assessment Act, and the current definitions do not yet have an agreement on terminology for cyber and cybersecurity workforce jobs. Based on the existing definitions, OPM provides a set of occupation codes within the federal framework that capture one component of the NICE Framework, highlighted in table A-1.

Table A-1
OPM position cyber codes related to NICE Framework
(Codes)

| Category | Specialty Area | Work Role | OPM Code |
|---|---|---|---|
| Securely Provision | Risk Management | Authorizing Official/Designating Representative | 611 |
| | | Security Control Assessor | 612 |
| | Software Development | Software Developer | 621 |
| | | Secure Software Assessor | 622 |
| | Systems Architecture | Enterprise Architect | 651 |
| | | Security Architect | 652 |
| | Technology R&D | Research & Development Specialist | 661 |
| | Systems Requirements Planning | Systems Requirements Planner | 641 |
| | Test and Evaluation | System Testing and Evaluation Specialist | 671 |
| | Systems Development | Information Systems Security Developer | 631 |
| | | Systems Developer | 632 |

OPM = Office of Personnel Management

Note(s):
Full list of work roles available at https://dw.opm.gov/datastandards/referenceData/2273/current?index=C.

Source(s):
OPM Presentation on Cyber Workforce for NCSES CWDI, December 2023.

Cybersecurity: "Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure."[30]

### *DOD: Cyber Workforce Framework*

Based on the NICE Framework, the DOD Cyber Workforce Framework defines cybersecurity personnel using 7 categories, 33 specialty areas, and 54 work roles with a set of skills and responsibilities.

Cybersecurity Personnel: "Personnel who secure, defend, and preserve data, networks, net-centric capabilities, and other designated systems by ensuring appropriate security controls and measures are in place, and taking internal defense actions. This includes access to system controls, monitoring, administration, and integration of cybersecurity into all aspects of engineering and acquisition of cyberspace capabilities."[31]

### *The Bureau of Labor Statistics' and Occupational Information Network*

The Bureau of Labor Statistics (BLS) defines occupations using a set of Standard Occupational Classification (SOC) codes that define job titles, wages, credentials, education needed, and industry and geographic breakdowns. SOC code 15-1212 for Information Security Analysts, a subset of the computer and mathematical occupations, is one example of a cybersecurity job type, with an estimated 163,000 jobs in the United States paying a median annual wage of $112,000 per year.[32]

BLS's Occupational Information Network (O*NET) defines SOC 15-1212 as those who "plan, implement, upgrade, or monitor security measures for the protection of computer networks and

information. Assess system vulnerabilities for security risks and propose and implement risk mitigation strategies. May ensure appropriate security controls are in place that will safeguard digital files and vital electronic infrastructure. May respond to computer security breaches and viruses."[33] O*NET draws on data from BLS to define wages and growth projections in the occupation.

### *White House: National Cyber Workforce and Education Strategy (2023)*

The most recent definition released by the White House expands beyond cybersecurity to define the broader cyber workforce. While still heavily focused on the security of cyber resources, the White House definition includes jobs that build and operate cyber systems.

Cyber Workforce: "Those who design, build, secure, operate, analyze, protect, and defend cyberspace resources. It encompasses those who work in the frequently overlapping fields of technology manufacturing, software development, IT, operational technology /industrial control systems, cybersecurity, cyberspace operations, cyber investigations and prosecutions, some intelligence roles, and related research and development. The cyber workforce also includes those who lead or support work in these fields through activities that include governance, law and compliance, policy, strategy and planning, privacy, acquisition, program and program management, and workforce management and development."[34]

## U.S. Nonfederal

### *CompTIA*

CompTIA (https://www.comptia.org/) is a professional organization that is among the global leaders in the cybersecurity industry. The CompTIA Security+ certification is among the most frequently cited credentials for cybersecurity jobs.[35] CompTIA partnered with Lightcast in developing the NIST-sponsored CyberSeek, a frequently cited resource for measuring the size of the cybersecurity workforce at the state and local levels and the gap between the regional demand and supply of cybersecurity workers. CompTIA's involvement in CyberSeek highlights the importance of CompTIA in the landscape of cybersecurity professional organizations.

CompTIA does not provide its own definition of the cybersecurity workforce but does refer to the NICE Framework and CyberSeek in some of its public-facing statements. While the CyberSeek definition of cybersecurity noted above provides some insight, a more thorough assessment of the underlying data methodology is required to flesh out CompTIA's operative definition of the cybersecurity workforce. Additional insight on the parameters of the cybersecurity workforce could be drawn from the requirements for CompTIA cybersecurity certifications, but these certifications do not capture many peripheral roles that include elements of cybersecurity work.

### *Lightcast*

Lightcast is a private sector provider of labor market analytics, pulling from online job postings and publicly available data on labor markets to analyze the state of the labor market and generate its own taxonomies. The Lightcast Occupation Taxonomy is a hierarchical structure with career areas as the most general classification, followed by occupation groups, occupations, and specialized occupations. Lightcast details eight occupation groups under its "Information and Computer Science" career area and then a set of occupations related to cybersecurity under "Network and Systems Engineering," including cybersecurity analysts, architects, consultants, engineers, administrators, technicians, and others.[36]

Lightcast offers a definition of cybersecurity systems in its skills taxonomy, as "Cyber security [*sic*] systems involve the use of specialized tools and techniques to protect computer networks, systems, and

devices from unauthorized access, attacks, and theft. It requires a unique set of skills, including knowledge of computer networks, programming languages, and security protocols. Cyber security experts must be able to identify and mitigate potential threats and implement preventative measures to ensure the safety and integrity of digital assets." It highlights a set of job titles requiring cybersecurity skills, including both core cybersecurity positions and other software roles that require cybersecurity skills.[37]

### *Information Systems Security Association*

The Information Systems Security Association, or ISSA International, is a professional organization that includes information security professionals and practitioners. According to its website, it provides educational forums, publications, and peer interaction. In 2023, it counted 6,523 general members across 137 U.S. chapters and 22 international chapters. ISSA hosts events and conferences and supports thought leadership and peer learning.[38]

ISSA has not released a single definition of the cybersecurity workforce but has developed a Cybersecurity Career Lifecycle to reflect the range of experience and skills that are part of the field.[39] Notably, the Lifecycle includes "Pre-Professionals," signaling a recognition that even professionals without formal cybersecurity titles or training can be considered part of the extended cybersecurity workforce. As with other cybersecurity certifications, examining the content and requirements for ISSA certification programs can provide some elements of core cybersecurity functions but would not capture the full range of roles that can be considered part of the cybersecurity workforce.

### *The International Information System Security Certification Consortium*

The International Information System Security Certification Consortium (ISC2) is a professional organization that offered its first certification in 1994 and counts over 500,000 members worldwide. ISC2 conducted its first annual survey in 2019 to estimate the size of the cybersecurity workforce and skills needs in the industry. In 2023, it estimated over 1.3 million cybersecurity workers in the United States based on surveys asking respondents for the number of cybersecurity professionals employed in their organizations, estimates from third parties, and extrapolating previous years' estimates.[40]

ISC2 relies on multiple third-party sources and survey respondents' own understandings of what counts as a cybersecurity workforce, indicating a fluid understanding of the cybersecurity workforce. ISC2's 2023 Cybersecurity Workforce Study noted a shift in points of entry into the field, with more people entering the profession without having previously served in an IT role. Like the ISSA Cybersecurity Career Lifecycle, this finding may indicate an increasingly porous boundary around the cybersecurity workforce.

### *Joint Task Force on Cybersecurity Education*

The Joint Task Force on Cybersecurity Education, launched in September 2015, focuses on developing curricula for education efforts. The task force included a mix of academic and private sector actors in cybersecurity who developed a template for cybersecurity education. The Cybersecurity Curricular Guidelines were released in 2017 and have been cited by outside authors as an exemplar for the definition of the workforce.

Cybersecurity: "Computing-based discipline involving technology, people, information, and processes to enable assured operations. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management in the context of adversaries."[41]

### *N2K*

A merger of CyberVista and CyberWire, N2K is a workforce intelligence company that provides workforce intelligence and training, including courses to prepare for common cybersecurity certifications offered by organizations like CompTIA, ISSA, and ISC2. In addition to training for individual cybersecurity professionals, N2K offers team-level certifications to address consistent knowledge gaps. Like other private cybersecurity workforce intelligence and training providers, N2K does not provide a single definition of the cybersecurity workforce but instead references the NICE Framework and offers services to help entities hire and develop career pathways for cyber/IT employees.[42] N2K identifies a challenge in many hiring processes where "job descriptions are too generalized, overcomplicated, or outdated."[43] Given the lack of clear boundaries around the cybersecurity workforce, N2K offers workforce mapping services to assess current capabilities, gaps, and create organizational charts that provide clearer pathways within an organization's "cyber/IT" workforce.[44]

### *U.S. State Government Initiatives*

Various state initiatives in the United States, including the Virginia Commonwealth Cyber Initiative (CCI), Cyber Florida, the California Cyber Institute, and Carolina Cyber Network, support research, workforce development, and coordination for cybersecurity education and workforce development. They rely on a mix of definitions, including the NICE Framework.

Cybersecurity: The Virginia CCI defines cybersecurity as a "working definition that focuses on subject areas at the intersection of data, security, and autonomy [where] a range of high-value employee skill sets can be identified, such as cryptography, compliance with legal standards, information security, computer network defense, and forensics."[45] CCI cites CyberSeek data for the size of the cybersecurity workforce and cybersecurity workforce gap.

## International

### *Organisation for Economic Co-operation and Development*

The Organisation for Economic Co-operation and Development (OECD) released its 2023 report, *Building a Skilled Cyber Security Workforce in Five Countries: Insights from Australia, Canada, New Zealand, United Kingdom, and United States*, drawing data from online job postings and the data firm Lightcast. OECD researchers classified a subset of SOC codes from BLS and broke them out into groups, including analysts, architects and engineers, auditors and advisors, and managers.[46] The data referenced relies on a mix of Lightcast's methodology of text analytics and a set of SOC codes using standard labor market data.

### *European Union Agency for Cybersecurity: European Cybersecurity Skills Framework*

The European Cybersecurity Skills Framework defines 12 cybersecurity work roles that are typically required for organizations with cybersecurity professionals. The framework was designed to be easily understood and comprehensive enough to provide appropriate in-depth cybersecurity insights, as well as flexible enough to allow customization based on each user's needs. The framework focuses on core cybersecurity roles but is intended to be simple enough to be used by all professionals incorporating cybersecurity into their organization.[47]

## Notes

[1] Office of the National Cyber Director, Executive Office of the President. 2023. *National Cyber Workforce and Education Strategy: Unleashing America's Cyber Talent.* https://www.whitehouse.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf.

[2] Higgins M. 2022. The History of Cybersecurity. *NordVPN.* https://nordvpn.com/blog/history-of-cybersecurity/ . Pattison-Gordon J. 2021. Through the Years: A Broad Look at Two Decades in Cybersecurity." *Government Technology* https://www.govtech.com/security/through-the-years-a-broad-look-at-two-decades-in-cybersecurity .

[3] Office of the National Cyber Director, Executive Office of the President. 2023. *National Cyber Workforce and Education Strategy: Unleashing America's Cyber Talent.* https://www.whitehouse.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf.

[4] Office of the National Cyber Director, Executive Office of the President (2023).

[5] Prior to 2023, NIST referred to the NICE Framework as the National Initiative for Cybersecurity Education (NICE) Framework. See National Institute of Standards and Technology. 2023. NICE Frequently Asked Questions. *NICE*. Available at https://www.nist.gov/itl/applied-cybersecurity/nice/about/frequently-asked-questions.

[6] National Institute of Standards and Technology. N.d. *NICE.* Available at https://www.nist.gov/itl/applied-cybersecurity/nice.

[7] National Institute of Standards and Technology. 2023. NICE Framework History and Change Logs. *NICE Framework Resource Center.* Available at https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-history-and-change-logs.

[8] Workforce Framework for Cybersecurity (NICE Framework), May 2023. https://www.nist.gov/system/files/documents/2023/06/05/NICE%20Framework%20%28NIST%20SP%20800-181%29_one-pager_508Compliant.pdf.

[9] Office of Personnel Management (OPM). N.d. *Guidance for Cybersecurity Positions.* Available at https://www.opm.gov/cyber-careers/cyber-careers-hiring/. OPM. 2018. *Interpretive Guidance for Cybersecurity Positions.* Available at https://www.opm.gov/policy-data-oversight/classification-qualifications/reference-materials/interpretive-guidance-for-cybersecurity-positions.pdf.

[10] NICCS Cyber Career Pathways Tool. 2024. Available at https://niccs.cisa.gov/workforce-development/cyber-career-pathways-tool.

[11] OPM (2018:6).

[12] Office of the National Cyber Director, Executive Office of the President (2023).

[13] CompTIA. N.d. CompTIA Security+ Certification. Available at https://www.comptia.org/certifications/security .

[14] ISC2. 2023. *ISC2 Cybersecurity Workforce Study: How the Economy, Skill Gap, and Artificial Intelligence are Challenging the Global Cybersecurity Workforce.* Available at https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf .

[15] Information Systems Security Association. 2023. *Cybersecurity Career Lifecycle®*. Available at https://www.issa.org/cyber-security-career-lifecycle/.

[16] N2K. 2023. *Workforce Framework for Cybersecurity.* Available at https://www.cybervista.net/nice-cybersecurity-workforce-framework/.

[17] Cal Poly California Cybersecurity Institute. 2022. NICE Framework Success Story: California Cyber Innovation Challenge. *NIST NICE Framework Resource Center*. Available at https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-success-story.

[18] European Union Agency for Cybersecurity. 2022. *European Cybersecurity Skills Framework (ECSF) - User Manual*. Available at https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf.

[19] European Commission (ESCO). N.d. European e-Competence Framework (e-CF). *ESCOpedia*. Available at https://esco.ec.europa.eu/en/about-esco/escopedia/escopedia/european-e-competence-framework-e-cf.

[20] ISC2. 2023. *ISC2 Cybersecurity Workforce Study: How the Economy, Skill Gap, and Artificial Intelligence are Challenging the Global Cybersecurity Workforce.* Available at https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf.

[21] Lightcast. N.d. Lightcast Occupation Taxonomy. 2023. Available at https://lightcast.io/lot/occupations/categories.

[22] Lightcast. N.d. *Cyber Security Systems.* Available at https://lightcast.io/open-skills/skills/ESD47E9C4D6597F149D7/cyber-security-systems.

[23] National Institute of Standards and Technology. 2023. NICE Framework History and Change Logs. *NICE Framework Resource Center*. Available at https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-history-and-change-logs.

[24] National Institute of Standards and Technology. 2020. *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.* Available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.

[25] CyberSeek. 2023. *What Is Cybersecurity*. Available at https://www.cyberseek.org/.

[26] National Science Foundation. 2023. *CyberCorps Scholarship for Service (SFS).* Available at https://new.nsf.gov/funding/opportunities/cybercorps-scholarship-service-sfs.

[27] National Initiative for Cybersecurity Careers and Studies. 2023. Available at https://niccs.cisa.gov/.

[28] Department of Homeland Security, Cybersecurity & Infrastructure Security Agency (DHS/CISA). 2020. Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future. Page 21. Available at https://www.cisa.gov/sites/default/files/publications/eo_wf_report_to_potus.pd_.pdf.

[29] DHS/CISA (2020:24).

[30] Office of Personnel Management. 2018. *Interpretive Guidance for Cybersecurity Positions: Attracting, Hiring, and Retaining a Federal Cybersecurity Workforce*. Available at https://www.opm.gov/policy-data-oversight/classification-qualifications/reference-materials/interpretive-guidance-for-cybersecurity-positions.pdf.

[31] Department of Defense. 2023. *DoD Cyber Workforce Framework.* Available at https://public.cyber.mil/wid/dcwf/.

[32] Bureau of Labor Statistics. 2022. *Occupational Outlook Handbook: Information Security Analysts.* Available at https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.

[33] O*NET Online. 2023. *Information Security Analysts.* Available at https://www.onetonline.org/link/summary/15-1212.00.

[34] Executive Office of the President, Office of National Cyber Director. 2023. *National Cyber Workforce and Education Strategy: Unleashing America's Cyber Talent.* Washington, DC: White House. Available at https://www.whitehouse.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf.

[35] CompTIA. N.d. CompTIA Security+ Certification. Available at https://www.comptia.org/certifications/security.

[36] Lightcast. N.d. Lightcast Occupation Taxonomy. 2023. Available at https://lightcast.io/lot/occupations/categories.

[37] Lightcast. N.d. *Cyber Security Systems.* Available at https://lightcast.io/open-skills/skills/ESD47E9C4D6597F149D7/cyber-security-systems.

[38] ISSA International. 2023. *Annual Membership Meeting* (Slideshow). Available at https://issawebstite.wpenginepowered.com/wp-content/uploads/2023/09/2023-Annual-Meeting-final.pdf.

[39] ISSA International. 2023. *Cybersecurity Career Lifecycle.* Available at https://www.issa.org/cyber-security-career-lifecycle/.

[40] ISC2. 2023. *ISC2 Cybersecurity Workforce Study: How the Economy, Skill Gap, and Artificial Intelligence are Challenging the Global Cybersecurity Workforce.* Available at https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf.

[41] Association for Computing Machinery. 2017. *Cybersecurity Curricular Guideline: CSEC 2017.* https://cybered.acm.org/.

[42] N2K. 2023. *Workforce Framework for Cybersecurity.* Available at https://www.cybervista.net/nice-cybersecurity-workforce-framework/.

[43] N2K. 2023. *How to Hire, Develop, and Keep Skilled Cybersecurity Talent with Workforce Intelligence.* Available at https://www.n2k.com/strategy-guide.

[44] N2K. 2023. *Maximize Your Talent Investment with Cyber Talent Insights.* Available at https://www.n2k.com/talent-insights.

[45] Commonwealth Cybersecurity Initiative. 2023. *Workforce Development.* Available at https://cyberinitiative.org/talent-development.html.

[46] Organisation for Economic Co-operation and Development (OECD), Lightcast. 2023. *Building a Cyber Security Workforce in Five Countries: Insights from Australia, Canada, New Zealand, United Kingdom, and United States.* Available at https://doi.org/10.1787/5fd44e6c-en.

[47] European Union Agency for Cybersecurity (ENISA). 2022. *European Cybersecurity Skills Framework (ECSF) User Manual. Available* at https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf.