Cybersecurity Workforce Supply and Demand Report

May 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.

Cybersecurity Workforce Data Initiative:

Cybersecurity Workforce Supply and Demand Report

May 2024

Abstract

In the past five years, federal, academic, and private sector research emphasizes a gap between the demand for and the supply of skilled workers in cybersecurity in the United States and worldwide. Efforts to quantify the cybersecurity workforce and the supply and demand for cybersecurity workers have been limited to private sector and administrative data providers using a mix of methodologies, taxonomies, and definitions of cybersecurity workers. Using the proposed definition of the cybersecurity workforce from the previously published definitions report, which combines work activities and job titles, this report proposes a methodology to quantify and estimate the size of the cybersecurity workforce and provides corresponding estimates of a lower bound and upper bound of values that could potentially constitute the current workforce, workforce pipeline, short-term demand, and long-term demand. The report then assesses the various sources of data available and some of the limitations and drawbacks of each. Because the definition of a cybersecurity job varies widely, the existing estimates for the supply of and demand for cybersecurity workers vary depending on the definition and criteria used. The analysis in this report shows that the cybersecurity workforce currently ranges between 164,000 and 3,492,000 workers out of an estimated total of 161,052,000 workers in the United States. Additionally, the workforce pipeline is growing quickly, with new graduates at every level. This rapid growth could constitute evidence that the United States does not lack a quantity of new workers and that, instead, the workforce gap is driven by other factors, such as an unclear pipeline and lack of clear data about the skills, knowledge, and credentials needed in the workforce. Short-term and long-term demand remain strong and are projected to outpace national job growth over the next decade.

Suggested Citation

Hogan M, Lilienthal K, 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 Supply and Demand 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
Kaitlin Lilienthal
Alison Bean de Hernandez
Patrick McHugh
Caren A. Arbeit
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; RTI editors, August Gering and Cat Olenick, for content and editorial feedback on earlier versions of this report; and Mahmoud Elkasabi, Joseph McMichael, and Matt Williams for their substantive contributions to the 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

Across the federal, academic, and private sectors, researchers and leaders emphasize a gap between the demand for cybersecurity workers and the supply of workers available. As part of the Cybersecurity Workforce Data Initiative (CWDI), we reviewed existing research and estimates of the size of the workforce in cybersecurity. This review included the current supply of workers (i.e., employees currently in cybersecurity occupations, unemployed individuals recently in cybersecurity occupations, and new graduates from postsecondary programs), the short-term demand for workers (i.e., current job openings), and the long-term demand for workers (i.e., projections of future growth). The CWDI's proposed definition of the cybersecurity workforce includes both core cybersecurity workers and cybersecurity-adjacent workers. This report focuses on the core, identifying those who have explicit cybersecurity jobs and those with cybersecurity as a primary or secondary work role. In this report, we propose a methodology to capture a range of values, estimating a lower bound and upper bound for supply and providing various estimates of short-term and long-term demand.

According to existing estimates from nonfederal professional organizations and administrative data providers, the current size of the cybersecurity workforce ranges between 1,180,000 and 1,340,000 workers, depending on the source of the estimate. Federal sources, such as the Census Bureau and the Bureau of Labor Statistics (BLS), use the Standard Occupational Classification (SOC) system to define occupations in the workforce, which does not necessarily line up with existing frameworks or definitions of cybersecurity work. Our methodology links nine SOC codes to cybersecurity work, including one key and eight additional core SOC codes that may have primary or secondary work roles in cybersecurity. We looked at data from the BLS Occupational Employment and Wage Statistics program, the Census Bureau's American Community Survey, and the National Center for Science and Engineering Statistics' (NCSES) National Survey of College Graduates (NSCG). Based on this methodology, the size of the workforce may range from approximately 164,000 workers to 3,492,000 workers. The wide range of estimates is due to differences in the definition of a cybersecurity worker (including only workers in the one key SOC occupation will produce a lower number than including workers in all nine identified SOC occupations) and differences in sampling and methodology among data sources. Unemployment rates among cybersecurity workers are low, and the number of unemployed workers in the labor force seeking employment ranges from 2,500 to 74,000 individuals.

The inflow of new workers into cybersecurity is difficult to estimate because of the range of postsecondary programs that may funnel workers into cybersecurity careers and the multiple potential pathways into cybersecurity work. As we learned through interviews about the cybersecurity workforce, workers may enter cybersecurity work roles later in their careers and may come from a variety of backgrounds, such as computer science and engineering. Our methodology used 26 Classification of Instructional Programs (CIP) codes that, according to BLS and the Department of Education's CIP-to-SOC crosswalk, map to the nine key and core cybersecurity SOC codes. According to data from the Integrated Postsecondary Education Data System, in 2022, there were about 25,000 degrees and certificates awarded in CIP code 11.1003 (Computer and Information Systems Security/Auditing/Information Assurance), but nearly 259,000 degrees and certificates were awarded in all 26 CIP codes related to cybersecurity. This wide range of values is due to the variety of degree and certificate programs that may supply cybersecurity workers. The total number of degrees and certificates awarded in Computer and Information Systems Security/Auditing/Information Assurance increased by 271% from 2012 to 2022, and the total number of awards in cybersecurity-related programs doubled over that decade.

Estimates of the current open positions posted on commercial job sites for cybersecurity range from 14,000 to 55,000 jobs, depending on the source and search terms. For example, searching for job postings with "cybersecurity" in the title yields fewer job openings than searching for job postings that contain cybersecurity knowledge, skills, and work roles in the job description. With nearly 1,000 knowledge, skills, and work roles in the Workforce Framework for Cybersecurity—commonly referred to as the NICE Framework—it can be difficult to narrow the criteria for searching. For example, there are more than 100,000 jobs requiring data security skills currently posted on commercial job sites. Federal job postings make up a small percentage of these jobs. Over the next 10 years, BLS projects that the total number of cybersecurity jobs may increase by between 10% and 31%, outpacing the projected national job growth rate of 3% over the next decade and ranking among the fastest-growing as projected by BLS.

Although this report attempts to quantify current cybersecurity workers, unemployed individuals and recent graduates potentially seeking cybersecurity jobs, and the number of current open jobs requesting cybersecurity professionals, there are still several gaps in our knowledge about supply and demand in the cybersecurity workforce. For example, more information is needed to understand if graduates are seeking jobs connected to their degree, as according to NSCG data, only 46% of college graduates in cybersecurity core occupations had a degree that was closely related to their field of work. There is a lack of information about the knowledge, skills, and credentials required for cybersecurity work, the on-ramps into cybersecurity jobs, and the source of a potential mismatch between the work experience sought by employers versus the experience held by new graduates.

The research and data, along with interviews conducted as part of the CWDI, highlight a lack of entry-level openings in cybersecurity and unclear on-ramps into the profession. Interviewees emphasized that job openings frequently require work experience in an adjacent computer science job, plus additional certifications or training on top of a postsecondary degree. More than two-thirds of workers in cybersecurity fields hold a bachelor's degree or higher, and of those, nearly half have a degree in a field not directly related to their current occupation. Industry leaders point out that experience levels, work roles, credentials, and certifications requested vary widely and are not consistent across cybersecurity jobs, making it difficult to operationalize data. To better operationalize data on the workforce in the future, we recommend systematically linking the knowledge, skills, and work roles in the NICE Framework to the Occupational Information Network, or O*NET, to better understand occupations. This will improve the presence of the cybersecurity workforce in future SOC code revisions and better classify cybersecurity work in future revisions to CIP codes. We also recommend that NCSES examine if existing NCSES survey items could be adapted to help measure the cybersecurity workforce.

Introduction

Understanding the number and characteristics of current cybersecurity workers and open cybersecurity jobs is critical to matching prospective workers with unfilled jobs. Filling open jobs with skilled workers will improve the cybersecurity posture of the United States. However, because the cybersecurity workforce is not defined by a finite set of credentials, job titles, occupation codes, industry codes, or professional licenses, it is challenging to provide estimates of the size and characteristics of the workforce using traditional sources of labor market data, such as statistics from the Bureau of Labor Statistics (BLS) or the Census Bureau. No single federal data source provides a comprehensive estimate of the size of the workforce or details trends in supply and demand.

Additionally, academic literature on supply and demand in the cybersecurity workforce is limited and focuses primarily on potential causes of the workforce gap. One paper found that even though government and academic programs targeting cyber education succeed in their individual goals, the lack of connection, overlap, and communication between them limits their impact on closing the workforce gap.[1] A second paper proposed a lack of diversity in the field as a reason for a shortage of cybersecurity workers, citing the annual workforce survey from the International Information System Security Certification Consortium (ISC2) and noting that cybersecurity professionals remain primarily White men with postsecondary degrees.[2] Neither of these sources provided estimates for or suggested a methodology for estimating the cybersecurity workforce.

Existing attempts to estimate the size of the cybersecurity workforce and the number of additional cybersecurity professionals needed to meet labor market demands come primarily from nonfederal professional organizations and administrative data providers. Currently, CyberSeek and ISC2 are frequently cited by industry experts as the best sources of data on the existing cybersecurity workforce and industry demands. CyberSeek—a product of the Computing Technology Industry Association (CompTIA), administrative data provider Lightcast, and the National Institute of Standards and Technology (NIST)—collects workforce data based on web scraping of job postings and proprietary data. ISC2, a membership organization that represents cybersecurity professionals, conducts an annual workforce report based on a survey of its membership and business leaders. ISC2 models the size of the workforce based on its internal data, combined with national and global statistics from government statistical agencies and labor market data providers.

Reports from CyberSeek and ISC2 in 2023 came to similar estimates of the size of the existing workforce and workforce gap: between 1,180,000 and 1,340,000 current cybersecurity workers and between 480,000 and 570,000 unfilled cybersecurity jobs in the United States. Table 1 shows the estimates of the existing workforce and workforce gap provided by CyberSeek and ISC2. However, the amount of information provided by these sources is limited because they rely on nonpublic data and methods. We do not rely on CyberSeek alone because the Cybersecurity Workforce Data Initiative (CWDI) requires a data source and methodology that can be made public, operationalized, and replicated. Similarly, the ISC2 workforce study provides a useful comparison point, but as a private industry survey, it is insufficient for the entirety of the cybersecurity workforce in the CWDI. Neither source provides information on the workforce pipeline or availability of workers in the labor force.

Table 1
Estimates of cybersecurity workforce and unfilled positions from administrative data sources: 2023
(Number)

Source	Existing workforce	Unfilled positions
CyberSeek	1,180,000	570,000
ISC2	1,340,000	480,000

Note(s):
Values are rounded to the nearest 10,000.

Source(s):
CyberSeek, 2023, Total Employed in Cybersecurity Workforce and Total Cybersecurity Job Openings (data reflect September 2022–August 2023), https://www.cyberseek.org/heatmap.html, accessed 10 November 2023; and ISC2, 2023, *ISC2 Cybersecurity Workforce Study, 2023: How the Economy, Skills 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?rev=52055d08ca644293bd7497725bb7fcb4&hash=A9468BDB3269DCD9CFF7E550F3D62E01 .

Estimates of supply and demand are crucial for closing the gaps between skilled workers looking for jobs and unfilled positions, but the currently available data and literature do not reliably provide those estimates. In addition to reliable, replicable estimates of the size of the workforce and workforce gap that use publicly available data, more information is needed on the pipeline of workers and profile of the workforce pipeline and supply of available workers in the labor force. Therefore, the CWDI analyzed a combination of existing federal labor market and postsecondary education data sources, as well as data from nonfederal and administrative sources, to provide estimates of supply and demand for the cybersecurity workforce.

Methodology

Definitions

To prepare estimates for the supply of and demand for cybersecurity workers, it was necessary to establish operational definitions of "supply," "demand," and "cybersecurity worker." These operational definitions determined which individuals and jobs were included and excluded from the estimates of the cybersecurity workforce.

Supply and Demand

The National Center for Science and Engineering Statistics (NCSES) delineates the difference between the labor force and the workforce in its reports, such as *The STEM Labor Force of Today: Scientists, Engineers, and Skilled Technical Workers*. NCSES defines the *workforce* as a subset of those in the labor force who are currently employed and relies on the BLS definition of the *labor force*, which includes both those who are employed and those who are looking for work.[3] Thus, in this report, *supply* is defined as individuals currently in the workforce, unemployed individuals who recently held jobs in cybersecurity and potentially are seeking work, and the inflow of new graduates from relevant postsecondary degree programs who possibly will be looking for work. Demand includes both short-term and long-term demand. For this report, *short-term demand* is defined as current job postings from job boards, and *long-term demand* is defined by BLS projections of 10-year job growth, as part of its Employment Projections program.[4]

Cybersecurity Workers and Cybersecurity Jobs

As discussed in the CWDI definitions report, the definition of the cybersecurity workforce varies depending on the source, and experts in the field agree that many of the existing definitions do not translate directly to labor market data.[5] According to the Workforce Framework for Cybersecurity—commonly referred to as the NICE Framework—the cybersecurity workforce contains workers whose primary role encompasses cybersecurity activities, plus those who have relevant knowledge and skills to

address cybersecurity risks.[6] The NICE Framework does not delineate the number or percentage of cybersecurity work roles that define a cybersecurity job or worker at any level of their definition. In this report, the definition of cybersecurity worker follows that of the NICE Framework and defines "cybersecurity workers" as individuals whose primary role is cybersecurity and individuals who use cybersecurity knowledge and skills in their work roles. Federal data sources that provide labor market estimates do not align with the NICE Framework, so further operationalization was needed to define a cybersecurity worker in the context of existing data sources, so that those data sources could be used to produce estimates.

Occupation Codes

Federal sources, such as the Census Bureau and BLS, use Standard Occupational Classification (SOC) codes to describe and define occupations and provide estimates of supply and demand.[7] There are numerous occupations defined by SOC codes that incorporate cybersecurity activities, knowledge, and skills, as outlined in the NICE Framework, so there is no single SOC code that would encompass the entire cybersecurity workforce.

Because cybersecurity work cuts across numerous SOC occupations, we examined the Occupational Information Network (O*NET) for occupations that contained knowledge, tasks, and skills related to cybersecurity to identify occupations that likely contain core cybersecurity workers. We identified nine SOC codes. These include information security analysts, who explicitly focus on cybersecurity and are defined, for the purposes of this report, as *key* cybersecurity workers, as well as eight other occupations that have primary work roles in cybersecurity and are defined, for the purposes of this report, as *core* cybersecurity workers. The one key and eight core occupations, as defined by SOC code, are listed below. Although the selected SOC codes will not perfectly align with the cybersecurity workforce, for the purpose of using federal data to create estimates in this report, *cybersecurity workers* are defined as individuals working in an occupation defined by one of these nine SOC codes.

- 15-1212: Information Security Analysts (Key)
- 11-3021: Computer and Information Systems Managers (Core)
- 15-1211: Computer Systems Analysts (Core)
- 15-1231: Computer Network Support Specialists (Core)
- 15-1241: Computer Network Architects (Core)
- 15-1242: Database Administrators (Core)
- 15-1243: Database Architects (Core)
- 15-1244: Network and Computer Systems Administrators (Core)
- 15-1299: Computer Occupations, All Other (Core)

Classification of Instructional Programs Codes

Like federal labor market data sources, federal data sources that provide estimates of postsecondary degree and certificate completions do not align with the NICE Framework. The Department of Education

uses the Classification of Instructional Programs (CIP) to define postsecondary programs of study. There are numerous CIP codes that describe programs of study containing cybersecurity knowledge and skills. There is not one singular CIP code that would encompass all graduates potentially seeking work in cybersecurity.

BLS and the Department of Education maintain a CIP-to-SOC crosswalk that maps postsecondary fields of study to related occupations. Thirty-eight CIP codes map to the nine SOC codes used to define the core cybersecurity workforce. Of those 38 CIP codes, we determined that 14 were not sufficiently related to cybersecurity. Two additional CIP codes not in the original 38 were added to the list of core cybersecurity fields of study: 43.0303, Critical Infrastructure Protection, and 43.0404, Cybersecurity Defense Strategy and Policy. The description of these two additional CIP codes align strongly to cybersecurity (see table A-1). In the CIP-to-SOC crosswalk, they map to criminal justice, law enforcement, or military occupations which include some cybersecurity skills and knowledge in their SOC profiles.[8] Therefore, 26 total CIP codes were determined to make up the degree programs that could create a potential pipeline of workers to cybersecurity jobs. In this report, one of the estimates of supply is an estimate of individuals who completed a degree or certificate in one of those 26 CIP codes. Table A-1 shows which CIP codes were used in this analysis and those that were excluded.

Cybersecurity Job Openings

Ideally, a cybersecurity job opening would be defined as a posting that falls under one of the nine SOC codes used in this paper. However, it was not possible to apply the same SOC code methodology to the search of job postings on commercial job board sites for several reasons. First, because SOC defines occupations with tasks, skills, and activities and not by job title, search results on job board sites cannot be assigned to a SOC code based on job title. Additionally, job descriptions contain numerous keywords describing required skills and knowledge, and skills and knowledge overlap among occupations, so a search for “network support specialist” and “network administrator” for example may turn up many of the same results, making it difficult to decide which SOC code each search result should be assigned. Because it was not possible to map results from commercial job board sites to SOC codes, instead, a selection of terms from the NICE Framework were entered into LinkedIn and Indeed to estimate the number of openings calling for those skills or work roles.

Table 2 outlines our operational definitions for this work.

Table 2
Operational definitions of key terms for estimating supply and demand
(Term and definition)

Term	Definition
Supply	Individuals currently in the workforce plus unemployed individuals and new graduates from relevant postsecondary degree programs who are or will be looking for work
Short-term demand	Current job postings from job boards
Long-term demand	Bureau of Labor Statistics projections of 10-year job growth, as part of its Employment Projections program
Labor force	Individuals who are employed, and those who are looking for work
Workforce	Individuals who are currently employed; a subset of the labor force
Cybersecurity worker	Individuals working in an occupation defined by one of the nine key and core Standard Occupational Classification (SOC) codes
Cybersecurity job opening	Job postings that fall under one of the nine key and core SOC codes

Source(s):
Bureau of Labor Statistics, Employment Projections (2022). National Science Board, National Science Foundation. 2024. The STEM Labor Force: Scientists, Engineers, and Technical Workers. *Science and Engineering Indicators 2024.* NSB-2024-5. Alexandria, VA. Available at https://ncses.nsf.gov/pubs/nsb20245/.

Data Sources

Traditional estimates for the size of a workforce use SOC codes or North American Industry Classification System (NAICS) codes to define the occupations or industries that make up that workforce. Because cybersecurity occupations cross industries and can be found in transportation, finance, science, education, healthcare, and other industries, analyses using NAICS codes were found to be insufficient for estimating supply and demand in the cybersecurity workforce. A methodology for conducting analyses using SOC codes was established as described above and was applied to multiple federal data sources that use SOC codes to obtain a range of estimates. Estimates of supply and demand vary by source, depending on the methodology and definitions used by that source.

It is important to note that the data sources used for estimates are from different years and have different levels of data lag. Many cited federal sources rely on data from 2021 and 2022, which reflected a different hiring and workforce landscape than seen in 2024. Surveys in 2023 from organizations like ISC2 indicated a slowing rate of hiring due to changing economic conditions. In addition, high-profile technology sector corporate layoffs in 2023 and early 2024 indicate a shifting demand in the technology workforce. This report cites the most recent research available, with the understanding that new data is becoming available on a regular basis, and different sources rely on different methods to define supply and demand. Table 3 shows the data sources used in this report, which estimates they were used for, and the year to which the data refer.

Table 3
Existing data sources used for estimating supply and demand
(Source and year)

Source	Year
Estimates of the size of the existing cybersecurity workforce	
Bureau of Labor Statistics, Occupational Employment and Wage Statistics (OEWS) survey	2022
Census Bureau, American Community Survey (ACS)	2022
National Science Foundation, National Survey of College Graduates (NSCG)	2021
Office of Personnel Management	2024
Estimates of the inflow of new cybersecurity workers from postsecondary programs of study	
Department of Education, Integrated Postsecondary Education Data System (IPEDS)	2022
National Science Foundation, Survey of Graduate Students and Postdoctorates in Science and Engineering (GSS)	2022
Estimates of current open job postings	
Occupational Information Network (O*NET)	2024
LinkedIn	2024
Indeed	2024
ClearanceJobs	2024
USAJOBS	2024
Estimates of long-term job growth	
Bureau of Labor Statistics, Occupational Employment and Wage Statistics (OEWS) survey	2022

Creating Estimates

After establishing operational definitions—for supply, demand, and cybersecurity workers (both currently employed and potential entrants into the workforce)—and selecting existing federal and nonfederal sources of labor market and postsecondary education data, estimates of supply and demand were calculated. Each estimate is a range of values. Values are rounded to the nearest thousand.

The lower number in each range is based on a narrow definition of cybersecurity and includes only individuals in the “key” cybersecurity occupation or postsecondary program of study—that is, SOC code 15-1212: Information Security Analysts and CIP code 11.1003: Computer and Information Systems

Security/Auditing/Information Assurance. This occupation and this program of study explicitly focus on cybersecurity. However, because the definition of cybersecurity workers includes those whose primary role comprises cybersecurity activities *and* workers with cybersecurity knowledge and skills who may sometimes work on cybersecurity tasks in their role, restricting the estimates to only workers in the key cybersecurity occupation or program of study underestimates the cybersecurity workforce.

The higher number in the range is based on a broader definition of cybersecurity and includes individuals in all nine "core" cybersecurity occupations or 26 postsecondary programs of study. Although it is probable that individuals employed in the core cybersecurity occupations spend some of their time doing cybersecurity work and employing cybersecurity knowledge and skills, these occupations are not solely cybersecurity occupations, so including these workers likely overestimates the cybersecurity workforce. Similarly, individuals who completed degrees or certificates in cybersecurity programs of study may or may not pursue employment in cybersecurity occupations, so including these graduates likely overestimates the cybersecurity pipeline. Expert interviews and data presented later in this report offer evidence that the pipeline to entering cybersecurity work is not linear, and that many workers work in a job not closely related to their degree or certification.

Estimates of short-term demand present the number of results returned from a search of a term from the NICE Framework in LinkedIn or Indeed, but they do not necessarily align directly with any SOC codes. The numbers are simply shown at face value as they appeared on the day of the search. Because the code for these commercial search engines in proprietary, it is not transparent how entering search terms produces results, so it is unknown why or how a certain number of results was returned in response to a keyword search. Estimates of long-term demand reflect the BLS projections of 10-year job growth, as part of its Employment Projections program.

We recognize that it is challenging to provide estimates of the size and characteristics of the cybersecurity workforce using traditional sources of labor market or postsecondary education data. There is not a universal definition of the cybersecurity workforce. Relevant knowledge and skills in cybersecurity can apply to numerous occupations and postsecondary degree programs, and the process of determining which occupations and postsecondary degree programs are *most* relevant is subjective. That is why transparency around the selection of data sources, SOC codes, CIP codes, and estimation methods underlying the estimates is essential. Estimates provided in this report are not intended to be definitive but to improve our understanding of the cybersecurity workforce given the current state of the research.

Estimates of Supply

Size and Characteristics of the Existing Cybersecurity Workforce and Labor Force

The number of individuals currently employed in cybersecurity occupations make up the existing cybersecurity workforce. The existing workforce is one important aspect of the supply of cybersecurity workers. Data from the BLS Occupational Employment and Wage Statistics (OEWS) program, the Census Bureau's American Community Survey (ACS), and NCSES's National Survey of College Graduates (NSCG) were examined to produce estimates for the size of the existing cybersecurity workforce.

Unemployed workers, defined as those in the labor force and not working but actively searching for work, constitute a share of the supply of workers to fill open jobs. The ACS and the NSCG both provide estimates of the number of unemployed individuals in the labor force. The ACS and the NSCG also provide information about the characteristics of the labor force, including sex, race, ethnicity, citizenship, and highest degree attained. The OEWS is an establishment survey, so it measures only current

employees and does not contain employee-level demographic data. Therefore, the ACS and the NSCG were examined to produce estimates for the number of individuals in the labor force, including those who are unemployed, and for the demographic and educational characteristics of the overall labor force.

BLS: OEWS

BLS conducts the OEWS program, which produces annual employment and wage estimates at the national and state levels using data from business surveys.[9] The OEWS program is widely cited and provides reliable data on the number of people working in different occupations.[10] BLS uses the SOC system to define occupations. Table 4 shows the number of individuals currently employed in key and core cybersecurity occupations, defined by SOC code, according to 2022 OEWS data.

Table 4
National workforce in cybersecurity occupations: 2022
(Number employed and 2022 dollars)

Occupation title	Occupation code	Total employment	Median annual pay ($)
Total across cybersecurity	na	2,430,200	-
Key cybersecurity	na	163,690	112,000
Information security analysts	15-1212	163,690	112,000
Core cybersecurity	na	2,266,510	-
Computer and information systems managers	11-3021	533,220	164,070
Computer systems analysts	15-1211	505,210	102,240
Computer occupations, all other	15-1299	416,320	98,740
Network and computer systems administrators	15-1244	325,930	90,520
Computer network architects	15-1241	173,920	126,900
Computer network support specialists	15-1231	168,920	68,050
Database administrators	15-1242	80,520	99,890
Database architects	15-1243	62,470	134,870

na = not applicable; NA= not available.

Note(s):
There are insufficient publicly available data to calculate the percentile range of annual salaries for the total across Standard Occupational Classification codes.

Source(s):
Bureau of Labor Statistics, Occupational Employment and Wage Statistics (2022).

According to OEWS, there were just under 164,000 people working as information security analysts in 2022. Including individuals working in all nine key and core occupations produces an estimate of 2,430,000 workers. In this data, “Computer Occupations, All Other” (SOC code 15-1299) is a particularly broad category. Although BLS names several subcategories under this code that are core cybersecurity occupations (e.g., 15-1299.06: Digital Forensics Analysts, 15-1299.05: Information Security Engineers, and 15-1299.04: Penetration Testers), detailed data are not yet available on the size of these specific occupations defined by eight-digit SOC codes.[11] Moving forward, more granular data from BLS on these occupations will allow a more accurate picture of the state of the cybersecurity workforce. For this analysis, all workers in “Computer Occupations, All Other” were included in the estimate, likely resulting in an overcount of the number of current cybersecurity workers.

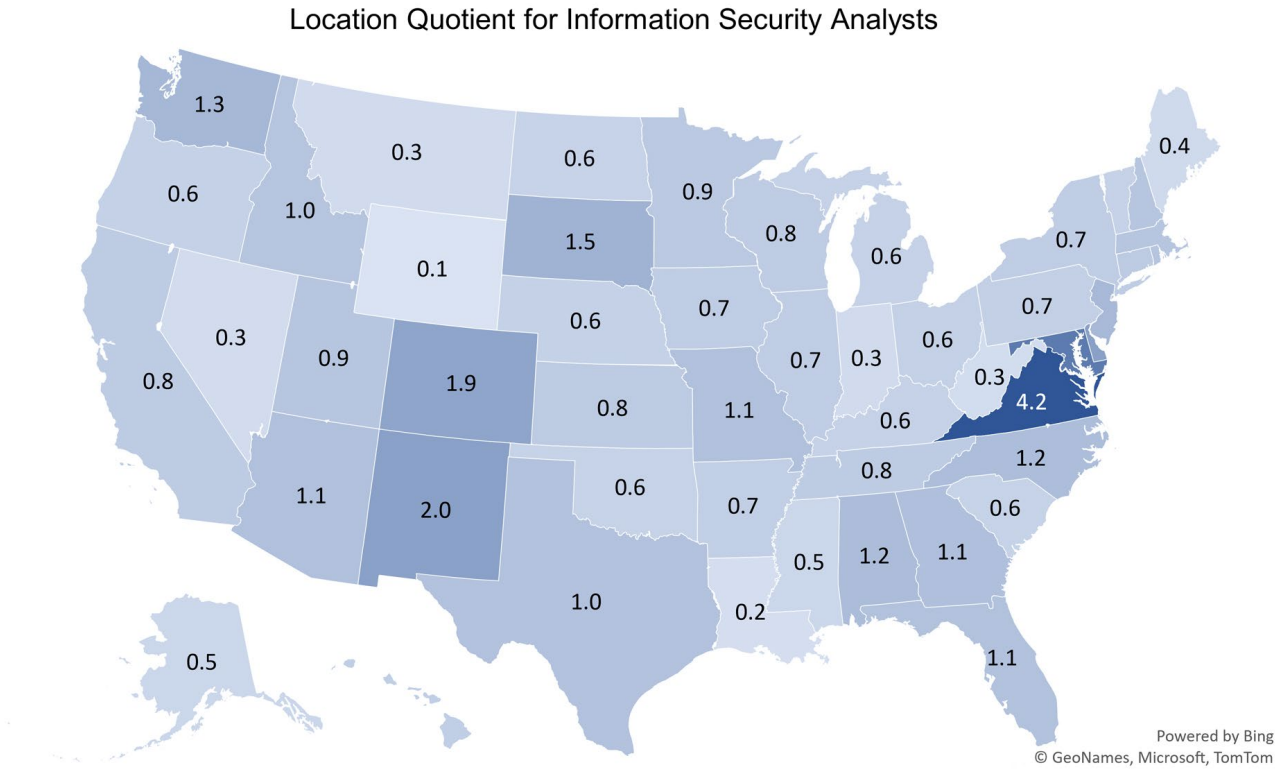
Although these estimates relied on OEWS data, which is known to be of high quality, existing SOC codes do not yet have the granularity to accurately estimate the population of the existing cybersecurity workforce. Even so, examining the OEWS data following the methods used for this report produces an estimate between 164,000 (narrowest definition) and 2,430,000 (broadest definition) cybersecurity workers employed in 2022.

Key Occupation: Information Security Analysts

After examining the data, we identified Information Security Analysts (15-1212) as a key part of the cybersecurity workforce. Information security analysts were reported to have a median annual pay of $112,000, earning above the national median and ranking among the highest-paid occupations in the United States.

Information security analysts tend to be geographically concentrated in certain states. OEWS also provides a measure called the location quotient (LQ), which shows the concentration of an occupation in an area relative to the U.S. average.[12] An LQ greater than 1.0 indicates that the area has a higher share of employment for that occupation than the national average. Figure 1 shows which states have high employment concentrations for information security analysts, with Virginia, Maryland, and the District of Columbia having the highest concentrations of information security analysts per capita relative to the U.S. average. Metropolitan areas with a high concentration of information security analysts include Huntsville, AL; Washington, DC; Colorado Springs, CO; Baltimore, MD; and San Jose, CA. This offers evidence that proximity to the federal government and high-tech industry is a component of demand for information security analysts.

Figure 1
Employment concentration for information security analysts, by state: 2022
(Location quotient)



Source(s):
Bureau of Labor Statistics, Occupational Employment and Wage Statistics (2022).

Census Bureau: ACS

The Census Bureau conducts the ACS, an annual household survey of a nationally representative sample of households. The Census Bureau uses its own four-digit occupation codes, but it provides a crosswalk

mapping those codes to the six-digit SOC codes employed by BLS. Table 5 shows the eight Census Bureau occupation codes that correspond to the nine SOC codes identified as representing key and core cybersecurity occupations. Table 5 also shows the estimated number of individuals employed in each of those occupations in 2022, the estimated total individuals in the labor force, as well as the educational and demographic profiles of the labor force.

Table 5

Core cybersecurity workers, occupations, and characteristics: 2022

(Number and percent)

Characteristic	Full survey	Cybersecurity total	Key	Core						
			Information security analysts	Computer systems analysts	Computer support specialists	Database administrators and architects	Network and computer systems administrators	Computer network architects	Computer occupations, all other	Computer and information systems managers
ACS occupation (OCC) code	na	na	1007	1006	1050	1065	1105	1106	1108	0110
Corresponding SOC code	na	na	15-1212	15-1211	15-1231	15-1242 15-1243	15-1244	15-1241	15-1299	11-3021
Number of respondents (unweighted)	2,379,642	38,484	2,073	6,674	7,565	1,662	2,609	1,254	9,139	7,508
Population estimate (number)	241,653,489	3,887,466	208,501	678,342	787,850	158,004	258,188	123,031	958,315	715,235
Employment (percentage)										
In labor force, employed	66.6	89.8	92.1	90.7	88.4	89.9	91.2	91.0	88.5	91.0
In labor force, unemployed	2.9	1.9	1.2	1.4	3.1	1.3	2.0	1.6	1.9	1.5
Not in labor force	30.4	8.3	6.7	8.0	8.5	8.8	6.9	7.4	9.5	7.5
Labor force estimate (number)	168,081,389	3,566,654	194,594	624,330	720,874	144,081	240,423	113,976	866,843	661,533
Workforce estimate (number)	161,052,133	3,492,211	192,015	615,002	696,517	142,071	235,370	111,969	848,431	650,836
Percent of survey (percentage)	100	2.1	0.1	0.4	0.4	0.1	0.1	0.1	0.5	0.4
Percent of cybersecurity-related occupations (percentage)	na	100	5.5	17.5	20.2	4.0	6.7	3.2	24.3	18.5
Sex (percentage)										
Female	50.5	26.5	16.7	40.4	24.3	31.6	17.3	10.6	23.4	27.8
Male	49.5	73.5	83.3	59.6	75.7	68.4	82.7	89.4	76.6	72.2
Highest degree (percentage)										
No high school diploma or similar	12.9	1.1	0.7	1.1	1.5	D	0.9	D	1.5	0.6
High school diploma or similar	25.6	7.8	5.0	5.2	11.5	5.2	7.7	8.5	10.3	4.1
Some college, no bachelor's	19.8	18.6	16.3	13.7	24.6	10.0	22.9	20.6	21.4	13.7
Associate's degree	8.6	11.8	10.8	8.0	14.7	6.6	16.5	15.0	13.8	8.6
Bachelor's degree	20.7	41.9	41.1	48.9	36.5	49.8	40.2	38.1	37.8	46.3
Master's degree	8.9	17.0	23.1	20.8	10.0	24.3	11.1	14.9	14.0	24.2
Professional degree beyond a bachelor's degree	2.0	0.8	1.5	1.0	0.5	D	0.3	D	0.6	0.9
Doctorate degree	1.4	1.1	1.4	1.3	0.7	1.8	0.4	1.2	0.6	1.6
Citizenship (percentage)										
U.S. citizen	92.1	92.9	94.3	92.4	93.8	87.0	95.6	94.3	92.9	92.1
Not a U.S. citizen[a]	7.9	7.1	5.7	7.6	6.2	13.0	4.4	5.7	7.1	7.9

Characteristic	Full survey	Cybersecurity total	Key	Core						
			Information security analysts	Computer systems analysts	Computer support specialists	Database administrators and architects	Network and computer systems administrators	Computer network architects	Computer occupations, all other	Computer and information systems managers
Race/ethnicity (percentage)										
Hispanic or Latino	18.3	10.4	9.4	10.1	12.2	7.8	10.4	11.6	11.4	8.3
Not Hispanic or Latino										
American Indian or Alaska Native	0.5	0.2	D	0.2	0.2	D	D	D	0.4	0.2
Asian	6.2	13.7	10.0	15.5	11.2	21.0	9.3	10.9	14.4	15.2
Black or African American	11.7	10.3	12.2	11.9	11.6	5.4	10.2	11.3	11.5	6.3
Native Hawaiian or Pacific Islander	0.1	0.1	D	D	D	D	D	D	D	D
White	58.9	60.4	62.5	57.3	59.1	62.5	64.8	62.5	57.4	65.6
Multiple races or other	4.3	4.9	5.7	4.9	5.5	3.1	5.1	3.5	4.8	4.4

D = suppressed to avoid disclosure of confidential information; na = not applicable.

ACS = American Community Survey; SOC = Standard Occupational Classification.

[a] Permanent resident and temporary visa holders cannot be identified separately in the ACS.

Note(s):
Full survey estimates include population 16 years and older living in households in the 50 states plus the District of Columbia. Percentages may not sum to 100% due to rounding; weighted counts may not sum due to rounding.

Source(s):
Census Bureau, 2022 American Community Survey (ACS), 1-Year Microdata.

According to the ACS, there were approximately 192,000 individuals ages 16 and over that were employed as information security analysts in 2022 out of approximately 3,492,000 individuals across all nine key and core cybersecurity occupations. Analyzing ACS data following the methods used for this report produces a range between 192,000 (narrowest definition) and 3,492,000 (broadest definition) cybersecurity workers in the workforce in 2022.

Of the estimated 3,567,000 workers in the cybersecurity labor force under the nine SOC codes identified, only about 74,000 individuals (1.9% of the population of cybersecurity workers) were reported to be unemployed. For information security analysts, an estimated 2,500 individuals, or 1.2% of the population, were unemployed. In summary, ACS data shows a range of between 2,500 (narrowest definition) and 74,000 (broadest definition) unemployed cybersecurity workers in the labor force who were potentially seeking cybersecurity jobs in 2022.

In addition to providing estimates of the number of individuals in the workforce and in the labor force, the ACS provides data on demographics and educational attainment. Data shown is limited to adults in the labor force, defined by ACS as those 16 years of age and older. As seen in table 5, over 73% of core cybersecurity workers are male (compared to 49.5% of the working age population) and 61% have a bachelor's degree or higher (compared to 33% of the working age population). The racial and ethnic demographics of the labor force show that Hispanic or Latino workers are underrepresented in the cybersecurity workforce and Asian workers are overrepresented compared to the overall labor force.

NCSES: NSCG

NCSES conducts the NSCG, a biennial survey containing a nationally representative sample of individuals with at least a bachelor's degree. The survey captures employment outcomes as well as educational outcomes and demographic information. The NSCG uses its own coding system for occupations, but like the ACS, eight NSCG occupation codes align with the nine key and core SOC codes (see table 6). These are further combined to reduce suppression. Table 6 also shows how many individuals were working in each of those occupations in 2021, the estimated total individuals in the labor force, as well as the educational and demographic profiles of the labor force.

Table 6

Coverage of cybersecurity workers in the NCSES NSCG, 2021

(Number and percent)

Characteristic	Full survey	Total cybersecurity	Key	Core					
			Information security analysts	Computer system analysts	Computer support specialists	Database administrators and computer network architects	Network and computer systems administrators	Other computer information science occupations	Computer and information systems managers
SOC	na	na	15-1212	15-1211	15-1231	15-1241 15-1242 15-1243	15-1244	15-1299	11-3021
NSCG N3OCPR code	na	na	110570	110550	110540	110520 110560	110580	110610	621420
Number of respondents (unweighted)	105,886	4,724	281	642	1,165	462	497	1,015	662
Population estimate	68,349,532	2,433,834	141,248	410,475	514,350	207,686	270,681	511,220	378,173
Employment (percentage)									
In the labor force (employed)	75.4	77.5	87.7	73.3	78.2	81.8	83.0	78.5	69.4
In the labor force (unemployed)	4.6	4.5	D	6.3	4.9	D	7.0	5.4	1.2
Not in the labor force	20.0	18.1	D	20.4	16.9	D	10.0	16.2	29.4
Labor force estimate	54,684,312	1,993,892	126,334	326,642	427,575	174,325	243,517	428,544	266,956
Workforce estimate	51,525,280	1,885,038	D	300,837	402,302	D	224,680	401,109	262,371
Percent of survey	100	3.6	0.2	0.6	0.8	0.3	0.4	0.8	0.5
Percent of cybersecurity related occupations	na	100	6.34	16.38	21.44	8.74	12.21	21.49	13.39
Highest degree distribution									
Bachelor's	62.0	70.7	66.5	85.4	67.7	76.5	74.6	69.0	54.5
Master's	27.9	27.8	32.5	13.6	31.6	22.5	24.8	28.2	42.5
Doctorate	4.0	1.2	D	1.0	0.6	0.9	D	1.2	3.0
Professional	6.0	0.4	D	D	D	D	D	D	D
Job related to highest degree									
Closely related	54.3	46.1	59.9	37.0	46.9	42.5	45.6	43.0	56.1
Somewhat related	26.1	32.7	27.8	29.3	34.9	33.1	30.8	35.8	32.1
Not related	19.7	21.3	12.3	33.7	18.2	24.5	23.7	21.2	11.8
Hold active certifications or licenses (percent)	40.3	26.8	59.0	22.0	23.2	21.0	27.9	21.0	35.1
License is for principal job (number)	17,644,273	412,034	60,654	42,307	79,786	30,391	44,731	77,717	76,447
License is in computer networking, administration, and security (number)	328,784	177,974	57,733	23,651	12,570	19,693	22,483	24,107	17,737
Sex									
Female	51.4	29.7	21.8	30.6	38.8	31.1	15.2	35.5	20.9
Male	48.7	70.3	78.2	69.4	61.2	68.9	84.8	64.5	79.1

Characteristic	Full survey	Total cybersecurity	Key	Core					
			Information security analysts	Computer system analysts	Computer support specialists	Database administrators and computer network architects	Network and computer systems administrators	Other computer information science occupations	Computer and information systems managers
Citizenship									
U.S. citizen	94.3	90.6	91.1	95.5	84.0	88.4	95.1	93.2	88.3
Permanent resident	3.3	3.8	7.3	1.9	4.9	2.4	3.6	3.1	5.1
Temporary visa holder	2.5	5.6	1.6	2.6	11.1	9.2	1.3	3.8	6.6
Race/ethnicity									
Hispanic or Latino	10.4	9.8	4.8	15.5	12.5	9.5	7.6	6.4	8.7
Not Hispanic or Latino									
Asian	10.7	20.3	11.1	13.7	28.8	25.8	11.4	18.7	25.8
American Indian or Alaska Native	0.3	0.2	D	D	D	D	D	D	D
Black or African American	8.2	8.4	14.8	12.8	8.8	3.2	8.5	6.1	6.4
Native Hawaiian or Pacific Islander	0.3	0.2	D	D	D	D	D	D	D
White	67.7	58.4	66.0	54.5	47.1	57.2	68.0	66.2	57.5
Multiple race or other	2.5	2.7	2.6	2.6	2.7	3.9	3.5	2.3	1.6

D = suppressed to avoid disclosure of confidential information; na = not applicable.

NSCG = National Survey of College Graduates; SOC = Standard Occupational Classification.

Note(s):
Data include the civilian, noninstitutionalized population in the labor force (employed or unemployed) ages 16–75. Percentages may not sum to 100% due to rounding; weighted counts may not sum due to rounding.

Source(s):
National Center for Science and Engineering Statistics, National Survey of College Graduates (NSCG), Public-Use File, 2021.

According to the NSCG, there were approximately 126,000 college graduates working as information security analysts in 2021. There were approximately 1,885,000 college graduates working across all nine key and core cybersecurity occupations. Examining the NSCG data following the methods used for this report produces an estimate between 126,000 (narrowest definition) and 1,885,000 (broadest definition) cybersecurity workers with a bachelor's degree or higher. Since the NSCG estimate only includes cybersecurity workers with a bachelor's degree or higher, we will continue to refer to the 164,000 estimate from OEWS as the lower bound of our estimates. In the NSCG, of the estimated 1,994,000 workers in the cybersecurity labor force in the nine SOC codes identified, about 109,000 workers were estimated to be unemployed.

The NSCG data follows the ACS data in reflecting that the cybersecurity labor force with a bachelor's degree or higher is more than 70% male and that its racial makeup is relatively representative of the overall population, with Asian workers overrepresented. However, since the NSCG only surveys individuals with bachelor's degrees or higher, the percentages differ from the ACS, which surveys the adult age population regardless of degree.

As shown in table 6, an estimated 27% of individuals in key and core cybersecurity occupations combined hold a license or certification for their principal job, with nearly 60% of information security analysts holding a license or certification. Thus, licenses and certifications may be important for the cybersecurity workforce. The license and certification data in table 6 also highlight a limitation of occupation codes, as only 178,000 of the 329,000 people (54%) with a cybersecurity license or certification were in the key or core cybersecurity occupations. This shows the likelihood that cybersecurity professionals are found in occupations other than the nine selected for this report.

The NSCG also provides estimates for the number of individuals working in a job closely related to their highest degree. About 21% of workers in key and core cybersecurity occupations work in a job unrelated to their highest degree, and less than half of these workers (46%) work in a job closely related to their highest degree. These data offer evidence to support what was heard in the CWDI expert interviews: there are numerous pathways into the cybersecurity workforce, and cybersecurity workers do not necessarily follow a linear path from a postsecondary credential in cybersecurity to a cybersecurity career.

Federal Government Office of Personnel Management

Currently, the Office of Personnel Management (OPM) tracks 52 work role codes and definitions aligned to the 2 November 2016 version of the NICE Framework. These OPM work role codes are outlined in further detail in the CWDI definitions report.

The OPM Cyber Workforce dashboard tracks the federal employees that fall into the 52 work roles outlined in the NICE Framework, and the data on the workforce indicates characteristics of the current federal cybersecurity workforce.[13] These characteristics include the following:

- The average age reported for federal cyber workers is 48 years old, and nearly 35% of federal cyber employees are eligible for retirement in the next 5 years.
- The federal cyber workforce is more than 73% male.
- Compared to the federal workforce overall, the federal cyber workforce has a higher rate of retention, a larger share of workers younger than 35 years old, and a lower rate of separations and quits.

- The Department of Defense Cyber Excepted Service and the Department of Homeland Security Cyber Talent Management System allow for specific cyber positions to earn salaries above the traditional federal pay schedules.[14] In 2023, 25% of employees were on "other pay plans," and more than 50% were GS-12 or higher, putting them among the highest-paid federal employees.[15]

OPM does not publicly provide a top-line number of the number of federal employees who fall under the 52 work role codes designated as cybersecurity.

Size and Characteristics of the Existing Cybersecurity Workforce and Labor Force: Conclusions

This analysis illustrates the challenges of estimating the size of the cybersecurity labor force using existing data sources. The estimated number of cybersecurity workers varies widely, depending on the definition of a cybersecurity worker. In addition, estimates from different data sources vary, according to the sample and methodology employed by that source. Table 7 summarizes the different estimated ranges of cybersecurity workers obtained from the three data sources in this section.

Table 7
Range of estimates for the number of current cybersecurity workers by data source
(Source, method, and number)

Source	Methodology	Low estimate: Includes information security analysts (SOC code 15-1212) only	High estimate: Includes all nine key and core occupations defined by SOC codes
Workforce			
BLS OEWS	Panel survey of approximately 1.1 million business establishments. Includes only current paid employees.	164,000	2,430,000
Census Bureau ACS	Nationally representative sample of households. Collects employment information for all persons over the age of 16 in the household within the last year. Limited to those in the labor force.	192,000	3,492,000
NCSES NSCG	Nationally representative sample of graduates with at least a bachelor's degree.	126,000	1,885,000
Labor force			
Census Bureau ACS	Nationally representative sample of households. Collects employment information for all persons over the age of 16 in the household within the last year. Limited to those in the labor force.	195,000	3,567,000
NCSES NSCG	Nationally representative sample of graduates with at least a bachelor's degree.	126,000	1,994,000

ACS = American Community Survey; BLS = Bureau of Labor Statistics; NCSES = National Center for Science and Engineering Statistics; NSCG = National Survey of College Graduates; OEWS = Occupational Employment and Wage Statistics; SOC = Standard Occupational Classification.

Note(s):
The NCSES NSCG workforce estimate cannot be shown due to suppression; 126,000 is the labor force estimate which is higher than the workforce estimate.

Source(s):
Bureau of Labor Statistics, Occupational Employment and Wage Statistics (2022); Census Bureau, 2022 American Community Survey (ACS), 1-Year Microdata; National Center for Science and Engineering Statistics, National Survey of College Graduates (NSCG), Public-Use File, 2021.

In summary, according to the data sources and estimation methodology in this report, the number of cybersecurity workers currently in the workforce could be as low as 164,000 or as high as 3,492,000, depending on the definition of a cybersecurity worker and the sample surveyed. The total supply of cybersecurity workers including employed and unemployed individuals in the labor force may be as high as 3,567,000 workers. The low-range estimate of 164,000 from OEWS is used because the 126,000 information security analysts obtained from the NSCG is a known undercount as the NSCG only surveys individuals with bachelor's degrees or higher, and the ACS data estimate that about one-third of the population of information security analysts does not have a bachelor's degree.

Furthermore, the methodology of using occupation codes to estimate the number of cybersecurity workers has limitations. Occupation descriptions in O*NET show that more than just information security analysts use cybersecurity knowledge and skills and perform cybersecurity tasks, so any estimate of only information security analysts exclusive of all other occupations will not encompass the whole cybersecurity workforce. However, the highest estimate of 3,492,000 obtained from the ACS is surely an overcount; not all workers in computer occupations are cybersecurity workers. Furthermore, as the NSCG data show, thousands of individuals with a cybersecurity license or certification were not reported to be in one of the nine SOC codes analyzed for this report, strongly suggesting that cybersecurity professionals can be found in other SOC occupations as well. What none of the data sources show is how many cybersecurity skills are used by individuals in the eight core occupations, nor how much of their job is spent using them. Since there is also no official number or percentage for how many cybersecurity skills an individual must use or how much of their job must be spent using them to be counted as a cybersecurity professional, it cannot be known from these data sources how many of the upper range of workers are cybersecurity workers.

Estimates for the Inflow of New Workers

The labor force includes currently employed individuals as well as unemployed individuals looking for work. New graduates from relevant postsecondary programs are included in the definition of the cybersecurity labor force supply because they are potentially seeking employment. Data from the Department of Education's Integrated Postsecondary Education Data System (IPEDS) and the National Science Foundation's Survey of Graduate Students and Postdoctorates in Science and Engineering (GSS) were examined to produce estimates for the size and characteristics of the population of new graduates.

Department of Education: IPEDS

IPEDS is a set of 12 survey components completed by all colleges, universities, and technical and vocational institutions that participate in the federal student financial aid programs. The IPEDS Completions survey component collects the number of postsecondary awards earned each academic year. Fields of study are categorized according to CIP code. Table 8 shows the number of degrees and certificates awarded in 2022 in the cybersecurity key, core, and related fields of study, defined by the CIP codes that were mapped to the nine key and core SOC codes. (See table A-1 or refer to the methodology section of this report for more detail on this mapping.)

Table 8

Degrees and certificates awarded in cybersecurity, by CIP code: 2022

(Number)

CIP title and type	CIP code	All awards	Certificates					Degrees				
			All certificates	Certificates of less than 1 year	Certificates of at least 1 year but less than 2 years	Certificates of at least 2 years but less than 4 years	Certificates above the baccalaureate	All degrees	Associate's degrees	Bachelor's degrees	Master's degrees	Research doctoral degrees
Key												
Computer and information systems security/auditing/information assurance	11.1003	24,964	6,999	4,789	1,385	0	825	17,965	4,150	7,131	6,566	118
Core	-	23,784	12,490	10,370	1,543	160	417	11,294	5,284	3,474	2,524	12
Computer systems networking and telecommunications	11.0901	11,920	7,876	6,772	903	4	197	4,044	2,890	745	407	2
Network and system administration/administrator	11.1001	4,636	2,939	2,323	476	140	0	1,697	1,472	168	57	-
System, networking, and LAN/WAN management/manager	11.1002	2,074	852	794	53	0	5	1,222	528	692	2	-
Information technology project management	11.1005	2,156	258	152	0	15	91	1,898	52	825	1,014	7
Critical infrastructure protection	43.0303	625	44	17	11	1	15	581	30	274	274	3
Cyber/computer forensics and counterterrorism	43.0403	1,820	291	127	85	-	79	1,529	304	607	618	-
Cybersecurity defense strategy/policy	43.0404	331	223	185	15	-	23	108	8	163	152	-
Healthcare information privacy assurance and security	51.0723	7	7	-	-	-	7	-	-	-	-	-
Related	-	209,985	26,426	20,647	3,084	279	2,416	183,559	22,177	112,370	45,937	3,075
Computer and information sciences, general	11.0101	50,454	8,682	7,764	656	44	218	41,772	5,471	25,124	10,406	771
Information technology	11.0103	32,494	7,021	6,061	584	1	375	25,473	5,901	13,069	6,369	134
Computer programming/programmer, general	11.0201	9,523	4,277	2,954	1,117	95	111	5,246	3,036	1,974	236	-
Information science/studies	11.0401	17,114	843	350	122	110	261	16,271	977	9,314	5,800	180
Computer systems analysis/analyst	11.0501	2,163	601	440	12	-	149	1,562	99	904	557	2
Computer science	11.0701	58,583	691	420	56	0	215	57,892	4,429	40,073	12,010	1,380
Data modeling/warehousing and database administration	11.0802	3,447	618	342	37	11	228	2,829	125	486	2,218	-
Cloud computing	11.0902	422	149	116	33	-	0	273	41	232	-	-
Computer support specialist	11.1006	2,894	1,581	1,153	428	-	-	1,313	1,235	78	-	-
Computer engineering, general	14.0901	12,377	152	110	-	-	42	12,225	36	9,746	2,042	401
Computer software engineering	14.0903	4,059	144	67	8	-	69	3,915	75	2,088	1,731	21
Computer engineering, other	14.0999	128	7	0	2	-	5	121	0	55	66	0
Systems engineering	14.2701	3,299	524	83	0	-	441	2,775	-	724	1,905	146
Human computer interaction	30.3101	1,968	330	261	-	-	69	1,638	60	858	711	9
Management information systems, general	52.1201	10,061	704	476	29	18	181	9,357	685	7,458	1,192	22

CIP title and type	CIP code	All awards	Certificates					Degrees				
			All certificates	Certificates of less than 1 year	Certificates of at least 1 year but less than 2 years	Certificates of at least 2 years but less than 4 years	Certificates above the baccalaureate	All degrees	Associate's degrees	Bachelor's degrees	Master's degrees	Research doctoral degrees
Information resources management	52.1206	932	67	20	-	-	47	865	7	161	688	9
Telecommunications management	52.2101	67	35	30	0	-	5	32	-	26	6	-

- = no programs reported to IPEDS.

CIP = Classification of Instructional Programs; LAN = local area network; WAN = wide area network.

Note(s):
Table includes completions data for Title IV degree-granting institutions in the United States. Does not include industry or other certifications offered outside of traditional postsecondary institutions or credentials. May not include credentials offered as part of bootcamps or other nontraditional degrees, even if offered at a Title IV institution. Data shown are the number of awards, not the number of individuals who earned them. Individuals who earned more than one degree or certificate in the 2021–22 academic year are counted in the number for each degree or certificate they earned.

Source(s):
Department of Education, National Center for Education Statistics, Integrated Postsecondary Education Data System (IPEDS), Completions component, accessed April 2024.

According to IPEDS, there were about 25,000 awards granted in Computer and Information Systems Security/Auditing/Information Assurance programs of study—the program of study most closely related to cybersecurity—in the 2021–22 academic year. Combining Computer and Information Systems Security/Auditing/Information Assurance with the eight core programs of study produces a total of about 49,000 awards granted. Including all 26 key, core, and related CIP codes produces a total of about 259,000 awards granted. Computer Science and Computer and Information Sciences, General had the largest number of awards granted, with 38.5% of the 259,000 awards granted in those two fields. This means that the high range of 259,000 cybersecurity awards is certainly an overcount, as not every individual earning a general computer science or information sciences degree or certificate will work in cybersecurity. However, the lower range of 25,000 Computer and Information Systems Security/Auditing/Information Assurance awards is certainly too restrictive, as individuals with degrees and certificates in other areas may have the skills and knowledge to pursue a cybersecurity career.

Because the data in table 8 represent the number of awards granted, not the number of individuals who earned awards, estimates based on IPEDS data are likely slight overcounts, as it is possible that a single individual earned more than one degree or certificate in the same year and is therefore counted more than once. Additionally, because IPEDS does not track graduates of postsecondary programs after graduation, IPEDS data cannot provide information about employment outcomes for graduates (i.e., whether individuals who completed these degrees or certificates pursued employment in a related field). Even so, examining IPEDS data following the methods used for this report produces an estimate between 25,000 (narrowest definition) and 259,000 (broadest definition) 2022 graduates from postsecondary programs who were potentially looking for work in the nine key and core cybersecurity occupations.

Nationally, the number of degrees and certificates awarded in key, core, and related cybersecurity fields of study has tripled, on average, over the past decade (2012–22). Table 9 shows this growth.

Table 9
Total degrees and certificates awarded in cybersecurity: 2012, 2017, and 2022
(Number and percent)

Field and degree type	2012	2017	2022	Growth rate 2012–22	Growth rate 2017–22	% of total 2022
Key						
Total awards	6,735	11,399	24,964	270.7	119.0	100
Certificates of less than 1 year	701	2,004	4,789	583.2	139.0	19.2
Certificates of at least 1 year but less than 2 years	141	384	1,385	882.3	260.7	5.5
Certificates of at least 2 years but less than 4 years	33	4	0	-100.0	-100.0	0.0
Certificates above the baccalaureate	328	749	825	151.5	10.1	3.3
Associate's degree	1,022	1,753	4,150	306.1	136.7	16.6
Bachelor's degree	3,683	3,692	7,131	93.6	93.1	28.6
Master's degree	816	2,764	6,566	704.7	137.6	26.3
Research doctoral degree	11	49	118	972.7	140.8	0.5
Core						
Total awards	25,796	19,713	23,784	-7.8	20.7	100
Certificates of less than 1 year	3,530	5,761	10,370	193.8	80.0	43.6
Certificates of at least 1 year but less than 2 years	1,904	1,980	1,543	-19.0	-22.1	6.5
Certificates of at least 2 years but less than 4 years	181	232	160	-11.6	-31.0	0.7
Certificates above the baccalaureate	122	202	417	241.8	106.4	1.8

Field and degree type	2012	2017	2022	Growth rate 2012–22	Growth rate 2017–22	% of total 2022
Associate's degree	16,094	7,334	5,284	-67.2	-28.0	22.2
Bachelor's degree	2,968	2,537	3,474	17.0	36.9	14.6
Master's degree	993	1,658	2,524	154.2	52.2	10.6
Research doctoral degree	4	9	12	200.0	33.3	0.1
Related						
Total awards	102,698	166,431	209,985	104.5	26.2	100
Certificates of less than 1 year	5,493	14,308	20,647	275.9	44.3	9.8
Certificates of at least 1 year but less than 2 years	2,789	2,446	3,084	10.6	26.1	1.5
Certificates of at least 2 years but less than 4 years	207	212	279	34.8	31.6	0.1
Certificates above the baccalaureate	1,352	1,879	2,416	78.7	28.6	1.2
Associate's degree	16,589	17,987	22,177	33.7	23.3	10.6
Bachelor's degree	47,893	76,930	112,370	134.6	46.1	53.5
Master's degree	26,232	50,307	45,937	75.1	-8.7	21.9
Research doctoral degree	2,143	2,362	3,075	43.5	30.2	1.5

CIP = Classification of Instructional Programs.

Note(s):
Total graduates per award level for academic years ending 2012, 2017, and 2022 in key, core, and related cybersecurity fields. Table includes completions data for Title IV degree-granting institutions in the United States. Does not include industry or other certifications offered outside of traditional postsecondary institutions or credentials. May not include credentials offered as part of bootcamps or other nontraditional degrees even if offered at a Title IV institution. Cyber/computer forensics and counterterrorism (CIP code 43.0403), cybersecurity defense strategy/policy (CIP code 43.0404), and health care information privacy assurance and security (CIP code 51.0723), all part of the core cybersecurity fields identified from the 2020 CIP codes, were not part of the CIP 2010 codes and so are not reflected in the 2012 and 2017 numbers in this table. Cloud computing (CIP code 11.0902), a cybersecurity-related field identified from the 2020 CIP codes, was not a part of the CIP 2010 codes and so is not reflected in the 2012 and 2017 numbers in this table.

Source(s):
Department of Education, National Center for Education Statistics, Integrated Postsecondary Education Data System (IPEDS), Completions component, accessed April 2024.

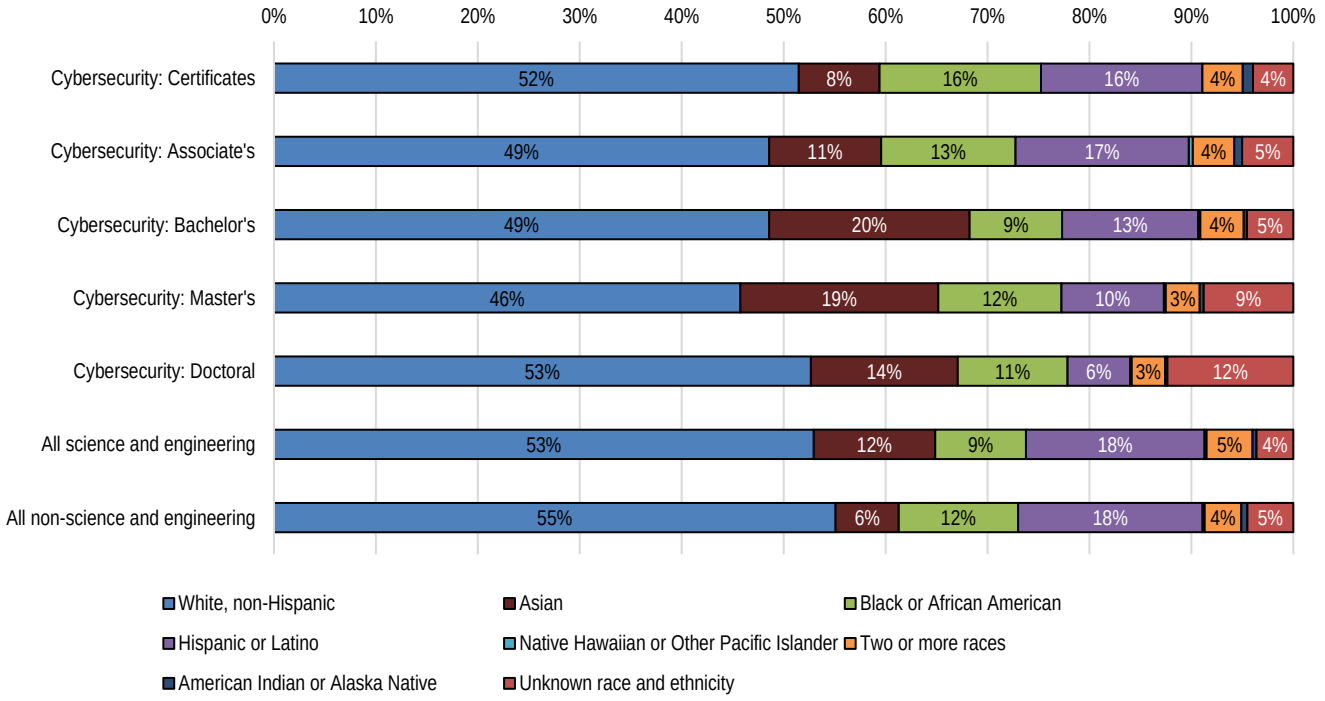
This rapid growth in the cybersecurity workforce pipeline and the large number of new graduates suggest that the workforce gap cited by industry leaders is due to factors other than quantity of potential workers. One of these factors could be the addition of new CIP codes in the 2020 revision of the CIP. These include Cyber/Computer Forensics and Counterterrorism, Cybersecurity Defense Strategy/Policy, Healthcare Information Privacy Assurance and Security, and Cloud Computing—all of which were not in the 2010 CIP taxonomy. These changes show that the advent of new technologies, policies, and cyber threats impacts postsecondary programs of study and, thereby, the knowledge and skills new workers coming into the cybersecurity workforce pipeline will have. These data also support a common theme from the CWDI expert interviews: the cybersecurity field evolves rapidly, and postsecondary institutions need to work hard to keep programs and curricula up-to-date. This situation possibly accounts for a gap between the skills and knowledge the supply of workers looking for jobs have and the skills and knowledge most in demand within the field.

Another notable point from the 2022 IPEDS data is that about 44% of awards in the eight core CIP programs were certificates of less than one year. Fifty-one percent of the awards in those CIP codes were certificates below the baccalaureate level. Twenty-five percent of awards in Computer and Information Systems Security/Auditing/Information Assurance were certificates below the baccalaureate level. These data point to additional changes in the postsecondary education landscape: more students are pursuing short-term certificates. Some of these students may not have a bachelor's degree or higher; some may, but in a different, unrelated field. These data support the theme that the pathway into cybersecurity jobs is not linear. In addition, it is possible that some jobseekers do not meet the degree requirements of job postings, which could also contribute to the workforce gap.

Demographics for Graduates of Cybersecurity Programs

As shown in table 5, there is an underrepresentation of Hispanic or Latino workers in cybersecurity relative to the working age population (10% of cybersecurity, 17% of population over age 16) and an overrepresentation of Asian workers (13% of cybersecurity, 6% of population over 16). Black or African American workers are estimated to make up 10% of the cybersecurity workforce and 11.5% of the population over 16. Similar patterns are seen in the racial and ethnic makeup of cybersecurity certificate and degree holders. As seen in figure 2, Hispanic or Latino graduates make up a representative share of certificate and associate degree holders when compared to the population over 16, but that share declines for higher degrees. Asian graduates are overrepresented at all levels of certificates and degrees, and Black or African American graduates make up, on average, about 12% of all degree holders, but there is a small decline in the share of higher-level degrees earned by Black or African American graduates.

Figure 2
Degrees awarded in cybersecurity, by race and ethnicity, 2022
(Percent of total)

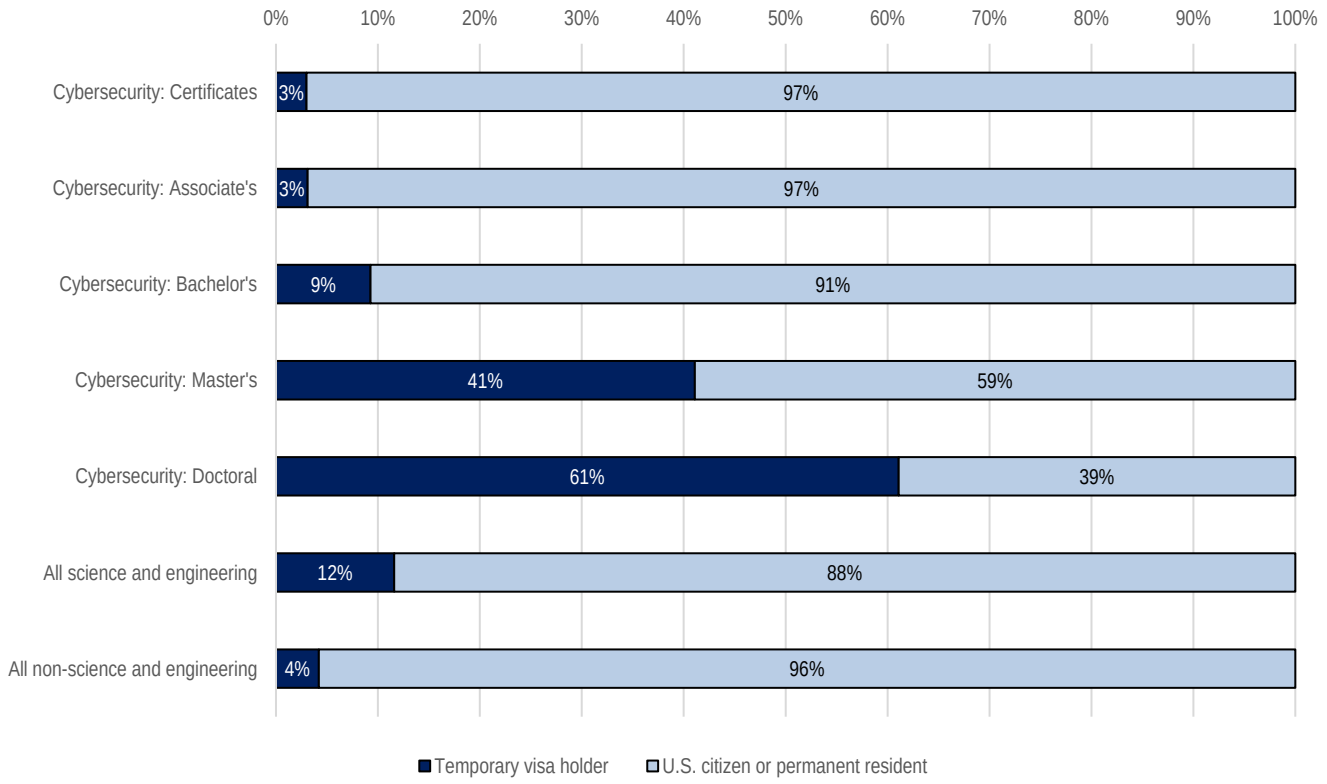


Note(s):
Bar color stacks are sorted from largest to smallest based on associate's degrees with "Unknown race and ethnicity" at the end. Temporary visa holders are excluded from all calculations in Panel 1. The rows "All non-science and engineering" and "All science and engineering" include the following degree levels: associate's degree, bachelor's degree, master's degree, and PhD. Native Hawaiians or Other Pacific Islanders are less than 0.1% of respondents in the survey. Science and engineering degrees awarded based on CIP codes identified by the National Science Foundation.

Source(s):
National Center for Science and Engineering Statistics, Integrated Postsecondary Education Data System (IPEDS), Degrees and Certificates Conferred, available at https://ncsesdata.nsf.gov/builder/ipeds_c, accessed 22 February 2024.

Figure 3 shows the percentage of awards granted to temporary visa holders and to U.S. citizens or permanent residents. Students holding temporary visas, an indicator of international student status, made up 41% of master's degrees and 61% of doctoral degrees granted in 2022. International graduates seeking employment in the United States need employer sponsorship for work visas and may face challenges obtaining the security clearances necessary for federal government and federal contractor jobs, creating a potential obstacle in the pipeline of recent graduates who can fill open cybersecurity positions in the United States.

Figure 3
Degrees awarded in cybersecurity, by visa status, 2022.
(Percent of total)

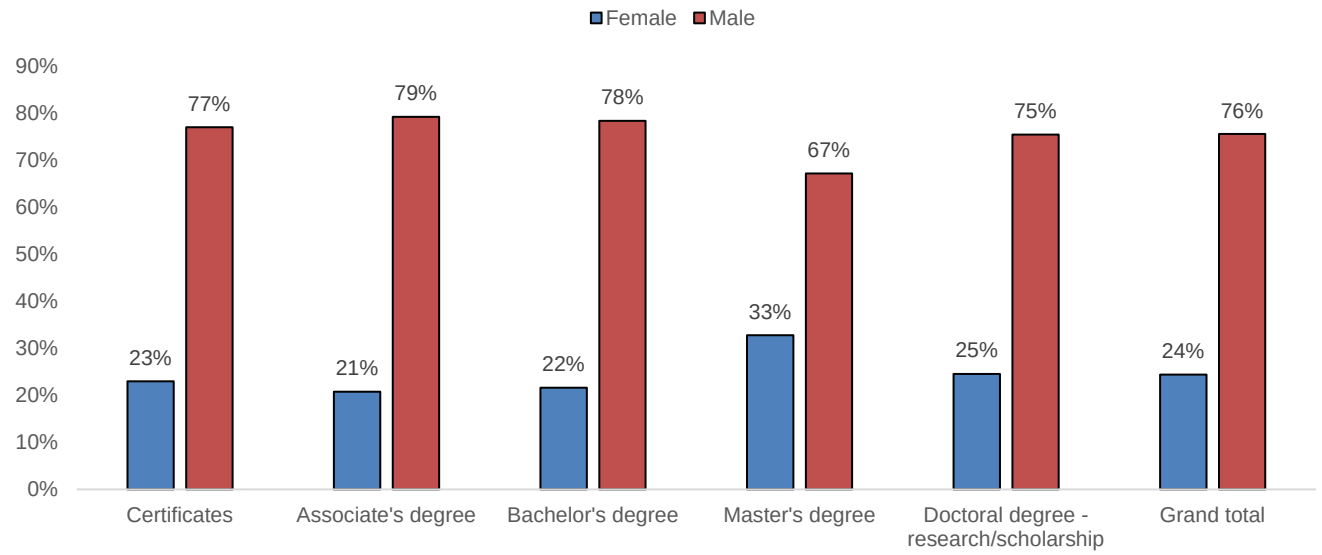


Note: The rows “All non-science and engineering” and “All science and engineering” include the following degree levels: associate’s degree, bachelor’s degree, master’s degree, and PhD. Science and engineering degrees awarded based on CIP codes identified by the National Science Foundation.

Source(s):
National Center for Science and Engineering Statistics, Integrated Postsecondary Education Data System (IPEDS), Degrees and Certificates Conferred, available at https://ncsesdata.nsf.gov/builder/ipeds_c, accessed 22 February 2024.

Figure 4 shows the percentage of awards granted in key, core, and related cybersecurity fields by sex. Most awards were granted to men, so the pipeline of new graduates seeking employment in cybersecurity occupations is primarily male. Data from the ACS (table 5) and the NSCG (table 6), show that more than 70% of current cybersecurity workers are also male. These data indicate that a potential avenue for increasing the supply of cybersecurity workers to meet demand is to engage more women in postsecondary degree programs related to cybersecurity occupations.

Figure 4
Degrees awarded in cybersecurity, by sex: 2022
(Percent)



Source(s):
National Center for Science and Engineering Statistics, Integrated Postsecondary Education Data System (IPEDS), Degrees and Certificates Conferred, available at https://ncsesdata.nsf.gov/builder/ipeds_c, accessed 22 February 2024.

Enrollment in Graduate-Level Cybersecurity Programs

The Survey of Graduate Students and Postdoctorates in Science and Engineering (GSS), collected by NCSES and supported by the National Institutes of Health, provides data on graduate enrollment in science and engineering. In the GSS, CIP code 11.1003, Computer and Information Systems Security/Auditing/Information Assurance, maps to GSS code 413, Computer and Information Systems Security. In 2022, there were 128 GSS institutions enrolling students at the master's or doctoral levels in computer and information systems security, with close to 10,000 graduate students enrolled. Both the number of programs and enrollment increased from 2020 to 2022.

Table 10

Graduate students, postdoctoral researchers, and nonfaculty researchers in computer and information systems security units: 2020–22

(Number)

Characteristics	2020	2021	2022
Institutions with at least one unit	105	115	128
All computer and information systems security	7,293	8,743	9,695
Part time	5,214	6,042	5,962
Full time	2,079	2,701	3,733
Master's	7,023	8,401	9,254
Part time	5,055	5,847	5,791
Full time	1,968	2,554	3,463
Doctoral	270	342	441
Part time	159	195	171
Full time	111	147	270
Postdoctoral researchers	6	9	11
Doctorate-holding nonfaculty researchers	2	18	18

Note(s):

Survey of Graduate Students and Postdoctorates in Science and Engineering (GSS) code 413, Computer and Information Systems Security, includes the Classification of Instructional Programs code of 11.1003, Computer and Information Systems Security/auditing/information assurance per GSS table A-16 (https://ncses.nsf.gov/pubs/nsf23312/table/A-16). Prior to 2020, 11.1003 was collected as part of GSS code 412, computer and information science, not elsewhere classified, https://ncses.nsf.gov/pubs/nsf22319/table/A-18b.

Source(s):

National Center for Science and Engineering Statistics, Survey of Graduate Students and Postdoctorates in Science and Engineering (GSS), Public-Use File: 2020–21.

Estimates of Demand

Estimates of demand for cybersecurity workers include estimates of short-term demand using point-in-time job openings scraped from job boards and estimates of long-term demand using BLS estimates of future job growth. Data show a high level of demand for cybersecurity jobs but a wide range in the number of open jobs. This section covers both private sector and federal employment.

Short-Term Demand

Estimates of short-term demand were obtained by searching current job postings in cybersecurity and related fields. As noted earlier, administrative data providers CyberSeek and ISC2 offered estimates in the range of half a million unfilled cybersecurity positions in the United States in the year 2023, but those estimates represent a sum of all the open positions over a 12-month period and are not comparable to the current, point-in-time estimates. Additionally, ISC2's annual workforce report highlighted headwinds in the industry as it moved into 2024 because many companies reported layoffs in 2023, citing the effects of inflation and the impact of artificial intelligence on cybersecurity jobs. However, many of the data in this section are representative of spring 2024 and show that demand remains high within the sector.

*O*NET*

O*NET estimates short-term demand through scraping the job posting sites CareerOneStop and ZipRecruiter and matching job postings to the SOC codes and job titles used in the O*NET database. On each SOC code's O*NET summary page, there is a section titled "Job Openings on the Web" which returns a list of openings from CareerOneStop and ZipRecruiter that align with the SOC code. As shown in table 11, there were approximately 23,000 openings for information security analysts and high demand in a wide range of additional core occupations. On O*NET, the broad category of "Computer Occupations, All Other" may be further disaggregated, so O*NET shows possible job openings for more detailed cybersecurity occupations such as penetration testers and information security engineers. Table 11 shows the number of search results returned for each SOC code. However, because job postings tend

to contain numerous keywords that cross over numerous SOC codes, jobs may be double-counted, so the data should not be summed to get a total.

Table 11
Number of current openings reported in core cybersecurity fields
(Number)

Occupation title	Occupation code	O*NET job openings
Key cybersecurity		
Information security analysts	15-1212	23,260
Core cybersecurity		
Computer and information systems managers	11-3021	29,496
Computer systems analysts	15-1211	35,531
Computer network support specialists	15-1231	4,662
Computer network architects	15-1241	9,295
Database administrators	15-1242	3,450
Database architects	15-1243	240
Network and computer systems administrators	15-1244	32,440
Computer occupations, all other	15-1299	na
Penetration testers	15-1299.04	147
Information security engineers	15-1299.05	1,451
Blockchain engineers	15-1299.07	29
Computer systems engineers/architects	15-1299.08	64,242

na = not available; data are not available for 15-1299, computer occupations, all other, but are available for 8-digit Standard Occupational Classification codes related to cybersecurity listed below.

Note(s):
Values may include job postings that correspond with multiple occupation titles and codes and should not be summed due to risk of double counting.

Source(s):
O*NET, National Jobs Projections; data are drawn from CareerOneStop and ZipRecruiter, May 2024.

Job Posting Sites

Commercial job sites such as Indeed and LinkedIn return a number of “hits” of open jobs in response to a keyword search. Table 12 shows the terms from the NICE Framework used to search and the number of results that were returned, offering a range of estimates for point-in-time demand for cybersecurity jobs. At the time of the search, there were nearly 116,000 jobs that appeared in the search results for “data security” on Indeed and nearly 70,000 jobs that appeared in the search results for “network security” on LinkedIn. Other search terms, such as “cybersecurity auditor” or “cybersecurity artificial intelligence” returned only hundreds of hits. Again, because of the overlap in key words, the same job postings appeared in the list of hits for multiple searches, so the data cannot be summed to get a total.

Table 12 also shows that the same search term typically returned a vastly different number of results on Indeed compared to LinkedIn. Although jobs can be posted on both sites, the sites differ in the algorithms their search engines use to return results. Because this code is proprietary, it cannot be known how or why the same search term returns different results between the two sites.

Table 12

Job listings, by search term: February 2024

(Number)

Search term	Job postings	
	Indeed	LinkedIn
Cyber security search term		
Cyber security	13,701	54,584
Cyber security threat detection	1,980	930
Cyber security incident response	3,480	1,049
Cyber security encryption	1,206	1,027
Cyber security artificial intelligence	599	1,845
Cyber security cloud security	2,256	1,043
Cyber security identity and access	3,617	1,164
Position type		
Cyber security engineer	4,358	4,024
Cyber security analyst	2,689	4,277
Cyber security auditor	590	202
Seniority level		
Cyber security entry-level	2,573	879
Cyber security senior level	738	1,228
Related concepts		
Network security	14,403	69,853
Information security	14,091	31,783
Data security	115,695	1,989

Source(s):
Indeed.com and LinkedIn.com job postings in the United States, accessed 26 February 2024.

Security Clearances

Federal government and contractor positions in cybersecurity can require a Top Secret/Sensitive Compartmentalized Information clearance, which typically requires sponsorship from an employer. Clearance requirements include that the applicant be a U.S. citizen, undergo an extensive background check and drug screening, and provide other information related to potential security risks.[16] According to ClearanceJobs, a private job posting site for security-cleared professionals, there are currently about 4,000 openings in information technology security for eligible candidates with a security clearance, out of more than 56,000 total openings for security-cleared professionals. As shown in table 13, the employers with the most openings are major federal defense contractors, with the Department of Defense ranking 10th, behind nine contractors, in job openings for cleared professionals in information technology security.

Table 13

Active information technology security jobs postings requiring security clearance, by employer: February 2024

(Number)

Employer	Active job postings
Booz Allen Hamilton	175
ManTech International	173
Leidos	160
Peraton	150
Base One Technologies	136
Lockheed Martin	102
RTX Corporation	97
General Dynamics Information Technology	97
Northrop Grumman	89
Department of Defense	64
SAIC	42

Notes(s):
Table only includes employers with 40 or more openings.

Source(s):
ClearanceJobs.com, accessed 26 February 2024.

When compared to overall job postings for cybersecurity jobs on LinkedIn and Indeed, security clearance jobs make up between 8% and 31% of postings. The wide range of results returned from searches on LinkedIn and Indeed account for this wide gap, making it difficult to precisely estimate how security clearance cybersecurity jobs compare to the overall job market.

Federal Job Openings

The 2023 White House National Cyber Workforce and Education Strategy places an emphasis on strengthening the federal cyber workforce, including improving coordination across agencies to recruit and retain cybersecurity workers. According to USAJOBS.gov, there were 445 job openings for “cyber” and 244 job openings for “cybersecurity” in the federal government in February 2024. When compared to more than 23,000 job openings tracked by O*NET for information security analysts across the private and public sector, and up to 54,000 hits for “cybersecurity” on LinkedIn, federal postings make up between less than 1% to 2% of cybersecurity openings in the market.

Long-Term Demand

BLS reports employment projections by occupation for the upcoming decade.[17] The most recent projections estimated job growth from 2022 to 2032. In the nine SOC codes defined as key and core cybersecurity in this report, BLS estimates a demand for more than 274,000 new jobs, or 11% growth, in the next 10 years, with information security analysts projected to have the fastest growth over the coming decade (table 14). BLS estimates 31.5% job growth among information security analysts, or more than 53,000 new jobs. This outpaces the projected national job growth of 2.8% over the next 10 years. Overall, the position of information security analyst ranks as the fifth-fastest-growing occupation in the BLS projections, ranking behind wind turbine technicians, nurse practitioners, data scientists, and statisticians.

When considering the data from BLS, it is important to note that the data cited are from the 2022 data release. The 2023 data release for the Employment Projections and Occupational Outlook Handbook for the 2023–33 projections cycle is scheduled for 29 August 2024 and will need to be updated.[18]

Table 14

Projections of the national workforce in cybersecurity occupations: 2022 and 2032

(Rank, number in thousands, and percent change)

Occupation title	Occupation code	Rank in employment		Employment (thousands)		Change in employment (thousands)	Percent change in employment
		2022	2032	2022	2032	2022–32	2022–32
All occupations	00-0000	na	na	164,482	169,148	4,665	3
Total across cybersecurity and related occupations	na	na	na	2,554	2,828	274	11
Core cybersecurity							
Information security analysts	15-1212	7	5	169	222	53	32
Cybersecurity-related							
Computer and information systems managers	11-3021	1	1	557	643	86	15
Computer systems analysts	15-1211	2	2	531	583	51	10
Computer occupations, all other	15-1299	3	3	449	493	44	10
Network and computer systems administrators	15-1244	4	4	340	348	8	3
Computer network support specialists	15-1231	6	6	178	190	13	7
Computer network architects	15-1241	5	7	180	187	6	4
Database administrators	15-1242	8	8	85	91	6	7
Database architects	15-1243	9	9	64	70	6	10

Note(s):

Table is sorted on the rank of employment in 2032. Due to slight differences in methodology, the 2022 employment counts differ slightly between the Bureau of Labor Statistic estimates in the Occupational Employment and Wage Statistics and Employment Projections, but the overall trend remains the same.

Source(s):

Bureau of Labor Statistics, Employment Projections (2022).

Currently, information security analysts are projected to have a relatively small overall employment in 2032 (169,000 jobs) within the estimated cybersecurity workforce, but this occupation is projected to grow more quickly than all other occupations within the cybersecurity workforce.

As the information security analyst occupation is expected to grow, BLS and O*NET point out that only 13% of survey respondents hold an associate's degree, whereas the remainder hold bachelor's degrees and postbaccalaureate certificates or advanced degrees. This presents a workforce gap where there is a lack of on-ramps to enter this high-wage, high-growth field.

Short- and Long-Term Demand: Conclusions

This analysis illustrates the challenges of estimating the number of open job postings for cybersecurity workers. First, any analysis resulting from a search of online job boards will be out of date by the next day, at the latest, as organizations are constantly posting, filling, and removing job postings. Additionally, the number of job postings cannot be summed either across job boards or within a single job board. Organizations may post jobs on multiple job boards, so there is duplication, meaning open jobs cannot be summed across job boards. Within a single job board, there is also duplication because different search terms, such as "cybersecurity," "information assurance," and "data security," may turn up some of the same jobs in results. Because job postings contain multiple key words, they cannot be isolated to one search term or one cybersecurity work role. Additionally, a single job opening may be posted across multiple geographic regions to attract remote workers. Although these jobs appear in search results as separate jobs in separate cities, they are not truly separate jobs but rather one remote job tagged in multiple cities to attract candidates from different regions. Furthermore, the search engines for sites like Indeed, LinkedIn, or ZipRecruiter are proprietary, so it cannot be known exactly how the search functions to produce results. Because of these factors, it is difficult to use existing data to obtain a deduplicated number of openings and calculate short-term demand for cybersecurity workers.

Despite the large number of unknowns when using job boards to search for current openings, there are a few conclusions that may be drawn from this analysis. First, because the number of federal openings on USAJOBS numbered in the hundreds where the number of openings on other job sites numbered in the tens of thousands, we can be fairly certain that most of the demand resides in the private sector. Second, despite discussion of layoffs in 2023, the BLS still projects large amounts of growth in the industry by 2032, including a 32% increase in information security analysts.

Findings and Takeaways

This report presents a methodology for estimating supply and demand in the cybersecurity workforce. It also explores data sources that can be used to estimate the size of the current workforce and labor force, the pipeline of new workers, and the short- and long-term demand for workers. However, this methodology does not provide definitive numbers of workers or jobs and is not yet granular enough to estimate the knowledge, skills, and credentials possessed by or needed for the cybersecurity workforce. Existing data and taxonomies make it difficult to accurately estimate supply and demand for cybersecurity workers, resulting in a wide range of values. The current data available are insufficient to accurately portray supply and demand for several reasons.

- The definition of a cybersecurity worker is not solely based on occupations and includes both core workers and adjacent workers who use cybersecurity tools and skills in their work roles. This definition does not yet map one-to-one with traditional delineations of jobs, such as SOC codes, and many emerging roles are not yet captured with existing labor market data. The existing data are based on occupations, rather than job characteristics or work roles. Some SOC definitions, such as “penetration testers,” are included under the “all other” category of computer occupations, and data are not available at a higher level of detail in sources from BLS and the Census Bureau.

- The pipeline of new cybersecurity workers is complex because cybersecurity workers come from a variety of degree or certificate programs and may have work experience prior to entering a cybersecurity work role. Nearly 259,000 degrees and certificates were awarded in fields related to cybersecurity occupations in 2022, but the data do not allow tracking of how many graduates entered the cybersecurity workforce. According to the 2021 NSCG, only 46% of cybersecurity workers with a college degree have a job that is closely related to their degree, whereas the remainder come from a somewhat related or unrelated background.

- Data lags make it difficult to accurately understand the workforce in a rapidly changing professional environment. Many federal data sources rely on data from 2021 or 2022, data from CyberSeek and ISC2 are from 2023, and web scraping job postings is capturing data from 2024. Each source portrays a different point in time in a rapidly changing labor market.

With the data available, we can conclude that estimates of supply and demand for cybersecurity professionals vary widely based on the definition of a cybersecurity job, data source, and data year. Data on the federal workforce is reliable, but openings in the federal government only represent between 1% and 2% of the total jobs available in cybersecurity, depending on the job definition and search criteria.

- Estimates of the existing supply of cybersecurity workers from administrative data providers CyberSeek and ISC2 range between 1,180,000 and 1,340,000, but that encompasses a wide range of jobs and work roles.

- Based on our criteria, the size of the core cybersecurity workforce ranges from 164,000 to as many as 3,492,000 workers, depending on the occupation codes used and data source cited. The wide range of estimates is due to a range of occupations defined by the SOC that have primary or secondary work roles in cybersecurity, but it is currently unknown what percentage of workers in those occupations have those work roles.

- According to the ACS, there were between 2,500 and 74,000 unemployed cybersecurity workers in the United States, representing an unemployment rate between 1% and 2%, depending on the definition. The unemployment rate for cybersecurity workers is lower than that of the adult population, and the labor force participation rate is higher, at nearly 90%.

- International graduate students on temporary visas make up a large share of master's degree recipients, and more than 60% of doctorate recipients in cybersecurity fields and may face obstacles to entering the cybersecurity workforce, including obtaining visa sponsorship.

- Two themes from the expert interviews were that cybersecurity workers may enter the cybersecurity field later in their career and that employers place a premium on experience. Data show a lack of entry-level opportunities for cybersecurity professionals. Additionally, data show fewer opportunities for the skilled technical workforce, as only 13% of job openings in CyberSeek are available to workers with an associate's degree, whereas the remaining 87% require a bachelor's or master's degree.

- Leading administrative data providers show large gaps between demand and supply. CyberSeek estimated a demand of more than 570,000 job openings in the United States for 2023, and the most recent ISC2 cybersecurity workforce study estimated more than 480,000 unfilled job openings over the last calendar year. The estimation methods used for this report produce an estimated range between 25,000 and 259,000 graduates with postsecondary awards in cybersecurity-related fields in 2022, plus between 2,500 and 74,000 unemployed workers actively looking for new work.

- The number of current cybersecurity postings on commercial job sites vary, depending on the site and search terms. In February 2024, openings ranged from nearly 14,000 postings for "cybersecurity" to nearly 116,000 postings for "data security skills" on Indeed and nearly 70,000 postings for "network security" on LinkedIn. O*NET reported 23,000 job openings for information security analysts but more than 64,000 openings for computer systems engineers and architects, a new field not yet captured by traditional labor market data providers. Differences in how jobs are described and how data are collected lead to discrepancies in estimates of current job openings.

Table 15 outlines the various estimates of supply and demand for the cybersecurity workforce, showing the variance between different sources and the low and high estimates for the current size, inflow of workers, short-term, and long-term demand for cybersecurity workers in the U.S.

Table 15
Summary of sources of supply and demand estimates
(Number)

Source and characteristics	Unit	Year	Count	Estimate (low)	Estimate (high)
Supply – current workforce					
CyberSeek	Jobs	2023	1,180,000	na	na
ISC2 Survey	Jobs	2023	1,340,000	na	na
Bureau of Labor Statistics (BLS), Occupational Employment and Wage Statistics (OEWS)	Jobs	2022	na	164,000	2,430,000
National Survey of College Graduates	Individuals	2021	na	126,000	1,885,000
Census Bureau, American Community Survey	Individuals	2022	na	192,000	3,492,000
Supply – inflow					
Department of Education, Integrated Postsecondary Education Data System	Awards	2022	na	25,000	259,000
National Survey of College Graduates	Unemployed individuals	2021	na	D	109,000
Census Bureau, American Community Survey	Unemployed individuals	2022	na	2,500	74,000
Demand					
BLS, OEWS	Job growth	2022–32	na	53,000	274,000
O*NET	Job postings	2024	23,000	na	na
LinkedIn	Job postings	2024	14,000	na	na
Indeed.com	Job postings	2024	55,000	na	na

D = suppressed to avoid disclosure of confidential information; na = not applicable.

Note(s):
Values are rounded to the nearest 1,000. The National Survey of College Graduates workforce estimate cannot be shown due to suppression; 126,000 is the labor force estimate, which is higher than the workforce estimate.

Source(s):
CyberSeek; ISC2 2023 Annual Workforce Survey; Bureau of Labor Statistics, Occupational Employment and Wage Statistics (OEWS) (2022); Census Bureau, American Community Survey (ACS), 1-Year Microdata (2022); Department of Education, National Survey of College Graduates (NSCG) (2021); Department of Education, Integrated Postsecondary Education Data System (IPEDS); O*NET; LinkedIn; Indeed.com.

In the accompanying evaluation of federal data for the CWDI, we conclude that no single federal data source has sufficient granularity and relevance to the cybersecurity workforce. Traditional sources of labor market information that gather data at the individual, household, or institutional level define occupations by SOC codes that have varying degrees of connection to cybersecurity work roles, job titles, and occupations. Future data collections can better capture the cybersecurity workforce by classifying workers based on their cybersecurity knowledge, skills, and work roles and by providing better alignment to the NICE Framework and our definition of cybersecurity work.

Recommendations

Based on current definitions, taxonomies, and data available on the cybersecurity workforce, it is difficult to accurately estimate the supply and demand for cybersecurity workers in the United States using existing data. As a result of this and other CWDI reports, we recommend several actions for the CWDI and NCSES, including collaborating with other federal agencies to improve the understanding of the supply and demand for cybersecurity workers using existing data.

- **Cognitively test if the methodology used by NCSES to measure research, development, and design (R&D) workers is suitable for measuring cybersecurity workers.** NCSES includes questions on the NSCG and other surveys (specifically, the Survey of Doctorate Recipients and the Early Career Doctorate Survey) to measure workers with R&D functions by R&D function

type, not based on their education, degree field, or occupation.[19] These items allow for estimates of whether R&D is a work activity, including if it is a primary or secondary work activity.[20] The item and methodology used for R&D workers thus provides a framework for capturing cybersecurity workers within the core and adjacent (and potentially involved) roles proposed in the CWDI definition report.

- **Examine if NCSES items on certificates, certifications, and licenses are sufficient for understanding the pathways of the cybersecurity workforce.** Both the NSCG and the National Training, Education, and Workforce Survey (NTEWS) include items on certifications and licenses, which may be important pathways into the cybersecurity workforce.

- **Merge the NICE Framework with O*NET.** Currently, O*NET contains knowledge, skills, and work activities that could potentially be matched with the knowledge, skills, and work roles outlined in the NICE Framework. A data-driven analysis could better identify SOC codes for core, involved, and adjacent cybersecurity occupations, as well as the share of knowledge, skills, and work roles that align with those in the NICE Framework using current SOC codes.

- **Improve the SOC taxonomy to better reflect cybersecurity workers.** The existing SOC framework was developed in 2018 and is due to be revised for a publication in 2028 to reflect new job roles. This would allow researchers to better estimate supply at a granular level. Currently, many key work roles fall under occupation codes that are "all other" or rolled up to a higher level of aggregation. Clearer SOC codes will allow for more detailed analysis of data from sources including BLS and the Census Bureau.

- **Improve the CIP taxonomy to better reflect the supply of cybersecurity workers.** As the number of postsecondary certificates and degree programs increases, additional detail will provide information on the types of credentials related to cybersecurity being awarded each year. New CIP codes and GSS codes added in 2020 better capture cybersecurity, and more data will continue to come in future surveys as new graduates enter the workforce.

Additionally, a future survey of cybersecurity workers would help to better understand the workforce pipeline and the steps that workers take to enter the field. Based on the rapid growth of cybersecurity and related degrees and certificates awarded, there is a large cohort of potential workers entering the field, but information about their career pathways is unclear considering the years of work experience, additional certificates and credentials, and types of job titles and occupations that formed their trajectory into the cybersecurity profession.

Appendix A: Academic Data

Table A-1

CIP-to-SOC code mapping

(SOC and CIP codes with titles and CIP definition)

SOC code	SOC title	CIP code	CIP title	Cybersecurity status	CIP definition
11-3021	Computer and Information Systems Managers	11.0101	Computer and Information Sciences, General	Adjacent	A general program that focuses on computing, computer science, and information science and systems. Such programs are undifferentiated as to title and content and are not to be confused with specific programs in computer science, information science, or related support services.
		11.0103	Information Technology	Related	A program that focuses on the design of technological information systems, including computing systems, as solutions to business and research data and communications support needs. Includes instruction in the principles of computer hardware and software components, algorithms, databases, telecommunications, user tactics, application testing, and human interface design.
		11.0401	Information Science/Studies	Adjacent	A program that focuses on the theory, organization, and process of information collection, transmission, and utilization in traditional and electronic forms. Includes instruction in information classification and organization; information storage and processing; transmission, transfer, and signaling; communications and networking; systems planning and design; human interfacing and use analysis; database development; information policy analysis; and related aspects of hardware, software, economics, social factors, and capacity.
		11.0701	Computer Science	Adjacent	A program that focuses on computer theory, computing problems and solutions, and the design of computer systems and user interfaces from a scientific perspective. Includes instruction in the principles of computational science, computer development and programming, and applications to a variety of end-use situations.
		11.0802	Data Modeling/Warehousing and Database Administration	Related	A program that prepares individuals to design and manage the construction of databases and related software programs and applications, including the linking of individual data sets to create complex searchable databases (warehousing) and the use of analytical search tools (mining). Includes instruction in database theory, logic, and semantics; operational and warehouse modeling; dimensionality; attributes and hierarchies; data definition; technical architecture; access and security design; integration; formatting and extraction; data delivery; index design; implementation problems; planning and budgeting; and client and networking issues.

SOC code	SOC title	CIP code	CIP title	Cybersecurity status	CIP definition
		11.0901	Computer Systems Networking and Telecommunications	Core	A program that focuses on the design, implementation, and management of linked systems of computers, peripherals, and associated software to maximize efficiency and productivity, and that prepares individuals to function as network specialists and managers at various levels. Includes instruction in operating systems and applications; systems design and analysis; networking theory and solutions; types of networks; network management and control; network and flow optimization; security; configuring; and troubleshooting.
		11.1001	Network and System Administration/Administrator	Core	A program that prepares individuals to manage the computer operations and control the system configurations emanating from a specific site or network hub. Includes instruction in computer hardware, software, and applications; local area (LAN) and wide area (WAN) networking; principles of information systems security; disk space and traffic load monitoring; data backup; resource allocation; and setup and takedown procedures.
		11.1002	System, Networking, and LAN/WAN Management/Manager	Core	A program that prepares individuals to oversee and regulate the computer system and performance requirements of an entire organization or network of satellite users. Includes instruction in performance balancing; redundancy; local area (LAN) and wide area (WAN) network management; system migration and upgrading; outage control; problem diagnosis and troubleshooting; and system maintenance, budgeting, and management.
		11.1003	Computer and Information Systems Security/Auditing/Information Assurance	Key	A program that prepares individuals to assess the security needs of computer and network systems, recommend safeguard solutions, and manage the implementation, auditing, and maintenance of security devices, systems, and procedures. Includes instruction in computer architecture, programming, and systems analysis; networking; telecommunications; cryptography; security system auditing and design; applicable law and regulations; risk assessment and policy analysis; contingency planning; user access issues; investigation techniques; and troubleshooting.
		11.1005	Information Technology Project Management	Core	A program that prepares individuals to design, develop, and manage information technology projects in a variety of companies and organizations. Includes instruction in principles of project management, risk management, procurement and contract management, information security management, software management, organizational principles and behavior, communications, quality assurance, financial analysis, leadership, and team effectiveness.

SOC code	SOC title	CIP code	CIP title	Cybersecurity status	CIP definition
		30.0801	Mathematics and Computer Science	Not related	A program with a general synthesis of mathematics and computer science or a specialization which draws from mathematics and computer science.
		30.1601	Accounting and Computer Science	Not related	A program that combines accounting with computer science and/or computer studies.
		30.3101	Human Computer Interaction	Related	An interdisciplinary program that focuses on the study of the interaction between people and technology and how that technology impacts society and combines disciplines within the fields of computing and information science (information systems, software engineering, artificial intelligence and design), engineering, and the behavior sciences (cognitive science, cognitive psychology, sociology, organizational psychology, and social psychology). Includes instruction in information technology, cognitive and behavioral sciences, and systems design.
		30.3901	Economics and Computer Science	Not related	A program of study that focuses on the theoretical and practical connections between computer science and economics. Includes instruction in data analysis, database design, data mining, computer algorithms, economics, econometrics, computer programing, mathematics, and statistics.
		30.7001	Data Science, General	Not related	A program that focuses on the analysis of large-scale data sources from the interdisciplinary perspectives of applied statistics, computer science, data storage, data representation, data modeling, mathematics, and statistics. Includes instruction in computer algorithms, computer programming, data management, data mining, information policy, information retrieval, mathematical modeling, quantitative analysis, statistics, trend spotting, and visual analytics.
		52.0205	Operations Management and Supervision	Not related	A program that prepares individuals to manage and direct the physical and/or technical functions of a firm or organization, particularly those relating to development, production, and manufacturing. Includes instruction in principles of general management, manufacturing and production systems, plant management, equipment maintenance management, production control, industrial labor relations and skilled trades supervision, strategic manufacturing policy, systems analysis, productivity analysis and cost control, and materials planning.

SOC code	SOC title	CIP code	CIP title	Cybersecurity status	CIP definition
		52.1201	Management Information Systems, General	Related	A program that generally prepares individuals to provide and manage data systems and related facilities for processing and retrieving internal business information; select systems and train personnel; and respond to external data requests. Includes instruction in cost and accounting information systems, management control systems, personnel information systems, data storage and security, business systems networking, report preparation, computer facilities and equipment operation and maintenance, operator supervision and training, and management information systems policy and planning.
		52.1206	Information Resources Management	Related	A program that prepares individuals to apply principles of information technology, computer systems management, and business operations to the planning, management, and evaluation of information services in organizations. Includes instruction in telecommunications, systems planning and integration, information policy, information security, contracting and purchasing, budgeting, information technology, operations management, human resources, communications skills, and applicable law and regulations.
		52.1207	Knowledge Management	Not related	A program that focuses on the study of knowledge management in government agencies and corporations for the purpose of supporting stated organizational goals and objectives and prepares individuals to function as information resource managers. Includes instruction in information technology, principles of computer and information systems, management information systems, applicable policy and regulations, and operations and personnel management.
		52.1299	Management Information Systems and Services, Other	Not related	Any program in business information and data processing services not listed above.
		52.2101	Telecommunications Management	Related	A program that prepares individuals to apply business skills to design, implement, and manage the voice, video, and data networking systems of organizations. Includes instruction in telecommunications concepts and technologies, network operations and management, wireless communications and mobile computing, cybersecurity, regulation and public policy, business practices and management, and written and oral communications.
15-1211	Computer Systems Analysts	11.0101	Computer and Information Sciences, General	Adjacent	A general program that focuses on computing, computer science, and information science and systems. Such programs are undifferentiated as to title and content and are not to be confused with specific programs in computer science, information science, or related support services.

SOC code	SOC title	CIP code	CIP title	Cybersecurity status	CIP definition
		11.0103	Information Technology	Related	A program that focuses on the design of technological information systems, including computing systems, as solutions to business and research data and communications support needs. Includes instruction in the principles of computer hardware and software components, algorithms, databases, telecommunications, user tactics, application testing, and human interface design.
		11.0501	Computer Systems Analysis/Analyst	Related	A program that prepares individuals to apply programming and systems analysis principles to the selection, implementation, and troubleshooting of customized computer and software installations across the life cycle. Includes instruction in computer hardware and software; compilation, composition, execution, and operating systems; low- and high-level languages and language programming; programming and debugging techniques; installation and maintenance testing and documentation; process and data flow analysis; user needs analysis and documentation; cost-benefit analysis; and specification design.
		11.0901	Computer Systems Networking and Telecommunications	Core	A program that focuses on the design, implementation, and management of linked systems of computers, peripherals, and associated software to maximize efficiency and productivity, and that prepares individuals to function as network specialists and managers at various levels. Includes instruction in operating systems and applications; systems design and analysis; networking theory and solutions; types of networks; network management and control; network and flow optimization; security; configuring; and troubleshooting.
15-1212	Information Security Analysts	11.0103	Information Technology	Related	A program that focuses on the design of technological information systems, including computing systems, as solutions to business and research data and communications support needs. Includes instruction in the principles of computer hardware and software components, algorithms, databases, telecommunications, user tactics, application testing, and human interface design.
		11.0701	Computer Science	Adjacent	A program that focuses on computer theory, computing problems and solutions, and the design of computer systems and user interfaces from a scientific perspective. Includes instruction in the principles of computational science, computer development and programming, and applications to a variety of end-use situations.

SOC code	SOC title	CIP code	CIP title	Cybersecurity status	CIP definition
		11.0901	Computer Systems Networking and Telecommunications	Core	A program that focuses on the design, implementation, and management of linked systems of computers, peripherals, and associated software to maximize efficiency and productivity, and that prepares individuals to function as network specialists and managers at various levels. Includes instruction in operating systems and applications; systems design and analysis; networking theory and solutions; types of networks; network management and control; network and flow optimization; security; configuring; and troubleshooting.
		11.1001	Network and System Administration/Administrator	Core	A program that prepares individuals to manage the computer operations and control the system configurations emanating from a specific site or network hub. Includes instruction in computer hardware, software, and applications; local area (LAN) and wide area (WAN) networking; principles of information systems security; disk space and traffic load monitoring; data backup; resource allocation; and setup and takedown procedures.
		11.1002	System, Networking, and LAN/WAN Management/Manager	Core	A program that prepares individuals to oversee and regulate the computer system and performance requirements of an entire organization or network of satellite users. Includes instruction in performance balancing; redundancy; local area (LAN) and wide area (WAN) network management; system migration and upgrading; outage control; problem diagnosis and troubleshooting; and system maintenance, budgeting, and management.
		11.1003	Computer and Information Systems Security/Auditing/Information Assurance	Key	A program that prepares individuals to assess the security needs of computer and network systems, recommend safeguard solutions, and manage the implementation, auditing, and maintenance of security devices, systems, and procedures. Includes instruction in computer architecture, programming, and systems analysis; networking; telecommunications; cryptography; security system auditing and design; applicable law and regulations; risk assessment and policy analysis; contingency planning; user access issues; investigation techniques; and troubleshooting.
		11.1005	Information Technology Project Management	Core	A program that prepares individuals to design, develop, and manage information technology projects in a variety of companies and organizations. Includes instruction in principles of project management, risk management, procurement and contract management, information security management, software management, organizational principles and behavior, communications, quality assurance, financial analysis, leadership, and team effectiveness.

SOC code	SOC title	CIP code	CIP title	Cybersecurity status	CIP definition
		43.0403	Cyber/Computer Forensics and Counterterrorism	Core	A program focusing on the principles and techniques used to identify, search, seize and analyze digital media and to conduct cyber investigations against criminal and terrorist activity. Includes instruction in computer boot processes and drives, jumper setting, file access and reconstruction, hacking, network systems, cryptography, programming, investigative techniques, forensic imagery, web-based investigation methods, cyberterrorism, and applicable laws and administrative procedures.
		51.0723	Healthcare Information Privacy Assurance and Security	Core	A program that prepares individuals for careers in designing, implementing, and administering comprehensive privacy and security protection programs in all types of healthcare organizations. Includes instruction in health information ethics, healthcare information privacy and security, healthcare compliance, healthcare information security and disaster recovery, and healthcare privacy law.
15-1231	Computer Network Support Specialists	11.0201	Computer Programming/Programmer, General	Adjacent	A program that focuses on the general writing and implementation of generic and customized programs to drive operating systems and that generally prepares individuals to apply the methods and procedures of software design and programming to software installation and maintenance. Includes instruction in software design, low- and high-level languages and program writing; program customization and linking; prototype testing; troubleshooting; and related aspects of operating systems and networks.
		11.0501	Computer Systems Analysis/Analyst	Related	A program that prepares individuals to apply programming and systems analysis principles to the selection, implementation, and troubleshooting of customized computer and software installations across the life cycle. Includes instruction in computer hardware and software; compilation, composition, execution, and operating systems; low- and high-level languages and language programming; programming and debugging techniques; installation and maintenance testing and documentation; process and data flow analysis; user needs analysis and documentation; cost-benefit analysis; and specification design.
		11.0701	Computer Science	Adjacent	A program that focuses on computer theory, computing problems and solutions, and the design of computer systems and user interfaces from a scientific perspective. Includes instruction in the principles of computational science, computer development and programming, and applications to a variety of end-use situations.

SOC code	SOC title	CIP code	CIP title	Cybersecurity status	CIP definition
		11.0901	Computer Systems Networking and Telecommunications	Core	A program that focuses on the design, implementation, and management of linked systems of computers, peripherals, and associated software to maximize efficiency and productivity, and that prepares individuals to function as network specialists and managers at various levels. Includes instruction in operating systems and applications; systems design and analysis; networking theory and solutions; types of networks; network management and control; network and flow optimization; security; configuring; and troubleshooting.
		11.0902	Cloud Computing	Related	A program that prepares individuals to design and implement enterprise software systems that rely on distributed computing and service-oriented architecture, including databases, web services, cloud computing, and mobile apps. Includes instruction in data management, distributed and cloud computing, enterprise software architecture, enterprise and cloud security, mobile systems and applications, server administration, and web development.
		11.1001	Network and System Administration/Administrator	Core	A program that prepares individuals to manage the computer operations and control the system configurations emanating from a specific site or network hub. Includes instruction in computer hardware, software, and applications; local area (LAN) and wide area (WAN) networking; principles of information systems security; disk space and traffic load monitoring; data backup; resource allocation; and setup and takedown procedures.
		11.1002	System, Networking, and LAN/WAN Management/Manager	Core	A program that prepares individuals to oversee and regulate the computer system and performance requirements of an entire organization or network of satellite users. Includes instruction in performance balancing; redundancy; local area (LAN) and wide area (WAN) network management; system migration and upgrading; outage control; problem diagnosis and troubleshooting; and system maintenance, budgeting, and management.
		11.1003	Computer and Information Systems Security/Auditing/Information Assurance	Key	A program that prepares individuals to assess the security needs of computer and network systems, recommend safeguard solutions, and manage the implementation, auditing, and maintenance of security devices, systems, and procedures. Includes instruction in computer architecture, programming, and systems analysis; networking; telecommunications; cryptography; security system auditing and design; applicable law and regulations; risk assessment and policy analysis; contingency planning; user access issues; investigation techniques; and troubleshooting.

SOC code	SOC title	CIP code	CIP title	Cybersecurity status	CIP definition
		11.1006	Computer Support Specialist	Related	A program that prepares individuals to provide technical assistance, support, and advice to computer users to help troubleshoot software and hardware problems. Includes instruction in computer concepts, information systems, networking, operating systems, computer hardware, the Internet, software applications, help desk concepts and problem solving, and principles of customer service.
15-1241	Computer Network Architects	11.0101	Computer and Information Sciences, General	Adjacent	A general program that focuses on computing, computer science, and information science and systems. Such programs are undifferentiated as to title and content and are not to be confused with specific programs in computer science, information science, or related support services.
		11.0103	Information Technology	Related	A program that focuses on the design of technological information systems, including computing systems, as solutions to business and research data and communications support needs. Includes instruction in the principles of computer hardware and software components, algorithms, databases, telecommunications, user tactics, application testing, and human interface design.
		11.0501	Computer Systems Analysis/Analyst	Related	A program that prepares individuals to apply programming and systems analysis principles to the selection, implementation, and troubleshooting of customized computer and software installations across the life cycle. Includes instruction in computer hardware and software; compilation, composition, execution, and operating systems; low- and high-level languages and language programming; programming and debugging techniques; installation and maintenance testing and documentation; process and data flow analysis; user needs analysis and documentation; cost-benefit analysis; and specification design.
		11.0901	Computer Systems Networking and Telecommunications	Core	A program that focuses on the design, implementation, and management of linked systems of computers, peripherals, and associated software to maximize efficiency and productivity, and that prepares individuals to function as network specialists and managers at various levels. Includes instruction in operating systems and applications; systems design and analysis; networking theory and solutions; types of networks; network management and control; network and flow optimization; security; configuring; and troubleshooting.

SOC code	SOC title	CIP code	CIP title	Cybersecurity status	CIP definition
		11.0902	Cloud Computing	Related	A program that prepares individuals to design and implement enterprise software systems that rely on distributed computing and service-oriented architecture, including databases, web services, cloud computing, and mobile apps. Includes instruction in data management, distributed and cloud computing, enterprise software architecture, enterprise and cloud security, mobile systems and applications, server administration, and web development.
		11.1001	Network and System Administration/Administrator	Core	A program that prepares individuals to manage the computer operations and control the system configurations emanating from a specific site or network hub. Includes instruction in computer hardware, software, and applications; local area (LAN) and wide area (WAN) networking; principles of information systems security; disk space and traffic load monitoring; data backup; resource allocation; and setup and takedown procedures.
		11.1003	Computer and Information Systems Security/Auditing/Information Assurance	Key	A program that prepares individuals to assess the security needs of computer and network systems, recommend safeguard solutions, and manage the implementation, auditing, and maintenance of security devices, systems, and procedures. Includes instruction in computer architecture, programming, and systems analysis; networking; telecommunications; cryptography; security system auditing and design; applicable law and regulations; risk assessment and policy analysis; contingency planning; user access issues; investigation techniques; and troubleshooting.
		14.0901	Computer Engineering, General	Related	A program that generally prepares individuals to apply mathematical and scientific principles to the design, development and operational evaluation of computer hardware and software systems and related equipment and facilities; and the analysis of specific problems of computer applications to various tasks.
		14.0999	Computer Engineering, Other	Related	Any instructional program in computer engineering not listed above.
15-1242	Database Administrators	11.0101	Computer and Information Sciences, General	Adjacent	A general program that focuses on computing, computer science, and information science and systems. Such programs are undifferentiated as to title and content and are not to be confused with specific programs in computer science, information science, or related support services.

SOC code	SOC title	CIP code	CIP title	Cybersecurity status	CIP definition
		11.0802	Data Modeling/Warehousing and Database Administration	Related	A program that prepares individuals to design and manage the construction of databases and related software programs and applications, including the linking of individual data sets to create complex searchable databases (warehousing) and the use of analytical search tools (mining). Includes instruction in database theory, logic, and semantics; operational and warehouse modeling; dimensionality; attributes and hierarchies; data definition; technical architecture; access and security design; integration; formatting and extraction; data delivery; index design; implementation problems; planning and budgeting; and client and networking issues.
		11.1003	Computer and Information Systems Security/Auditing/Information Assurance	Key	A program that prepares individuals to assess the security needs of computer and network systems, recommend safeguard solutions, and manage the implementation, auditing, and maintenance of security devices, systems, and procedures. Includes instruction in computer architecture, programming, and systems analysis; networking; telecommunications; cryptography; security system auditing and design; applicable law and regulations; risk assessment and policy analysis; contingency planning; user access issues; investigation techniques; and troubleshooting.
15-1243	Database Architects	11.0101	Computer and Information Sciences, General	Adjacent	A general program that focuses on computing, computer science, and information science and systems. Such programs are undifferentiated as to title and content and are not to be confused with specific programs in computer science, information science, or related support services.
		11.0103	Information Technology	Related	A program that focuses on the design of technological information systems, including computing systems, as solutions to business and research data and communications support needs. Includes instruction in the principles of computer hardware and software components, algorithms, databases, telecommunications, user tactics, application testing, and human interface design.
		11.0401	Information Science/Studies	Adjacent	A program that focuses on the theory, organization, and process of information collection, transmission, and utilization in traditional and electronic forms. Includes instruction in information classification and organization; information storage and processing; transmission, transfer, and signaling; communications and networking; systems planning and design; human interfacing and use analysis; database development; information policy analysis; and related aspects of hardware, software, economics, social factors, and capacity.

SOC code	SOC title	CIP code	CIP title	Cybersecurity status	CIP definition
		11.0501	Computer Systems Analysis/Analyst	Related	A program that prepares individuals to apply programming and systems analysis principles to the selection, implementation, and troubleshooting of customized computer and software installations across the life cycle. Includes instruction in computer hardware and software; compilation, composition, execution, and operating systems; low- and high-level languages and language programming; programming and debugging techniques; installation and maintenance testing and documentation; process and data flow analysis; user needs analysis and documentation; cost-benefit analysis; and specification design.
		11.0701	Computer Science	Adjacent	A program that focuses on computer theory, computing problems and solutions, and the design of computer systems and user interfaces from a scientific perspective. Includes instruction in the principles of computational science, computer development and programming, and applications to a variety of end-use situations.
		11.0802	Data Modeling/Warehousing and Database Administration	Related	A program that prepares individuals to design and manage the construction of databases and related software programs and applications, including the linking of individual data sets to create complex searchable databases (warehousing) and the use of analytical search tools (mining). Includes instruction in database theory, logic, and semantics; operational and warehouse modeling; dimensionality; attributes and hierarchies; data definition; technical architecture; access and security design; integration; formatting and extraction; data delivery; index design; implementation problems; planning and budgeting; and client and networking issues.
		11.0902	Cloud Computing	Related	A program that prepares individuals to design and implement enterprise software systems that rely on distributed computing and service-oriented architecture, including databases, web services, cloud computing, and mobile apps. Includes instruction in data management, distributed and cloud computing, enterprise software architecture, enterprise and cloud security, mobile systems and applications, server administration, and web development.

SOC code	SOC title	CIP code	CIP title	Cybersecurity status	CIP definition
		11.1003	Computer and Information Systems Security/Auditing/Information Assurance	Key	A program that prepares individuals to assess the security needs of computer and network systems, recommend safeguard solutions, and manage the implementation, auditing, and maintenance of security devices, systems, and procedures. Includes instruction in computer architecture, programming, and systems analysis; networking; telecommunications; cryptography; security system auditing and design; applicable law and regulations; risk assessment and policy analysis; contingency planning; user access issues; investigation techniques; and troubleshooting.
		14.0901	Computer Engineering, General	Related	A program that generally prepares individuals to apply mathematical and scientific principles to the design, development and operational evaluation of computer hardware and software systems and related equipment and facilities; and the analysis of specific problems of computer applications to various tasks.
		14.0903	Computer Software Engineering	Related	A program that prepares individuals to apply scientific and mathematical principles to the design, analysis, verification, validation, implementation, and maintenance of computer software systems using a variety of computer languages. Includes instruction in discrete mathematics, probability and statistics, computer science, managerial science, and applications to complex computer systems.
		14.2701	Systems Engineering	Related	A program that prepares individuals to apply mathematical and scientific principles to the design, development and operational evaluation of total systems solutions to a wide variety of engineering problems, including the integration of human, physical, energy, communications, management, and information requirements as needed, and the application of requisite analytical methods to specific situations.
		30.7001	Data Science, General	Not related	A program that focuses on the analysis of large-scale data sources from the interdisciplinary perspectives of applied statistics, computer science, data storage, data representation, data modeling, mathematics, and statistics. Includes instruction in computer algorithms, computer programming, data management, data mining, information policy, information retrieval, mathematical modeling, quantitative analysis, statistics, trend spotting, and visual analytics.
		30.7099	Data Science, Other	Not related	Any instructional program in data science not listed above.

SOC code	SOC title	CIP code	CIP title	Cybersecurity status	CIP definition
		52.1201	Management Information Systems, General	Related	A program that generally prepares individuals to provide and manage data systems and related facilities for processing and retrieving internal business information; select systems and train personnel; and respond to external data requests. Includes instruction in cost and accounting information systems, management control systems, personnel information systems, data storage and security, business systems networking, report preparation, computer facilities and equipment operation and maintenance, operator supervision and training, and management information systems policy and planning.
15-1244	Network and Computer Systems Administrators	11.0101	Computer and Information Sciences, General	Adjacent	A general program that focuses on computing, computer science, and information science and systems. Such programs are undifferentiated as to title and content and are not to be confused with specific programs in computer science, information science, or related support services.
		11.1001	Network and System Administration/Administrator	Core	A program that prepares individuals to manage the computer operations and control the system configurations emanating from a specific site or network hub. Includes instruction in computer hardware, software, and applications; local area (LAN) and wide area (WAN) networking; principles of information systems security; disk space and traffic load monitoring; data backup; resource allocation; and setup and takedown procedures.
		11.1003	Computer and Information Systems Security/Auditing/Information Assurance	Key	A program that prepares individuals to assess the security needs of computer and network systems, recommend safeguard solutions, and manage the implementation, auditing, and maintenance of security devices, systems, and procedures. Includes instruction in computer architecture, programming, and systems analysis; networking; telecommunications; cryptography; security system auditing and design; applicable law and regulations; risk assessment and policy analysis; contingency planning; user access issues; investigation techniques; and troubleshooting.
15-1299	Computer Occupations, All Other	11.0101	Computer and Information Sciences, General	Adjacent	A general program that focuses on computing, computer science, and information science and systems. Such programs are undifferentiated as to title and content and are not to be confused with specific programs in computer science, information science, or related support services.

SOC code	SOC title	CIP code	CIP title	Cybersecurity status	CIP definition
		11.0301	Data Processing and Data Processing Technology/Technician	Not related	A program that prepares individuals to master and use computer software programs and applications for inputting, verifying, organizing, storing, retrieving, transforming (changing, updating, and deleting), and extracting information. Includes instruction in using various operating system configurations and in types of data entry such as word processing, spreadsheets, calculators, management programs, design programs, database programs, and research programs.
		11.0401	Information Science/Studies	Adjacent	A program that focuses on the theory, organization, and process of information collection, transmission, and utilization in traditional and electronic forms. Includes instruction in information classification and organization; information storage and processing; transmission, transfer, and signaling; communications and networking; systems planning and design; human interfacing and use analysis; database development; information policy analysis; and related aspects of hardware, software, economics, social factors, and capacity.
		11.0701	Computer Science	Adjacent	A program that focuses on computer theory, computing problems and solutions, and the design of computer systems and user interfaces from a scientific perspective. Includes instruction in the principles of computational science, computer development and programming, and applications to a variety of end-use situations.
		11.1005	Information Technology Project Management	Core	A program that prepares individuals to design, develop, and manage information technology projects in a variety of companies and organizations. Includes instruction in principles of project management, risk management, procurement and contract management, information security management, software management, organizational principles and behavior, communications, quality assurance, financial analysis, leadership, and team effectiveness.
		26.1103	Bioinformatics	Not related	A program that focuses on the application of computer-based technologies and services to biological, biomedical, and biotechnology research. Includes instruction in algorithms, network architecture, principles of software design, human interface design, usability studies, search strategies, database management and data mining, digital image processing, computer graphics and animation, CAD, computer programming, and applications to experimental design and analysis and to specific quantitative, modeling, and analytical studies in the various biological specializations.

SOC code	SOC title	CIP code	CIP title	Cybersecurity status	CIP definition
		26.1104	Computational Biology	Not related	A program that focuses on computational theoretical approaches to understanding biological systems, including computational models of biological processes, computational management of large-scale projects, database development and data-algorithm development, and high-performance computing, as well as statistical and mathematical analyses.
		30.0801	Mathematics and Computer Science	Not related	A program with a general synthesis of mathematics and computer science or a specialization which draws from mathematics and computer science.
		30.1601	Accounting and Computer Science	Not related	A program that combines accounting with computer science and/or computer studies.
		30.3001	Computational Science	Not related	A program that focuses on the study of scientific computing and its application. Includes instruction in scientific visualization, multi-scale analysis, grid generation, data analysis, applied mathematics, numerical algorithms, high-performance parallel computing, and numerical modeling and simulation with applications in science, engineering and other disciplines in which computation plays an integral role.
		30.3101	Human Computer Interaction	Related	An interdisciplinary program that focuses on the study of the interaction between people and technology and how that technology impacts society and combines disciplines within the fields of computing and information science (information systems, software engineering, artificial intelligence and design), engineering, and the behavior sciences (cognitive science, cognitive psychology, sociology, organizational psychology, and social psychology). Includes instruction in information technology, cognitive and behavioral sciences, and systems design.
		40.0512	Cheminformatics/Chemistry Informatics	Not related	A program that focuses on applying computer science approaches in the representation, analysis, design, and modeling of chemical structures and associated metadata, such as biological activity endpoints and physicochemical properties. Includes instruction in chemical information technology, computational chemistry, computer science, database design, molecular modeling, scientific computing, and statistics.

SOC code	SOC title	CIP code	CIP title	Cybersecurity status	CIP definition
		43.0403	Cyber/Computer Forensics and Counterterrorism	Core	A program focusing on the principles and techniques used to identify, search, seize and analyze digital media and to conduct cyber investigations against criminal and terrorist activity. Includes instruction in computer boot processes and drives, jumper setting, file access and reconstruction, hacking, network systems, cryptography, programming, investigative techniques, forensic imagery, web-based investigation methods, cyberterrorism, and applicable laws and administrative procedures.
		51.2706	Medical Informatics	Not related	A program that focuses on the application of computer science and software engineering to medical research and clinical information technology support, and the development of advanced imaging, database, and decision systems. Includes instruction in computer science, health information systems architecture, medical knowledge structures, medical language and image processing, quantitative medical decision modeling, imaging techniques, electronic medical records, medical research systems, clinical decision support, and informatics aspects of specific research and practice problems.
NA	NA	43.0303	Critical Infrastructure Protection	Core	A program focusing on the design, planning and management of systems and procedures for protecting critical national physical and cyber infrastructure from external threats, including terrorism. Includes instruction in homeland security policy, critical infrastructure policy, information security, matrix vulnerability assessment, threat assessment, physical security, personnel security, operational security, contingency planning, case analyses of specific industries and systems, redundancy planning, emergency and disaster planning, security systems, and intelligence operations.
	NA	43.0404	Cybersecurity Defense Strategy/Policy	Core	A program that focuses on the study of strategy, policy, and standards regarding the security of and operations in cyberspace. Includes instruction in incident response, information assurance, recovery policies, vulnerability reduction, deterrence, threat reduction, and resiliency.

NA = not available.
CIP = Classification of Instructional Programs; SOC = Standard Occupational Classification.

Source(s):
Bureau of Labor Statistics, SOC 2018 codes and titles; National Center for Education Statistics, CIP 2020 codes, titles, and definitions; and National Center for Science and Engineering Statistics, Cybersecurity Workforce Data Initiative (CWDI).

Notes

[1] Hudnall M. 2019. Educational and Workforce Cybersecurity Frameworks: Comparing, Contrasting, and Mapping. *Curricular Foundations for Cybersecurity* 52(3):18–28.

[2] Burrell DN. 2020. An Exploration of the Cybersecurity Workforce Shortage. *In* Information Resources Management Association, editor, *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications*, pp. 1072–81. Hershey, PA: IGI Global. Lyon V. 2020. *Exploring Strategies for Recruiting and Retaining Diverse Cybersecurity Professionals.* Unpublished doctoral dissertation, Walden University. Mountrouidou X, Vosen D, Kari C, Azhar MQ, Bhatia A, Gagne G, Maguire J, Tudor L, Yuen TT. 2018. Securing the Human: A Review of Literature on Broadening Diversity in Cybersecurity Education. *Proceedings of the Working Group Reports on Innovation and Technology in Computer Science Education*, pp. 157–76.

[3] National Science Board (NSB), National Science Foundation. 2024. *Science and Engineering Indicators 2024: The State of U.S. Science and Engineering*. NSB-2024-3. Alexandria, VA. Available at https://ncses.nsf.gov/pubs/nsb20243. National Science Board, National Science Foundation. 2024. The STEM Labor Force: Scientists, Engineers, and Technical Workers. Science and Engineering Indicators 2024. NSB-2024-5. Alexandria, VA. Available at https://ncses.nsf.gov/pubs/nsb20245/. National Science Board (NSB), National Science Foundation. 2021. The STEM Labor Force of Today: Scientists, Engineers and Skilled Technical Workers. *Science and Engineering Indicators 2022*. NSB-2021-2. Alexandria, VA. Available at https://ncses.nsf.gov/pubs/nsb20212. Bureau of Labor Statistics (BLS). n.d. *Definitions*. Available at https://www.bls.gov/cps/definitions.htm#laborforce.

[4] Bureau of Labor Statistics (BLS). n.d. *Employment Projections*. Available at https://www.bls.gov/emp/.

[5] 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.

[6] National Institute of Standards and Technology (NIST). 2023. *Workforce Framework for Cybersecurity (NICE Framework) One Pager*. Gaithersburg, MD. Available at https://www.nist.gov/document/nice-framework-one-pager.

[7] The SOC system is a federal statistical standard, which allows for consistent collection, calculation, and distribution of occupation-related data; see https://www.bls.gov/soc/.

[8] Although the descriptions of these two CIP codes align with cybersecurity, the aligned occupations in the SOC include small numbers of civilian cybersecurity focused workers (i.e., Managers, All other; Special Forces).

[9] Bureau of Labor Statistics (BLS). n.d. *Occupational Employment and Wage Statistics*. Available at https://www.bls.gov/oes/.

[10] Similarly, BLS conducts the Quarterly Census of Employment and Wages to classify employment by industry using NAICS codes. However, cybersecurity jobs cut across industries, and NAICS is an insufficient measure to accurately estimate the size of the workforce.

[11] Eight-digit SOC codes are the most detailed codes available in O*NET, but OEWS currently only produces data for six-digit SOC codes.

[12] Bureau of Labor Statistics (BLS). 2024. *About OEWS Charts and Maps*. Available at https://www.bls.gov/oes/about_charts.htm.

[13] Due to privacy reasons, OPM does not disclose the number of federal employees who fall into the 52 work roles in the NICE Framework.

[14] Doubleday J. 2023. OPM Cyber Hiring Proposal to 'Level Playing Field' Across Agencies. *Federal News Network* November 7. Available at https://federalnewsnetwork.com/hiring-retention/2023/11/opm-cyber-hiring-proposal-to-level-playing-field-across-agencies/.

[15] The General Schedule (GS) Pay Scale ranges from 1 to 15 and is adjusted based on locality pay adjustments. In 2024, GS-12 Step 1 earned $99,200 in the Washington, DC, metro area. Explanation of the GS Scale is available at https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/2024/general-schedule.

[16] General Services Administration. n.d. *Top Secret/Sensitive Compartmented Information (TS/SCI) Clearance*. Available at https://handbook.tts.gsa.gov/general-information-and-resources/business-and-ops-policies/top-secret/.

[17] Bureau of Labor Statistics (BLS). 2023. *Employment Projections: EP Data Tables*. Available at https://www.bls.gov/emp/tables.htm. Data in the current report reference 2022 projections and will be updated when 2023 projections are made available.

[18] Bureau of Labor Statistics (BLS). n.d. *Employment Projections: 2023–33 Employment Projections Release and Skills Data*. Available at https://www.bls.gov/emp/notices/2023/projections-release-2023-33.htm.

[19] Burke A, Finamore J, Foley D, Jankowski J, Moris F; National Center for Science and Engineering Statistics (NCSES). 2021. Measuring R&D Workers Using NCSES Statistics. NSF 21-335. Alexandria, VA: National Science Foundation. Available at https://ncses.nsf.gov/pubs/nsf21335/.

[20] See Burke et al. (2021). Also see NSCG items A24 and A25, which measure multiple job functions; these items could potentially be revised to include cybersecurity (https://ncses.nsf.gov/423/assets/0/files/nscg-2023-new-respondents.pdf).