



Cybersecurity  
Workforce  
Data Initiative

# Cybersecurity Workforce Data Initiative Assessment Summary Report

January 2025

Contractor Awardee: RTI International

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 NCSES or 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. This contract deliverable has been reviewed for unauthorized disclosure of confidential information under NCSES-DRN25-013. Please send questions to [ncsesweb@nsf.gov](mailto:ncsesweb@nsf.gov).

---

# **NCSES Cybersecurity Workforce Data Initiative:**

## Cybersecurity Workforce Data Initiative Assessment Summary Report

### **Abstract**

To launch the Cybersecurity Workforce Data Initiative (CWDI) established by the National Center for Science and Engineering Statistics (NCSES), we conducted a comprehensive analysis on the feasibility of producing nationally representative statistics for the cybersecurity workforce to inform a potential pilot study. This included an analysis of existing definitions, data, sources, and surveys about the cybersecurity workforce in the United States. In this report, we provide an overview of the activities conducted by NCSES, with contractual support from RTI International, for the CWDI between October 2023 and December 2024. This includes the creation of the working group, website and branding and the research and analysis of definitions, knowledge gaps, supply and demand, federal and nonfederal data sources, research questions, and survey items. These activities were informed by expert interviews, workshops, and interested parties, which allowed for broad outreach and engagement with the cybersecurity community. The outputs from these activities provide inputs for an upcoming pilot study of the cybersecurity workforce.

### **Suggested Citation**

---

Hogan M, Dominguez García G, Arbeit CA; National Center for Science and Engineering Statistics. 2025. *NCSES Cybersecurity Workforce Data Initiative: Cybersecurity Workforce Data Initiative Assessment Summary Report*. Alexandria, VA: National Science Foundation. Available at <https://ncses.nsf.gov/about/cybersecurity-workforce-data-initiative>.

### **Contact**

---

National Center for Science and Engineering Statistics  
[ncsesweb@nsf.gov](mailto:ncsesweb@nsf.gov)

## Contents

---

Acknowledgments.....	4
Executive Summary .....	5
Introduction.....	8
NCSSES CWDI Project Team and Working Group.....	8
Collaboration Across Federal Agencies.....	8
NCSSES CWDI Website and Visual Brand .....	9
CWDI Interested Parties .....	9
Conducting Background Research and Gathering Insights from Interested Parties.....	9
Step 1: Developing Definitions on the U.S. Cybersecurity Workforce.....	10
Step 2: Conducting Interviews with Interested Parties to Understand Knowledge Gaps.....	11
Step 3: Conducting Interviews with Interested Parties to Quantify Supply and Demand.....	12
Step 4: Holding Workshops for Interested Parties.....	13
Workshop 1: Definitions.....	14
Workshop 2: Knowledge Gaps .....	14
Workshop 3: Supply and Demand .....	15
Workshop Findings and Takeaways .....	15
Step 5: In-Depth Reviews of Existing Data Sources .....	16
Federal Data Analysis .....	16
Nonfederal Data Analysis.....	17
Step 6: Developing High-Priority CWDI Research Questions and Potential Survey Items.....	18
Research Questions .....	18
Review of Survey Items.....	19
Conclusions, Takeaways, and Next Steps.....	20

## Acknowledgments

---

*Report Authors:*

Michael Hogan

Guillermo Dominguez García

Caren A. Arbeit

RTI International, under contract to the National Center for Science and Engineering Statistics (NCSES)  
[cwdi@rti.org](mailto:cwdi@rti.org)

Thank you to the workshop panelists, participants, and attendees. Thank you to the federal staff and agencies who have participated in the workshops, interviews, and data sharing activities.

Thank you to the NCSES Cybersecurity Workforce Data Initiative working group members; RTI editors August Gering and Cat Olenick; and RTI publications specialist Alex Cone for content and editorial feedback on earlier versions of this report.

## Executive Summary

---

In 2023, the National Center for Science and Engineering Statistics (NCSES), part of the U.S. National Science Foundation (NSF), established the Cybersecurity Workforce Data Initiative (CWDI) as directed by the CHIPS and Science Act of 2022. The goal of the CWDI is to assess the feasibility of generating national estimates and statistics about the U.S. cybersecurity workforce using federal and administrative data sources to inform a potential pilot study. The CWDI project team, including NCSES and RTI International, led the research activities with the support of the CWDI working group consisting of NCSES staff and experts. Activities included background research and data gathering between October 2023 and December 2024. This part of the initiative established the baseline, including defining the workforce, assessing existing data, gathering input from interested parties and experts, and developing research questions. Given the national urgency of cybersecurity in light of rapidly evolving technology, it is important to have reliable data to be able to accurately understand and address the workforce needs. The background information gathered and analyzed will inform the survey development, testing, pilot, analysis, and auxiliary data work stages which started in October 2024.

The research included in this report kicked off in October 2023 with a background report, establishment of the NCSES working group to support the CWDI project team, and the development of the website, visual brand, interested parties list, and review process. Throughout the research conducted in this report, the CWDI project team worked closely with federal agencies and nonfederal organizations, gathered data, conducted interviews, and addressed feedback. This helped the project team understand the cybersecurity workforce community and engage with key experts in the field through interviews and workshops. To prepare for the workshops, the project team conducted interviews and reviewed data on the definitions of the cybersecurity workforce, knowledge gaps, and supply and demand for cybersecurity workers. As a result of this work, the project team developed a proposed definition of the workforce that included both cybersecurity occupations and cybersecurity activities and work roles. The [NICE Workforce Framework for Cybersecurity \(NICE Framework\)](#), the most commonly cited taxonomy of cybersecurity work in the United States, relies on activities and work roles, whereas many other measures of labor market data rely on occupation titles. The CWDI project team then estimated the supply and demand for workers in cybersecurity based on a set of publicly available data sources published between 2021 and 2024, which led to a wide range of estimates from fewer than 200,000 to as many as 3.5 million workers in the core workforce. This reflected the challenge of the creating the definition and working with existing federal data that relied on delineations from federal taxonomies (e.g., Standard Occupational Classification, or SOC, and Classification of Instructional Programs, also referred to as CIP codes), which only partially capture the supply of the cybersecurity workforce.

In the summer of 2024, the CWDI project team hosted a series of three workshops with 321 unique attendees. The workshops convened interested parties; shared findings; and solicited additional inputs through expert panels, polls, question and answer sessions, and small group breakout discussions. From the three workshops, key findings included the need to further refine the definition, capture data on both job titles and work activities, and gather better data on credentials and pathways, as well as a need for reliable federal data to capture the workforce. Experts and participants from different industries provided a breadth of insights into the additional data needs for decision-making and planning. They agreed that a publicly available data source on the cybersecurity workforce was needed and would provide valuable data to inform better decision-making in workforce development.

Following the workshops, the CWDI project team reviewed federal and nonfederal data sources that could potentially address these gaps. Although many of the federal data sources mapped to traditional workforce coding schemas like SOC, CIP, and the North American Industry Classification System (NAICS), these do not capture the types of work roles and work activities in cybersecurity identified by

resources like the NICE Framework. Future revisions to existing codes could help address this, however it is currently difficult to obtain publicly available data on the percentage of workers engaged in cybersecurity activities across job titles. Nonfederal data sources, such as job boards and surveys, offer complementary data on things like work activities and certifications, but the CWDI working group is unsure if they meet the standards of data quality per the guidelines recommended by Federal Committee on Statistical Methodology due to the confidentiality of their data and methods.

Based on the findings from the definitions, data analysis, knowledge gaps, workshops, and review of data sources, the CWDI project team developed a priority set of research questions for a pilot survey focused on demographics of the workforce, educational credentials, and employment trajectories and outcomes. These questions would help inform a broader question of the role of the cybersecurity workforce in the national workforce. Using this framework, the team specified priority detailed questions. Finally, the team reviewed survey items from seven federal surveys and one private survey creating an inventory of potential survey items. Of the inventoried survey items, 62 potential survey items were identified for a future pilot survey based on their ability to answer the CWDI project team's research questions.

The primary goal of these activities was to understand the landscape of definitions, knowledge gaps, data, relevant interested parties, and surveys relevant to quantifying the cybersecurity workforce in the United States. Cybersecurity is a rapidly evolving field with unique demands for a skilled workforce, including those who are in core cybersecurity occupations and those with relevant work activities as digital technology and information security touch nearly every facet of work, education, government, and everyday life. Through these activities, the project team has identified the following key findings:

- The cybersecurity workforce is defined by a mix of job roles and work activities. Cybersecurity work spans both core cybersecurity occupations and other adjacent occupations with relevant knowledge, skills, and work activities. The line between these two groups of occupations is blurred.
- Entry points into the cybersecurity workforce are not well understood or captured by data, and a critical knowledge gap is in the types of career pathways and credentials that can help meet the evolving workforce needs for cybersecurity.
- Depending on the definition, occupation codes, and data sources used, the size of the cybersecurity workforce ranges from fewer than 200,000 to nearly 3.5 million workers using federal data sources released between 2021 and 2024. Although many independent estimates fall within this range, we offer a wide range of estimates because we do not yet know to what degree primary or secondary cybersecurity work activities overlap with existing occupation codes.
- Cybersecurity work is partially captured by federal data sources from the Bureau of Labor Statistics, Census Bureau, NSF/NCSES, and Department of Education. However, due to the limitation of classifications, such as SOC codes, Census occupation codes, and CIP codes that capture cybersecurity, it is difficult to identify the cybersecurity workforce using existing surveys.
- Nonfederal administrative sources could provide some data in the absence of a comprehensive, single federal data source on the cybersecurity workforce. Data products from independent organizations offer some good insights, but limitations on public access and granularity make them challenging for capturing the entirety of the workforce.
- Several existing surveys have questions that could be relevant to a future pilot data collection on the cybersecurity workforce.

This background research shows the need for federal data on the cybersecurity workforce that should include a survey, or surveys, collecting individual-level data on cybersecurity workers with a sampling frame that allows for data collection on the general population specific to the cybersecurity workforce. The CWDI project team is in the process of developing the survey questions to be piloted in 2025, which requires a sample design, Office of Management and Budget clearance, and survey item testing research. The CWDI project team will work on these critical activities for the potential administration of a pilot study for NCSES to collect data on this workforce.

## **Introduction**

---

In 2023, the National Center for Science and Engineering Statistics (NCSES), part of the U.S. National Science Foundation (NSF), established the Cybersecurity Workforce Data Initiative (CWDI) as directed by the CHIPS and Science Act of 2022. The goal of the CWDI is to assess the feasibility of generating national estimates and statistics about the U.S. cybersecurity workforce and inform a potential pilot study. In an environment of increasingly complex cybersecurity risks and technology, leaders in government, defense, business, healthcare, education, and technology emphasize a lack of understanding about the workforce and a need to address a growing skills gap in cybersecurity, with large numbers of unfilled positions and an unclear career pathway for workers.

The first phase of the CWDI, between October 2023 and December 2024, consisted of the CWDI project team conducting background research to understand the state of the workforce and the feasibility of assessing the workforce using existing federal and administrative data. This part of the initiative included a series of activities to define the workforce, assess existing data, gather input from interested parties and experts, and develop research questions. The background information gathered, analyzed, and summarized in this report will inform the upcoming survey development, testing, pilot, analysis, and auxiliary data work. As a component of the research activities and workshops presented in this report, the project team created a website for the CWDI and engaged with a large community of national experts and interested parties.

### **NCSES CWDI Project Team and Working Group**

The CWDI project team included staff from contractor RTI International and staff from NSF NCSES. The project team included the support of the CWDI working group: NCSES and NSF staff and experts who provided guidance and resources. The team created connections with other federal and nonfederal interested parties and experts, and reviewed data and deliverables. The members of the working group contributed methodological and substantive expertise in several areas, including statistical and survey methodology, workforce data and surveys, study development, and communication and outreach. The working group provided critical input on all reports, deliverables, and presentations.

As part of its mandate, NCSES serves as a federal clearinghouse for the collection, interpretation, analysis, and dissemination of objective data on the U.S. science and engineering enterprise. As one of the 13 principal federal statistical agencies, NCSES collects data and coordinates with other federal agencies to provide data on the state of science and engineering in the United States, including critical data about the workforce.

### **Collaboration Across Federal Agencies**

The CWDI project team engaged several federal agencies and experts beyond NSF to better understand the cybersecurity workforce, the state of initiatives, and the knowledge gaps in existing data and programs. This included interviews with representatives from the Census Bureau, Bureau of Labor Statistics (BLS), Department of Defense (DoD), Department of Homeland Security's Cyber & Infrastructure Security Agency (CISA), White House Office of the National Cyber Director, White House Office of Science & Technology Policy, Argonne National Lab, Office of Personnel Management (OPM), and National Institute for Standards and Technology (NIST). Additionally, the team worked closely with the NICE Framework team at NIST, the leading federal organization tracking and organizing cybersecurity skills and work activities. Representatives of CISA, NICE, and Argonne National Lab participated in workshop panels. Additionally, the CWDI project team attended the 2024 NICE Conference and NCSES presented at the 2024 Federal Committee on Statistical Methodology (FCSM) Conference.

## NCSES CWDI Website and Visual Brand

The CWDI project team created the content and branding for a dedicated Web page on the [NCSES CWDI website](#) to share all materials and relevant project reports and updates. This included creating a visual brand to accompany all materials, presentations, outreach, and work products. The page hosted the registration forms for and information about the [CWDI workshops](#) and is the central location for all public-facing CWDI reports and updates. The CWDI working group maintains and updates the website, which will continue to serve as a repository for project resources moving forward.

## CWDI Interested Parties

Through the interviews, workshops, and other CWDI activities, the CWDI project team has been compiling and regularly updating its interested parties list. The list includes individuals from federal, state, and local governments; private sector researchers, employers, and cybersecurity experts; and cybersecurity and workforce experts from primary, secondary, and higher education. The list is updated on an ongoing basis with those who have interacted with the CWDI, asked for information, or have been identified by the CWDI project team. The interested parties list also serves as a mailing list to keep all relevant parties informed of any upcoming activities.

## Conducting Background Research and Gathering Insights from Interested Parties

---

To support the initiative, the CWDI project team gathered, summarized, and analyzed data related to the goals of summarizing the existing landscape of knowledge about the cybersecurity workforce. This included examining the following areas: definitions, knowledge gaps, supply and demand, federal and nonfederal data, existing research questions, and survey items. These activities occurred between October 2023 and December 2024 (Table 1).

Table 1  
**Report activities with start and end dates**  
(Activity and dates)

Activity	Start and end dates
Kick off project and do background research	October–December 2023
Conduct knowledge gap interviews and summarize	January–March 2024
Evaluate definitions and conduct definitions interviews	January–April 2024
Assess existing data on supply and demand	February–June 2024
Evaluate federal data sources	April–August 2024
Host CWDI Workshops and create summary report	May–September 2024
Evaluate nonfederal and administrative data sources	May–September 2024
Develop research questions	June–July 2024
Identify potential survey items	July–October 2024
Summarize work and key findings from background research	October–December 2024

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

In this report, we review the processes and outcomes of these activities in chronological order, including the activities that led up to and informed the workshops, as well as the activities delivered and completed since the workshops. Across these stages, the CWDI project team identified key themes and takeaways and share findings across activities to best inform the research.

## Step 1: Developing Definitions on the U.S. Cybersecurity Workforce

The CWDI project team started background research in October 2023 with a scan of federal and nonfederal cybersecurity workforce initiatives, frameworks, and taxonomies. The scan included documents from the NIST NICE Framework, CISA, National Security Agency (NSA), NSF CyberCorps Scholarships for Service (CyberCorps), OPM, DoD, and BLS, among others. Nonfederal and international programs and taxonomies included CyberSeek, United Kingdom Cybersecurity Careers framework and European Union Framework. The review showed that some frameworks (e.g., NICE Framework) relied on knowledge and skills, whereas others (e.g., the European framework) relied on job titles.

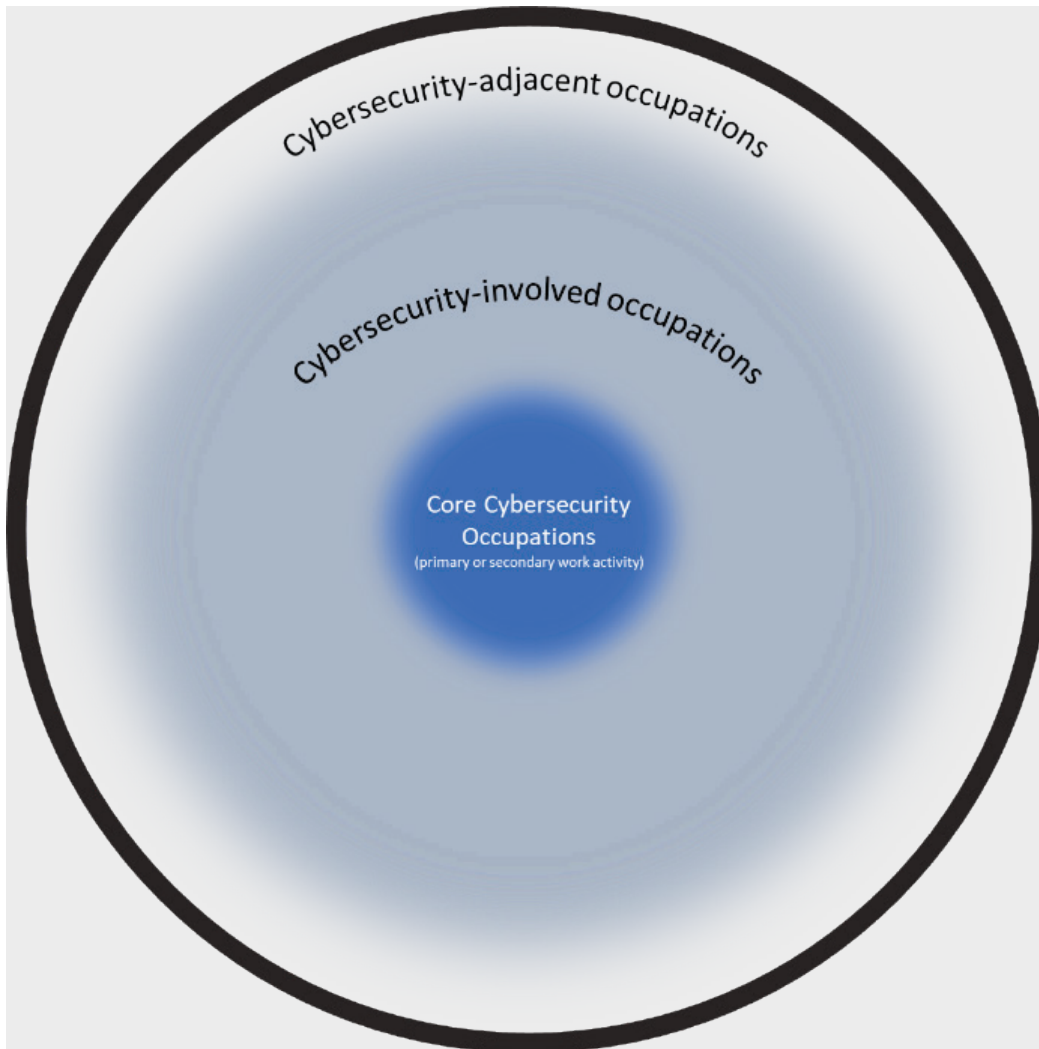
The scan of recent initiatives kicked off the research for defining the workforce. Along with reviewing existing frameworks and definitions of the cybersecurity workforce, we interviewed cybersecurity practitioners and workforce experts.<sup>1</sup> Interviewees generally agreed that the cybersecurity workforce is defined not solely by job titles or occupation codes but by work roles in developing, implementing, and using cybersecurity tools. However, there was not a consensus on who should be included as a cybersecurity worker and who should not. Interviewees emphasized a need for a better definition of the workforce—one that could be translated into reliable data.

Using this input, the CWDI project team proposed a working definition for the initiative in the [Cybersecurity Workforce Data Initiative: Cybersecurity Workforce Definitions Report](#) based on the scan of existing frameworks. We then revised the working definition following analysis of the interviews with experts and practitioners. As a result, the CWDI project team created a multilayered definition that includes both a broad set of cybersecurity work roles and skills with components of narrower definitions often endorsed by non-U.S. governments and cybersecurity professional organizations:

*The cybersecurity workforce includes a core set of cybersecurity occupations focused on cybersecurity. Workers in other occupations where their primary or secondary work activities include cybersecurity are also part of the core cybersecurity workforce. Cybersecurity-involved workers engage in cybersecurity work as a work activity that is not their primary or secondary work activity. Finally, workers not already identified as core or cybersecurity-involved workers whose tasks, skills, knowledge, and/or jobs functions are related to cybersecurity are part of the cybersecurity-adjacent workforce.<sup>2</sup>*

This definition allowed the CWDI project team to collect and analyze data on a narrow set of core occupations and opened up the definition to a more flexible set of work roles aligning with the NICE Framework. With the information available, the line between core, adjacent, and involved workers in cybersecurity is blurry. Our definitions allow for a range of workers in the cybersecurity-involved and adjacent workforce, recognizing that many workers have a range of work activities that relate to cybersecurity (Figure 1). As many experts pointed out, nearly every job in the United States has work roles that touch digital technology, and there are cybersecurity implications that may come along with them.

Figure 1  
Proposed framework for cybersecurity occupations



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

Additionally, as part of the background review, we began to identify knowledge gaps, which informed the concurrent task.

## Step 2: Conducting Interviews with Interested Parties to Understand Knowledge Gaps

In parallel with defining the workforce, the CWDI project team interviewed experts on knowledge gaps in the cybersecurity workforce.<sup>3</sup> Participants described the data missing from what we currently know about the U.S. cybersecurity workforce, with many identifying gaps that support the need for a CWDI pilot study.

A common theme from the interviews is that there are limited publicly available data on the basic characteristics of the cybersecurity workforce, including demographics and educational pathways, as well as limited data on the employers of cybersecurity workers. More specifically, the needed and desired information about the cybersecurity workforce centers around the end goal of improving U.S. cybersecurity resilience by ensuring that cybersecurity roles are filled with workers who have the needed skills and competencies. To achieve that goal, it is necessary to understand the cybersecurity workforce, including those who may be trained but not yet working in the field. This needs to be reconciled with

employer-level information about their cybersecurity workforce needs in terms of skills and experience. Interview participants were hopeful that a new federal data source could benefit jobseekers trying to begin or advance a cybersecurity career, educators and trainers trying to improve their curricula or credentials, and employers trying to attract workers.

### **Step 3: Conducting Interviews with Interested Parties to Quantify Supply and Demand**

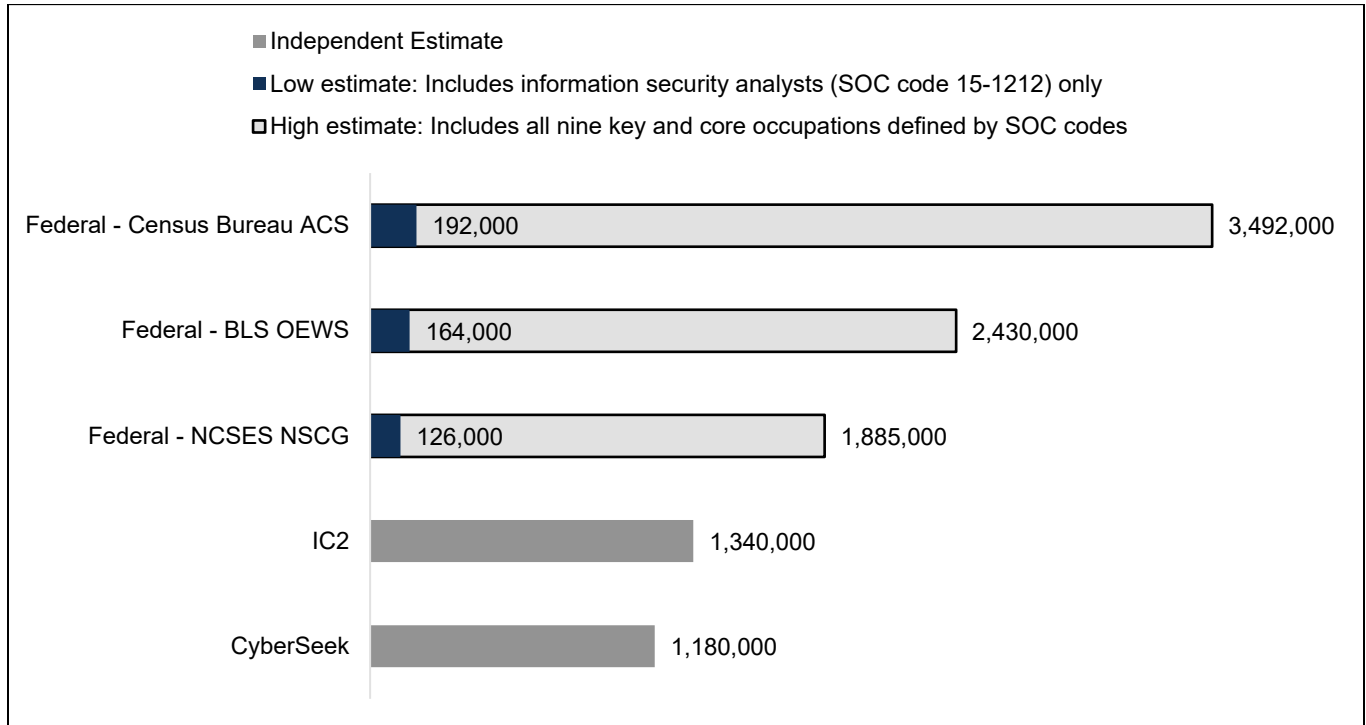
Having defined the workforce and identified knowledge gaps, the CWDI project team then worked to quantify the supply of cybersecurity workers, as well as the demand for workers, using existing data sources. We investigated data sources with the potential to estimate the size of the current workforce and labor force, the pipeline of new workers, and the short- and long-term demand for workers. To delineate the core workforce, we identified nine Standard Occupational Classification (SOC) codes that indicate cybersecurity work and—by examining data from the BLS Occupational Employment and Wage Statistics program, the Census Bureau’s American Community Survey (ACS), and the NCSES National Survey of College Graduates (NSCG)—we found that the size of the core workforce in 2023 ranged from around 164,000 workers to 3,492,000 workers (Figure 2). The data from these sources were published between 2021 and 2024. We also found that the number of current job openings ranges from 14,000 to 55,000 active postings for the same range of years, and BLS projections indicate that the number of jobs in cybersecurity occupation codes could increase by 10%–31%, depending on the SOC code, from 2022 to 2032.

The wide ranges in our findings exist because the data reported by existing federal surveys are delineated by occupation codes through SOC or the Census Bureau and are rolled up to a higher level of aggregation. Cybersecurity occupations have evolved since the last SOC revision published in 2018, and many new work roles fall under “computer occupations, all other,” making it difficult to quantify with existing federal data and definitions. Because there are many occupations, such as software engineering, that could have cybersecurity as a primary or secondary work activity, we do not yet know what percentage of workers in those fields identify as cybersecurity workers, making it difficult to get a precise estimate.

As the [\*Cybersecurity Workforce Data Initiative: Cybersecurity Workforce Supply and Demand Report\*](#) describes, current data provides wide-ranging estimates, with some key findings on educational attainment and demographics. However, further research and better data on both occupations and work activities in cybersecurity are needed to obtain a more precise estimate of supply and demand and to understand the number of workers in the cybersecurity-involved and -adjacent workforce.<sup>4</sup> Although there were several nonfederal data sources that used different methods to estimate the workforce (Figure 2), interviewees from the private sector expressed a desire for more precise federal data on the workforce.

Figure 2

Estimates of the size of the workforce based on various definitions



ACS = American Community Survey; BLS = Bureau of Labor Statistics; ISC2 = International Information System Security Certification Consortium; NCSSES = National Center for Science and Engineering Statistics; NSCG = National Survey of College Graduates; OEWS = Occupational Employment and Wage Statistics; SOC = Standard Occupational Classification.

Source(s):

Census Bureau, American Community Survey; Bureau of Labor Statistics, Occupational Employment and Wage Statistics; National Center for Science and Engineering Statistics, National Survey of College Graduates; International Information System Security Certification Consortium; CyberSeek; and National Center for Science and Engineering Statistics, Cybersecurity Workforce Data Initiative (CWDI).

#### Step 4: Holding Workshops for Interested Parties

Following the activities focused on gathering information about knowledge gaps and definitions, developing a definition, and exploring the supply and demand of the cybersecurity workforce, the CWDI project team conducted a series of three virtual 2-hour workshops on each topic in May and June 2024. The intent of the workshops was to share our progress to date with interested parties and to solicit input to help refine the definition of the cybersecurity workforce, better understand knowledge gaps, and gather data sources that could help us better capture the supply and demand of the cybersecurity workforce. The workshops were free and open to the public with preregistration. Information on the workshops was shared on the CWDI [workshops Web page](#), via an NCSSES-led outreach campaign, and through emails to everyone on the interested parties list. Panelists were identified from the definitions and knowledge gap interviews and the interested parties' lists.

The first workshop focused on the working definition of the cybersecurity workforce, the second one was about the knowledge gaps regarding the cybersecurity workforce, and the third one addressed existing data sources that can provide estimates on the supply and demand of the workforce. The workshops served to disseminate the CWDI interim findings and elicit discussion on each of the topics to gather information. The workshops provided productive discussions that helped amend our working definition of the workforce and reinforced the need to produce estimates of the U.S. cybersecurity workforce. Information gathered at the workshops also helped tailor priority research questions for the next phase of work.

In total, more than 321 people attended at least one workshop, where they heard about and provided feedback on our findings (through breakout groups and polls), listened to panels of experts, and engaged in question-and-answer sessions with them. Each workshop included 140–165 participants. Across all three workshops, the most frequent occupational sector of the attendees was higher education, with more than 60% of attendees representing higher education. Federal government and private sector followed, with 10%–13% of attendance at each workshop (Table 2).

Table 2  
**Registration and attendance at CWDI workshops**  
 (Number and percent)

Characteristics	Total		Workshop 1		Workshop 2		Workshop 3	
	Number	Percent	Number	Percent	Number	Percent	Number	Percent
Attendance	321	100	142	100	158	100	165	100
Federal government	33	10.3	18	12.7	20	12.7	18	10.9
Higher education	205	63.9	90	63.4	100	63.3	102	61.8
Private sector	35	10.9	11	7.7	16	10.1	22	13.3
State or local government	11	3.4	7	4.9	4	2.5	6	3.6
All other	37	11.5	16	11.3	18	11.4	17	10.4

Note(s):  
 The counts in this table show the number of unique individuals per category. Counts per workshop do not sum to the total because individuals could register and attend multiple workshops. "Other or unknown" includes participants in elementary education, consulting, media, nonprofit, think tanks, and other settings, as well as people who joined workshops from their phones or who did not provide any employment information. Fourteen participants joined at least one workshop but did not register with that e-mail address or phone number. Data exclude National Center for Science and Engineering Statistics and RTI International staff who attended as part of the project or working group team. Due to rounding, percentages may not sum to total.

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

**Workshop 1: Definitions**

In the first workshop, held on May 7, 2024, we presented our [definition of the cybersecurity workforce](#), which balanced both occupation titles and knowledge, skills, and work activities. Panelists discussed the tension between a narrow and broad definition. There were concerns that a narrow definition would lead to the exclusion of certain work roles and ignore a part of the population, whereas an excessively broad one would be unhelpful in policymaking discussions. Additionally, participants pointed out that focusing on job titles would be challenging due to the variability in titles and work activities for a title across organizations. Participants largely agreed that a definition that balances skills, knowledge, and work activities with occupations would capture the cybersecurity workforce accurately.

The definitions workshop highlighted that participants were most familiar with the NICE Framework. Additionally, it exposed some challenges with operationalizing the definition, including the rapidly changing nature of cybersecurity practice and work, the broad set of jobs that encompass cybersecurity skills, and the lack of a common language around cybersecurity, such as the interchangeable use of “cyber jobs” and “cybersecurity jobs.” This workshop helped us revise and strengthen our definition.

**Workshop 2: Knowledge Gaps**

In the second workshop, held on May 23, 2024, we discussed the [critical knowledge gaps](#) that need to be filled to better understand the cybersecurity workforce. Participants discussed the importance of understanding the educational and career pathways of cybersecurity practitioners, as well as their demographic information, to understand and develop the workforce. Participants also emphasized the need to better understand hiring practices, as well as the skills gaps that exist between jobseekers and the skills employers seek. Finally, given our definition of the cybersecurity workforce, participants also encouraged us to make a clearer distinction between the core, adjacent, and involved groups of cybersecurity workers and to report if any overlaps exist.

### **[Workshop 3: Supply and Demand](#)**

The third workshop, held on June 11, 2024, presented data on the [supply and demand of the cybersecurity workforce](#) using existing data sources. Due to the ample ways in which the workforce is measured depending on data source, the numbers presented included large ranges, causing challenges in pinpointing supply and demand gaps or in recommending effective policies to build the country's cybersecurity workforce. The data presentation described the challenges around identifying the cybersecurity workforce in current data and was limited to core cybersecurity occupations captured in federal data, with some nonfederal sources as a comparison. Participants also discussed the limitations of known data sources, as well as the importance of recruiting, retaining, and promoting a broad pool of talent to upskill the workforce and build pathways into cybersecurity.

Participants helpfully identified additional sources of workforce data. Based on the input, the CWDI project team analyzed additional nonfederal data for the [Cybersecurity Workforce Data Initiative: Administrative Data Evaluation Report](#).

### ***Workshop Findings and Takeaways***

After completing the three workshops, the CWDI project team summarized each workshop and compiled key themes and takeaways across the workshops. These were compiled into a set of recommendations. Overall, the workshops provided additional information and motivation for an individual-level pilot data collection of cybersecurity workers.

Key takeaways emerged from cross-cutting themes of these workshops, as well as points that were salient in specific workshops.

We identified adjustments to our definition of the cybersecurity workforce and the examples used to describe our definitions. This came from feedback that our definition should more clearly delineate the distinct categories (core, adjacent, involved) within the cybersecurity workforce. We adjusted the definition needed to account for the variety of audiences (and their needs) that will use this definition, as well as the fast-evolving nature of the field.

We identified an overarching theme related to the challenge of having various cybersecurity job titles and activities within titles across organizations. Practitioners emphasized that the language of cybersecurity jobs and work roles was not uniform, highlighting the need to collect both job titles and work activities for potential cybersecurity workers when surveying individuals and organizations.

Across the workshops, participants discussed the limitations of knowledge about pathways into and through the cybersecurity workforce. This led to a recommendation that an individual-level survey should include items on educational and credential pathways into cybersecurity positions.

The workshops included conversations related to perceived underrepresented populations in the cybersecurity workforce and concerns that these are preventing recruitment into the workforce. Thus, any data collection should seek to understand intersectional differences in pathways and work experiences.

Overall, the workshops reinforced the need for more detailed and reliable estimates of the U.S. cybersecurity workforce from a trusted government statistical agency. Such a data source would help decision-making for researchers, practitioners, employers, educators, and policymakers who are working to develop this rapidly evolving and growing field.

## Step 5: In-Depth Reviews of Existing Data Sources

Based on the feedback from workshops, interviews with experts, and the sources used to provide ranges of estimates of the cybersecurity workforce supply and demand, the CWDI project team reviewed 13 federal survey data sources and 12 data sources from nonfederal and administrative data providers. To structure this review, the project team employed the three domains of the FCSM data quality framework: utility, objectivity, and integrity.<sup>5</sup> This approach allowed us to evaluate data sources based on their relevance; ability to map to existing frameworks and taxonomies; granularity; and availability of information on credentials, pathways, employment outcomes, and demographics. The review also determined the timeliness of the data, the sample size and coverage, and accessibility. Although no single data source met all the criteria required to address the data needs for the CWDI, the review did provide valuable insights into federal and auxiliary data sources and highlighted open questions that will inform future data collection efforts.

### Federal Data Analysis

For the *Cybersecurity Workforce Data Initiative: Federal Data Evaluation Report*, we reviewed 13 federal data sources, including household-level data, individual-level data, data on educational institutions and employers, and aggregate data. All reviewed federal data sources were determined to meet FCSM standards of objectivity and integrity because they are required to follow federal guidelines for survey development, data collection, data distribution, data security, and confidentiality. All data sets analyzed have reference periods between 2020 and 2024, and public-use files were available for each source, ensuring accessibility and transparency. We reviewed the sources outlined in Table 4.

Table 4

#### Federal surveys and use of key coding schemas: 2022-2023

(Survey name, acronym, and agency)

Survey name	Survey acronym	Occupation codes (SOC/Census)	Maps to		
			CIP codes	NICE Framework	NAICS
American Community Survey	ACS	Yes	No	No	No
Annual Business Survey	ABS	No	No	No	Yes
Current Population Survey	CPS	Yes	No	No	No
Integrated Postsecondary Education Data System	IPEDS	No	Yes	No	No
Longitudinal Employer-Household Dynamics	LEHD	No	No	No	No
National Postsecondary Student Aid Study	NPSAS	No	Yes	No	No
National Survey of College Graduates	NSCG	Yes	Yes	No	No
Occupational Employment and Wage Statistics	OEWS	Yes	No	No	Yes
Occupational Information Network	O*NET	Yes	No	No	No
Occupational Requirements Survey	ORS	Yes	No	No	No
Quarterly Census of Employment and Wages	QCEW	No	No	No	Yes
Survey of Doctorate Recipients	SDR	No	Yes	No	No
Survey of Graduate Students and Postdoctorates in Science and Engineering	GSS	No	Yes	No	No
Survey of Income and Program Participation	SIPP	Yes	No	No	No

CIP = Classification of Instructional Programs, 2020; NAICS = North American Industry Classification System; SOC = Standard Occupation Classification, 2018.

Source(s):

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

Each data source provided some strengths in capturing the cybersecurity workforce and offered insights into items that a new questionnaire could utilize or modify specifically for the cybersecurity workforce. Yet, based on our analysis, we determined that the existing datasets do not currently provide sufficient utility to fully capture the scope of the cybersecurity workforce. Although all 13 data sources met the FCSM standards of objectivity and integrity, several gaps in coverage and limitations in granularity were identified. None of the existing data sources contained all the relevant variables of interest, nor could they be disaggregated at a level of detailed occupation, work activity, or demographic characteristics. In addition, existing sources did not align with the NICE Framework, and other existing taxonomies, such as Classification of Instructional Programs [CIP], SOC, and North American Industry Classification System [NAICS], were not sufficient to identify the cybersecurity workforce. Therefore, the need for a new, targeted federal effort to better analyze and measure the cybersecurity workforce is supported. Specifically, we identified the need for a bridge between the NICE Framework with nationally representative federal data taxonomies (such as CIP, the Occupational Information Network, and SOC) and the surveys that use these taxonomies.<sup>6</sup>

### ***Nonfederal Data Analysis***

To complement the review of the federal data, we analyzed 12 nonfederal data sources, using the same evaluation criteria as for federal sources in the [Cybersecurity Workforce Data Initiative: Administrative Data Evaluation Report](#). Specifically, we included job posting sites, industry surveys from business associations, proprietary data sources, and payroll data sources. The compilation of these data sources was based on a combination of literature review, interviews, and workshop polls. Although nonfederal data sources can be valuable in filling gaps left by federal data sources, we were unable to verify if they met the standards set by the FCSM for utility, objectivity, and integrity due to the confidentiality of their methods and data. A major challenge was the proprietary nature of many of the data sources, which meant that we were limited in accessing raw data or detailed sampling methodology. As a result, we were unable to assess the reliability or representativeness of the data (Table 5).

Table 5

**Nonfederal and administrative data source type, by subcategory: 2024**

(Data source and data type)

<b>Subcategory</b>	<b>Data source</b>	<b>Data type</b>
Job posting site	ClearanceJobs	Job postings and surveys
Job posting site	Indeed	Job postings
Job posting site	LinkedIn	Job postings
Job posting site	National Labor Exchange	Job postings, state job banks
Job posting site	ZipRecruiter	Job postings
Payroll data	ADP	Payroll data
Proprietary data model	CyberSeek	Proprietary data, Lightcast model
Survey	CompTIA	Member survey
Survey	CRA Taulbee Survey	Survey of PhD-granting institutions
Survey	ISC2	Member survey
Survey	SANS Institute/GIAC	Member survey and interviews
Survey	WiCyS/N2K	Member survey

CompTIA = Computing Technology Industry Association; CRA = Computing Research Association; ISC2 = International Information System Security Certification Consortium; WiCyS = Women in Cybersecurity.

Source(s):

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

Although we could not fully determine the objectivity and integrity of the 12 selected data sources due to lack of access, we examined them based on several criteria, including relevance, granularity, accessibility, coverage and sample size, and timeliness. Our analysis found that job posting sites like LinkedIn or Indeed can provide a high-level view of job supply; however, a more detailed analysis

specific to the cybersecurity workforce or cybersecurity-related job postings would require access to individual-level data, which is often difficult to obtain. Moreover, even if we were able to access these data, questions would remain regarding the quality and coverage of the data. High-level summaries are available through keyword searches on the public sites.

We found that nonfederal data sources complemented federal data to a certain extent but were not a suitable replacement for direct data collection through surveys, interviews, and workshops. Sources like CyberSeek that relied on a combination of federal and nonfederal data to build complex models were particularly valued by interviewees and workshop participants.<sup>7</sup> This review highlighted the need for further efforts to secure these types of data and underscores the necessity of conducting an individual-level pilot study to better understand and measure the cybersecurity workforce.

## **Step 6: Developing High-Priority CWDI Research Questions and Potential Survey Items**

Following the definitions, knowledge gaps, supply and demand, workshops, and review of existing federal and nonfederal data sources, the CWDI project team developed priority research questions to inform the ongoing research efforts of the initiative. The development of research questions highlighted the need for a pilot survey on the cybersecurity workforce to support answering basic questions about the composition, educational pathways, and work experiences of the cybersecurity workforce. After developing research questions, planning for a pilot survey began. This planning included compiling an inventory of existing survey items to systematically identify the alignment of items with the research questions.

### ***Research Questions***

The CWDI project team formalized research questions to inform the research efforts of the CWDI during the pilot survey. Taking the previous data gathered to date, the project team developed and recommended to NCSES 15 research questions covering demographics, educational credentials and certifications, and employment experiences and outcomes (Table 6) for the pilot survey. These research questions are the focus for the rest of the work under the CWDI.

Table 6

**Research questions by question type**

Research question	Question type
<b>Demographics</b>	
1. Who comprises the cybersecurity workforce?	Broad
1a. What are the demographic characteristics of the cybersecurity workforce?	Specific
1b. How do the demographic characteristics of the cybersecurity workforce vary by cybersecurity worker type?	Specific
<b>Education levels and credentials</b>	
2. What credentials (i.e., certifications, licenses, and work-related experiences) are most common among cybersecurity workers?	Broad
2a. What are the education and credential pathways (i.e., their educational backgrounds and jobs held) that are most common among cybersecurity workers?	Specific
2b. Given how fast cybersecurity is changing, what are cybersecurity workers doing to stay knowledgeable in their field?	Specific
<b>Employment requirements and outcomes</b>	
3. How much do cybersecurity workers earn, by years in the field, occupation, and type of organization?	Broad
4. What are the occupations and job titles of cybersecurity workers?	Broad
5. What are the work activities of cybersecurity workers?	Broad
5a. What is the relationship between work activities, occupations, and job titles?	Specific
6. How long have cybersecurity workers been working in cybersecurity?	Specific
<b>Population level</b>	
7. How many people in the United States are working in cybersecurity jobs?	Broad
8. How many people in the United States are getting degrees or certificates or other credentials in cybersecurity?	Broad
9. How many cybersecurity job openings are there?	Broad
10. What is the ratio between supply and demand of cybersecurity workers in the current period, and what is it projected to be in the future?	Broad

Source(s):

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

***Review of Survey Items***

The research questions were the basis for a review of survey items, as a pilot survey should be designed to address the research goals of the CWDI. For the review of survey items, the project team developed a broad inventory of survey items for consideration to draft a questionnaire for the pilot survey, providing flexibility to address research questions and avoid restricting the set of potential survey items too early in the process. The surveys were reviewed in detail to identify potential survey items with perceived relevance to answering our research questions. Items that could address one or more research questions were added to an item inventory.

After mapping survey items in the inventory to research questions, we identified remaining gaps in research question coverage. In total, our inventory contained 395 survey items across four main areas of focus. Namely, we identified 134 potentially relevant items from several modules of the Current Population Survey and 197 items from NCSES surveys, such as the NSCG; National Training, Education, and Workforce Surveys; and Survey of Earned Doctorates. We also reviewed and identified additional items from the Survey of Income and Program Participation, ACS, Census Household Pulse Survey, and the National Survey of Family Growth. We will follow the Office of Management and Budget (OMB) Statistical Policy Directive 15 when asking about a participant's race and ethnicity.<sup>8</sup> We recommended 62 items across six domains related to the research questions. We recommend the 62 items for possible use in the survey based on an assessment of the degree to which they related to the high-priority research questions. Items that were necessary to answer one or more of the high-priority research questions or support the key constructs were rated as being of high priority. When multiple items covered the same topic, NCSES survey items were prioritized so results may be compared to other NCSES surveys.

Table 7

**Recommended Survey Items**

Research Question/Inventory Item	Number recommended
All Inventory Items	62
Demographics	15
Educational credentials and background	19
Earnings	5
Occupation and job titles	10
Work activities	9
Time working in the field	4

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

The 62 recommended survey items are the basis for drafting a questionnaire for a pilot study. This next step will include building the logic of the survey, ordering the questions, and preparing for a cognitive testing plan to be submitted for OMB clearance.

## Conclusions, Takeaways, and Next Steps

---

Over the past year, the CWDI has successfully examined the landscape of definitions, knowledge gaps, data sources, interested parties, and surveys relevant to quantifying the cybersecurity workforce in the United States. Cybersecurity is a rapidly evolving field with unique demands for a skilled workforce, including among them those who are in core cybersecurity occupations and those with relevant work activities, as digital technology and information security touch nearly every facet of work, education, government, and everyday life. Through this task, we have identified the following key findings:

- The cybersecurity workforce is defined by a mix of occupations, job roles, and work activities. Cybersecurity work spans both core cybersecurity occupations and other adjacent occupations with relevant knowledge, skills, and work activities. The line between these two groups of workers is blurred, making it difficult to quantify using existing data and definitions. The NICE Framework, the most comprehensive tool to understand the cybersecurity workforce, defines the workforce through knowledge, skills, and work activities but does not yet map to existing federal data definitions for occupations.
- A critical knowledge gap is in the types of career pathways and credentials that can help to meet the evolving workforce needs for cybersecurity. Entry points into the cybersecurity workforce are not well understood or captured by data. Many experts pointed out a gap in the workforce with a large unmet demand for experienced professionals but a growing supply of early career workers who could not find employment with their skill sets.
- Depending on the definition, occupation codes, and data sources used, the size of the cybersecurity workforce may range from less than 200,000 to nearly 3.5 million based on data released between 2021 and 2024. Many independent estimates fall within this range. Compared to the national workforce, the cybersecurity workforce is more likely to be male and have a 4-year college degree or higher but is less likely to be unemployed. Many cybersecurity occupations, such as information security analysts, are projected among the fastest-growing occupations from 2022 to 2032.

- Cybersecurity work is captured in part in federal data sources from BLS, Census Bureau, NSF/NCSES, and Department of Education. However, they have limitations because SOC codes, Census occupation codes, and CIP codes that capture cybersecurity are not yet granular enough to identify the cybersecurity workforce using existing surveys.
- Data from nonfederal administrative sources address some of the data gaps in the absence of a comprehensive, single federal data source on the cybersecurity workforce. Data products from organizations like CyberSeek and the International Information System Security Certification Consortium (ISC2) quantify the workforce and provide some national-level estimates. Other independent sources, such as National Labor Exchange, ADP, LinkedIn, and Indeed, are a potential source of cybersecurity data, but lack of access and granularity make them insufficient to capture the entirety of the workforce.
- Several existing surveys have questions that can be relevant to a future pilot data collection on the cybersecurity workforce.
- Federal agencies beyond NSF are actively supporting workforce initiatives and data efforts related to cybersecurity, including NIST through the NICE Framework, OPM through its classifications of federal workers, CISA, CyberCorps, NSA/Department of Homeland Security National Centers for Academic Excellence in Cybersecurity, DoD, and other federal statistical agencies. There is an opportunity through CWDI to improve coordination among these entities.

Future data collection for the cybersecurity workforce should include a survey, or surveys, which collect individual-level data on cybersecurity workers. Future work will require a sampling frame that allows for data collection on the general population and that is specific to the cybersecurity workforce. For the CWDI, we are in the process of developing survey questions to be piloted. These questions will lead to an OMB submission for conducting cognitive interviews to test the recommended survey items. We are also working on identifying the proper sources of a pilot sample that can represent both the general population and the cybersecurity workforce. These critical tasks will help to build out the pilot study for NCSES to collect data on the cybersecurity workforce.

## Notes

<sup>1</sup> For the definitions interviews, we developed an open-ended interview protocol to understand the current state of the workforce and how different groups define it. RTI obtained approval from its institutional review board (IRB) under the Exempt Research determination. In January and February 2024, the CWDI project team conducted 14 interviews via videoconference with 23 federal (several interviews included multiple interviewees) and 9 nonfederal (private-sector and educational) representatives. This included a mix of cybersecurity industry experts, academic leaders, researchers, practitioners, and representatives of federal agencies actively collecting data on the cybersecurity workforce or hiring for cybersecurity positions. The CWDI project team identified participants through prior participation in NSF or National Institute of Standards and Technology (NIST) activities related to cybersecurity, review of academic leaders, and contacts among research leaders and inside key private sector, academic, and federal government agencies involved in cybersecurity and workforce.

<sup>2</sup> 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://nces.nsf.gov/760/assets/0/files/nces-cwdi-working-definitions.pdf>.

<sup>3</sup> For the knowledge gap interviews, we developed an open-ended interview protocol to understand the needed or desired information regarding the U.S. cybersecurity workforce. RTI obtained approval from its institutional review board (IRB) under the Exempt Research determination. In January and February 2024, the CWDI project team conducted 15 interviews via videoconference, with 7 federal interviews and interviewees and 9 nonfederal interviewees over 8 interviews. Participants represented a variety of organizations, including federal agencies, research laboratories, postsecondary education institutions, professional organizations for cybersecurity or information technology professionals, nonprofit organizations, and corporations. The CWDI project team identified participants through prior participation in NSF or National Institute of Standards and Technology (NIST) activities related to cybersecurity, review of academic leaders, and contacts among research leaders and inside key private sector, academic, and federal government agencies involved in cybersecurity and workforce.

<sup>4</sup> 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://nces.nsf.gov/about/cybersecurity-workforce-data-initiative>.

<sup>5</sup> Federal Committee on Statistical Methodology (FCSM). 2020. *A Framework for Data Quality*. FCSM 20-04. Washington, DC. Available at [https://nces.ed.gov/fcsm/pdf/FCSM.20.04\\_A\\_Framework\\_for\\_Data\\_Quality.pdf](https://nces.ed.gov/fcsm/pdf/FCSM.20.04_A_Framework_for_Data_Quality.pdf); Schmitt RR. 2020. *A Framework for Data Quality*. Washington, DC: Federal Committee on Statistical Methodology, Work Group on Transparent Reporting of Data Quality.

<sup>6</sup> Hogan M, Lilienthal K, Arbeit CA, Bean de Hernandez A; National Center for Science and Engineering Statistics (NCSES). 2024. *Cybersecurity Workforce Data Initiative: Federal Data Evaluation Report*. Alexandria, VA: National Science Foundation. Available at <https://nces.nsf.gov/about/cybersecurity-workforce-data-initiative>.

<sup>7</sup> Hogan M, Dominguez Garcia G, Arbeit C; National Center for Science and Engineering Statistics (NCSES). 2024. *Cybersecurity Workforce Data Initiative: Administrative Data Evaluation Report*. Alexandria, VA: National Science Foundation. Available at the Cybersecurity Workforce Data Initiative web page, <https://nces.nsf.gov/about/cybersecurity-workforce-data-initiative>.

---

<sup>8</sup> [The 2024 Statistical Policy Directive No. 15](#)