NSF | NCSES | Cybersecurity Workforce Data Initiative

Administrative Data Evaluation Report

September 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 the NCSES CWDI Working Group email address, NCSES-CWDI@nsf.gov.

NCSES Cybersecurity Workforce Data Initiative:

Administrative Data Evaluation Report

September 2024

Abstract

The Cybersecurity Workforce Data Initiative (CWDI) reviewed existing administrative, nonfederal data sources to determine their potential use to analyze and measure the U.S. cybersecurity workforce. These sources were analyzed to determine their integrity, objectivity, and utility for understanding the entirety of the workforce across the country in both the public and private sectors. Their utility included relevance to the cybersecurity workforce, granularity, accessibility, coverage, and timeliness of the analysis. The analysis showed that, of the 12 administrative, nonfederal data sources identified, none met the criteria of integrity and objectivity set by the standards of the Federal Committee on Statistical Methodology, based on available data. Sources included data from job boards, data from industry surveys, and proprietary data models, each of which presented different levels of relevance and granularity. Accessibility is a primary challenge with administrative data, as many sources require a paid subscription or membership for access. This analysis supports the development of a new federal pilot study to generate publicly available, reliable national data and estimates on the cybersecurity workforce.

Suggested Citation

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://ncses.nsf.gov/about/cybersecurity-workforce-data-initiative.

Contact

John Finamore and Ruiyi Li
CWDI Contracting Officer's Representative and Project Lead
Science Technology, and Innovation – Public Information
National Center for Science and Engineering Statistics
NCSES CWDI Working Group email address: ncses-cwdi@nsf.gov

Contents

Acknowledgements

Report Authors:

Michael Hogan, Guillermo Dominguez Garcia, Caren A. Arbeit, RTI International, under contract to the National Center for Science and Engineering Statistics (NCSES)

RTI International CWDI team email address: cwdi@rti.org

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

Executive Summary

The Cybersecurity Workforce Data Initiative, supported by the National Center for Science and Engineering Statistics within the U.S. National Science Foundation, is setting out to determine the feasibility of producing national estimates and statistics on the U.S. cybersecurity workforce. In response to this, RTI International conducted a series of analyses including defining the cybersecurity workforce, identifying knowledge gaps, assessing supply and demand, and evaluating federal data sources to analyze and measure the workforce. These steps showed that there was not a single data source providing the needed and relevant information to understand the entirety of the workforce. To complement this work, RTI reviewed administrative, nonfederal data available on the workforce to understand the landscape of data from job posting boards, nonfederal surveys, and private data providers and identify their relevance and ability to fill the existing gaps in the data.

RTI reviewed 12 administrative, nonfederal data sources most frequently identified by experts and stakeholders as related to the cybersecurity workforce. Nonfederal data sources fill an important role by collecting data from job boards, surveys, state-level data sources, and other administrative data and proprietary data sources that include information not necessarily covered by federal surveys. However, none of the 12 data sources produced national estimates on the cybersecurity workforce nor met the standards set by the Federal Committee on Statistical Methodology for utility, objectivity, and integrity. In some cases, the absence of access to the raw data or detailed methodology made it difficult for RTI to determine objectivity and integrity of the administrative data sources. The utility of the data varied based on the relevance and granularity of data available, including data on educational attainment, employment outcomes, race, gender, age, and other demographic variables. Across all sources, our analysis showed that accessibility was one of the largest challenges, with all sources presenting barriers to accessing proprietary data.

The data sources assessed fell into four broad categories. The first, job posting sites, rely on worker profiles from sources such as LinkedIn or Indeed that are matched with job postings from employers or from state workforce boards, in the case of the National Labor Exchange. These sources provide some high-level data publicly but require a paid subscription or service contract to access and conduct analysis. The second source category comprises industry surveys from business associations, which are useful for understanding a narrow subset of the workforce but have limited coverage and data accessibility. Third, proprietary data tools, such as CyberSeek, combine job posting and federal data to create analytical models of the workforce but do not have the readily accessible data needed to perform complex analysis. Last, payroll data sources, where we include ADP payroll data, provide comprehensive earnings data but lack the ability to map to existing occupational taxonomies.

Our analysis found that the current landscape of nonfederal administrative data, including job boards, professional associations, institutional surveys, and proprietary data products, offered a range of data estimates and tools that complemented federal data but was not sufficient or comprehensive enough to fully understand the workforce. High-quality data sources, such as CyberSeek and the International Information System Security Certification Consortium, rely on a mix of nonfederal and federal data from sources like the Bureau of Labor Statistics to build their models, and data providers emphasized in interviews the need for reliable, consistent federal data on the cybersecurity workforce. Because the administrative data reviewed is insufficient to meet the data gaps in the cybersecurity workforce, the development of a new federally led survey questionnaire and pilot study for producing national estimates of the cybersecurity workforce is supported.

Introduction

In 2023, the National Center for Science and Engineering Statistics (NCSES), a principal federal statistical agency within the U.S. National Science Foundation (NSF) began work on the Cybersecurity Workforce Data Initiative (CWDI) in response to a mandate in the CHIPS and Science Act of 2022. The CWDI is tasked with determining the feasibility of producing national estimates and statistics on the U.S. cybersecurity workforce. In response to this, RTI International conducted a series of analyses, including defining the cybersecurity workforce, identifying knowledge gaps, assessing supply and demand, and evaluating federal data sources, to analyze and measure the workforce. These steps showed that existing federal data was insufficient to capture the needed and relevant information to understand the entirety of the workforce. The findings showed that additional data was needed to accurately estimate key statistics, such as supply and demand and credential attainment, to address present and future workforce measurement needs.

Following these steps, RTI reviewed administrative, nonfederal data available on the U.S. cybersecurity workforce. Our analysis found that the current landscape of nonfederal administrative data, including job boards, professional associations, institutional surveys, and proprietary data products, offered a range of data estimates, methodologies, and tools that complemented federal data. The data allowed RTI to explore industry-specific data on jobs and credentials, as well as worker-specific data from both job board profiles and surveys. The data offered unique insights that were not captured by federal data, but no single source was sufficient or comprehensive enough to fully understand the workforce. The data sources assessed included a mix of relevant information about supply, demographics, credentials, and employment outcomes. However, data are not public or readily accessible across any of the sources at a level of granularity or timeliness to be able to produce national estimates on the cybersecurity workforce. This calls for a new federal pilot study on the cybersecurity workforce.

This report presents a review of the 12 administrative, nonfederal data sources most frequently identified by experts and stakeholders as related to the cybersecurity workforce. The goal is to provide an analysis of the feasibility of these data sources to fill the existing data gaps in the cybersecurity workforce as of August 2024.

Methodology

RTI reviewed 12 data sources from nonfederal and administrative data providers, examining them for relevance; ability to map to existing frameworks and taxonomies; granularity; and availability of information on credentials, employment outcomes, and demographics. Additionally, RTI assessed the data coverage, accessibility, and timeliness. RTI determined a preliminary list of sources through the expert interviews and input from the three workshops conducted on cybersecurity workforce definitions, knowledge gaps, and supply and demand. RTI solicited specific input during the supply and demand workshop, asking participants to provide input on the sources they frequently used and cited to understand the workforce.

As seen in table 1, participants responding to a poll in the third workshop most frequently cited LinkedIn, Indeed, CyberSeek, and USAJOBS as the most common sources of cybersecurity workforce data from job posting sites, each with 26 responses or more. Additional tools cited included ClearanceJobs, ZipRecruiter, the Department of Labor’s CareerOneStop, and the Computing Research Association (CRA) Taulbee Survey.

Table 1

Job posting sites, by workshop participant citation frequency: 2024

(Number)

Job posting site	Times cited by participants
LinkedIn	42
Indeed	31
CyberSeek	29
USAJOBS	26
ClearanceJobs	9
ZipRecruiter	7
CareerOneStop	7
Other	2

Note(s): Participants had the option to select all that apply.

Source(s):
National Center for Science and Engineering Statistics, Cybersecurity Workforce Data Initiative (CWDI), Workshop 3 Poll.

Using a similar approach to that of the *Cybersecurity Workforce Data Initiative: Federal Data Evaluation Report*, RTI referenced three domains of the Federal Committee on Statistical Methodology (FCSM) data quality framework when reviewing administrative data sources: utility, objectivity, and integrity.[1] In the absence of access to the raw data or detailed methodology, RTI could not determine objectivity and integrity of the administrative data sources. For example, RTI did not have access to the sampling methodology of membership surveys or to the reasoning behind how a job posting was determined to be a cybersecurity job on a job site. With data that is publicly available, it is difficult to determine the reliability or quality of data from job posting sites that may contain duplicate job postings, evergreen job postings that remain open indefinitely, or job postings that may or may not be actively accepting applications. Similarly, there is insufficient data to determine the reliability of profiles from jobseekers. Proprietary data tools relied on a mix of data from job sites and federal data sources, but there was no information to determine objectivity or integrity of the results. RTI reviewed the utility of each data source based on the data available, focusing on

- relevance to the cybersecurity workforce, including how it determines cybersecurity jobs and whether it maps to existing taxonomies or frameworks, such as the NICE Framework;
- granularity of data, including demographic data (e.g., gender, race, ethnicity, age, and other characteristics) of the cybersecurity workforce, as well as detailed data on employment outcomes, wages, hours, occupations, work activities, and credential attainment;
- accessibility of underlying data, methodology, and relevant reports—in the case of proprietary data providers, data access costs and requirements;
- coverage and sample size, including coverage of the cybersecurity workforce, because some data sources are limited to a subset of workers—such as members of a professional organization or certificate holders—which may not capture the entirety of the workforce; and
- timeliness of data and punctuality of results.

RTI reviewed data from the following administrative, nonfederal sources outlined in table 2. Sources in this report are presented in alphabetical order under four subcategories: job posting site, payroll data, proprietary data model, and survey. In our analysis, we include data from both surveys and data collected through job postings and payroll data, as well as sources that combine proprietary and federal data, such as CyberSeek.

Table 2

Administrative data source type, by subcategory: 2024

(Data source and data type)

Subcategory	Data source	Data type
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 Certifications	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).

Additionally, RTI reviewed other sources, including the following, and determined they did not have enough utility to understand the cybersecurity workforce:

- Certification data from vendors like Red Hat, Microsoft, Cisco, and Amazon were limited to their proprietary certifications and could not encompass the entirety of the workforce.

- Business data from financial firms, such as PitchBook or Bloomberg, had valuable information on trends in venture capital, initial public offerings, and financial performance of cybersecurity firms, but RTI determined they did not provide data related to the workforce. The Securities and Exchanges Commission includes cybersecurity and cyber incidents in the required disclosures of public companies, but the disclosures do not explicitly include data on the workforce.[2]

- Publications and data from administrative providers like CrowdStrike and Advisen contain information on the risks and costs associated with reported cybersecurity breaches but do not contain data on the workforce.

- USAJOBS is a job posting site for the federal government. RTI reviewed federal jobs data through the Office of Personnel Management in the *Cybersecurity Workforce Data Initiative: Federal Data Evaluation Report*, so USAJOBS is outside the scope of this report. RTI determined that USAJOBS is a reliable data source for federal postings but does not cover the entirety of the workforce.

RTI conducted an in-depth review of the data sources identified in table 2 to understand how they could address the feasibility of producing national-level statistics on the cybersecurity workforce. Although no individual data source meets all the criteria in the FCSM data quality framework, together they present unique and useful approaches to understanding the workforce and a perspective on how nonfederal actors are quantifying the workforce. In its upcoming work, RTI is requesting data and questionnaires from these sources, where applicable, to be able to better understand how they estimate the workforce and what lessons can be learned for the CWDI.

Analysis of Data Sources

Although RTI could not consistently determine the objectivity and integrity of the 12 administrative data sources reviewed based on the FCSM data quality framework, RTI reviewed the sources based on their utility, including relevance, granularity, accessibility, coverage and sample size, and timeliness. This section provides a review of the 12 data sources based on RTI's analysis of publicly available data, interviews, and initial data requests in July and August 2024.

Table 3 summarizes the strengths and limitations of each data source in alphabetical order. A full review of each data source is included in the Data Source Summaries section and in table A-1 in the appendix.

Table 3

Cybersecurity workforce relevance and limitations, by data source: 2024

(Strengths and limitations)

Subcategory	Data source	Cybersecurity workforce relevance (strengths)	Cybersecurity workforce gaps (limitations)
Job posting site	ClearanceJobs	ClearanceJobs is a job posting site that publishes job advertisements of positions that require security clearances. It also provides reports with salaries of certain IT and security occupations.	The positions are not linked to existing taxonomies; the sample is restricted to jobs requiring clearances; reports provide information only at an aggregate level.
Job posting site	Indeed	Indeed data are frequently cited in labor market research. Their data come from job postings on its own platform. Indeed provides data on job availability, salary ranges, skill requirements, and geographical distribution of cybersecurity roles. Indeed Hiring Insights also publishes reports using employee surveys, jobseeker surveys, user interactions, and BLS data.	No alignment to other existing taxonomies; data are not as granular as LinkedIn's, particularly when it comes to industry trends.
Job posting site	LinkedIn	LinkedIn data are a widely cited source of job posting information. LinkedIn Talent Solutions offers customized reports to understand career pathways and employment trends by job titles, roles, experience levels, geography, skill sets, and degree.	LinkedIn data are not mapped to commonly used taxonomies. It is possible to run into duplicate job postings or "evergreen" jobs.
Job posting site	National Labor Exchange	The National Labor Exchange aggregates job listings from state job banks, private employers, and other job postings, paying special attention to posting deduplication. It provides educational requirements for specific job listings. Job posting keywords are linked to the NICE Framework.	Reports are not specific to cybersecurity. It may omit job postings included in private companies, such as LinkedIn. It is unknown how much data are available on jobseekers.
Job posting site	ZipRecruiter	ZipRecruiter is a job posting site linked to O*NET and SOC codes. Their annual Labor Market Outlook report discusses cybersecurity when discussing the supply of government jobs. ZipRecruiter also provides a Job Growth dashboard, as well as surveys on job confidence of new hires.	ZipRecruiter reports seldom delve into cybersecurity. Their administrative data are linked to O*NET but do not specifically define cybersecurity.
Payroll data	ADP	ADP Research Institute data are derived from payroll transactions, capturing more than 25 million U.S. workers, as well as from ongoing surveys that have reached more than 550,000 workers in 29 countries. The data offer insights into wages, salaries, and worker demographics across various industries, including cybersecurity. The data include detailed earnings information elements like overtime, bonuses, and commissions; job location; ability to work remotely; worker feelings on artificial intelligence impacts to their jobs; and salary expectations.	Data are not mapped to any occupational code framework. Additionally, is the data are limited to individuals employed by ADP client companies and do not provide insights into certifications, career pathways, or skills required for cybersecurity roles.
Proprietary data tool	CyberSeek	CyberSeek provides proprietary data from Lightcast on the supply and demand of cybersecurity. The jobs are mapped using the NICE Framework. It is the most frequently cited administrative data source and provides national estimates of the cybersecurity workforce as interactive tools that help users identify career pathways based on certifications or jobs held.	CyberSeek data rely on proprietary data and modeling that are not replicable or widely accessible. There is also a lack of data on the workforce pipeline.

Subcategory	Data source	Cybersecurity workforce relevance (strengths)	Cybersecurity workforce gaps (limitations)
Survey	CompTIA	CompTIA is a large member organization for cybersecurity professionals and a certification provider. Their website provides information on potential career pathways with each credential offered. It also provides information on credentials needed to achieve a role, median salary, and job growth trends via BLS OEWS data. Occupations are linked to NICE codes.	CompTIA does not provide information on credential attainment, such as the number of certificate holders. One may be able to obtain these by contacting them. The sample size is limited to members.
Survey	CRA Taulbee Survey	Survey of computer science, computer engineering, or information PhD-granting institutions. The survey provides information on demographics of graduating students and enrolled students, as well as those post-graduation.	Sample is limited to PhD-granting institutions in computer science, computer engineering, and information. There is no mapping to existing taxonomies, and public information is only available at an aggregate level.
Survey	ISC2	ISC2 provides global and national estimates of the cybersecurity workforce via a mix of survey responses and modeling from BLS's Quarterly Census of Employment and Wages, the Census Bureau's Statistics of U.S. Businesses, and the Census Bureau's County Business Patterns.	ISC2 data provide limited information on employment outcomes. For example, ISC2 does not provide data on salary outcomes by job title or skill within cybersecurity. Additionally, occupations are not mapped to commonly used taxonomies.
Survey	SANS Institute/GIAC Certifications	Provides a report surveying human resources and cybersecurity managers on their perceived effectiveness of employees, hiring challenges, and overall experience. The survey also delves into the top five NICE cybersecurity work role categories (Investigation, Implementation and Operation, Oversight and Governance, Design and Development, Protection and Defense).	Data are limited to surveys of human resources and cybersecurity managers who respond to the survey. These typically include those that have trained with the SANS Institute. The reports lack granularity.
Survey	WiCyS/N2K	WiCyS publishes an annual report on women in cybersecurity, detailing the capabilities of members and aligning them with NICE standards. The *State of Inclusion* report also surveys members on the structural barriers that women in cybersecurity experience.	The sample size is limited to women who are members; the data are not granular because statistics are lumped into large categories.

BLS = Bureau of Labor Statistics; CompTIA = Computing Technology Industry Association; CRA = Computing Research Association; ISC2 = International Information System Security Certification Consortium; IT = information technology; OEWS = Occupational Employment and Wage Statistics; O*NET = Occupational Information Network; SOC = Standard Occupational Classification; WiCyS = Women in CyberSecurity.

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

Relevance

RTI determined the 12 data sources had some relevance to the cybersecurity workforce, identifying CyberSeek, the International Information System Security Certification Consortium (ISC2), and the National Labor Exchange (NLx) as having the highest relevance to the whole workforce. Although the sources take different approaches to understanding the whole of the U.S. cybersecurity workforce, they provided the most comprehensive national view of the workforce, including data on supply and demand, credentials, geographic distribution, and job titles and roles.

- CyberSeek focuses exclusively on the United States, whereas ISC2 collects data globally. CyberSeek is the most frequently cited administrative data source in the United States related to cybersecurity, relying on data from Lightcast, a data analytics firm that combines job postings data with data from federal sources, such as the Bureau of Labor Statistics (BLS) and the Department of Education, to model workforce statistics.

- ISC2 combines data from BLS's Quarterly Census of Employment and Wages, the Census Bureau's Statistics of U.S. Businesses, and the Census Bureau's County Business Patterns with its own member survey to provide global and national estimates of the cybersecurity workforce. ISC2 includes detailed questions about work roles, job titles, industries, credentials and certificates, and demographic information in its member survey, which it analyzes and shares in its annual report.

- The NLx combines data from employers and state workforce agencies to create a list of job openings that align with federal standards, such as the NICE Framework, as well as state workforce data, such as unemployment and workforce development agencies.

Other sources are either limited in their scope or do not collect relevant information. For instance, the CRA Taulbee Survey's sample is limited to PhD-granting institutions in computer science, computer engineering, and information, and the Women in Cybersecurity (WiCyS) survey is limited to women who are members. ClearanceJobs is limited to jobs that require federal security clearance. Additionally, job posting sites, such as Indeed or LinkedIn, often have "evergreen" postings, "ghost" postings, or duplicates, limiting the accuracy of the supply-side data. Payroll data from ADP offer a perspective on job trends at a national level, but do not have a high level of granularity on workplace activities, job titles, or occupations.

As a component of relevance, we examined how the administrative data sources could potentially be mapped to existing frameworks or taxonomies. Of the administrative data sources, five are aligned to the NICE Framework through keywords or references, including CyberSeek, the Computing Technology Industry Association (CompTIA), the WiCyS/N2K survey, the SANS Institute/GIAC Certifications, and the NLx. Only one job board, ZipRecruiter, is aligned with the Occupational Information Network (O*NET) or Standard Occupational Classification (SOC) codes. Others, such as LinkedIn and Indeed, use their own proprietary taxonomies.

Quantifying the cybersecurity workforce without mapping to existing taxonomies is complicated because it relies on the researcher selecting keywords that encompass all of the workforce. RTI found that cybersecurity workers hold many different titles and perform roles that these sources may not capture, and it relies on those surveyed (or in the case of job posting sites, members) to accurately describe their roles, tasks, and occupations.

Granularity

Among the data sources, there is a high variability in the granularity of data collected and reported. Across all the data, sources collect information on one or more of the following: geography, race, sex and gender identity, ethnicity, employment status, age, educational background, experience level, disability status, and specific questions related to work activities and expertise. Granular data related to social identity and demographic indicators are not reported consistently, and different sources share different levels of detail.

In most cases, the publicly available data are in the form of reports or aggregated results, making it difficult to analyze the data at a granular level. Platforms like Indeed and LinkedIn provide industry-specific reports but require subscription to a paid service or a data use agreement. Sources including ClearanceJobs, CompTIA, CRA Taulbee Survey, and ISC2 provide aggregate information on the earnings of workers, by job sector, credential, college degree, or other demographic information. However, granular data is not publicly available.

Finally, several of the sources provide data that is not specific to the cybersecurity workforce. For instance, reports on ClearanceJobs are limited to the information technology (IT) and security occupations (but not specific to cybersecurity), and ZipRecruiter's reports are not broken down by job sector.

Accessibility

Of the 12 data sources, none make their raw data accessible to the public. There are varying levels of public data shared by data providers that allow for some summary statistics and high-level findings, as well as interactive data tools that present aggregate findings, such as with CyberSeek. To access data, different sources require different approaches.

- Requires paid subscription to data service: LinkedIn Talent Insights, Indeed Hiring Insights, Lightcast (part of CyberSeek)

- Offers aggregate reports free to download: ISC2 Survey, WiCyS Survey, SANS/GIAC Survey, ClearanceJobs, CRA Taulbee Survey, the NLx

- Allows for data access through a data use agreement: LinkedIn (agreement with NSF), the NLx

- Publishes quarterly updates on trends in the workforce: ADP

- Requires membership to organization: CompTIA

Job posting boards, including ClearanceJobs, ZipRecruiter, LinkedIn, and Indeed, are free to browse and provide some limited summary statistics on current job postings, but analytics and detailed data require a paid subscription or a data service. The NLx allows for granular data analysis through a data sharing agreement.

Coverage and Sample Size

Among the nonfederal and administrative data sources, the coverage and sample size vary.

Job posting boards contain data on their users, including employers and jobseekers. The NLx, ZipRecruiter, LinkedIn, and Indeed are marketed to a national workforce, including private sector and public sector employment. ClearanceJobs is limited to job postings that require security clearance, which are most frequently in the government, national security, and defense sectors. As mentioned earlier in the report, challenges with the use of job boards data include duplicate job postings and "evergreen" or "ghost" job postings, where companies post openings to collect résumés, but it is unknown if the posting results in a new employee hired. The NLx emphasizes that job postings on its site do not have duplicates or scams, but estimates of evergreen or ghost job postings on other sites vary.

Survey sample sizes range. The ISC2 workforce study relied on an online survey and collected data from 14,865 individuals around the world, modeling the workforce at 5.5 million people. Approximately 40% of survey respondents were located in the United States. CompTIA's sample size is unknown but surveys certification program and exam participants, as well as employers hiring in cybersecurity. The CRA Taulbee Survey provides information on 176 of 314 member departments in computer science, computer engineering, and information.[3] SANS/GIAC interviews human resource and cybersecurity managers. WiCyS surveys approximately 8,000 women who are members of their organization.

Payroll data from ADP cover an estimated 25 million workers in the United States, providing the largest sample size among the nonfederal data sources. CyberSeek, the most relevant source for purposes of capturing the U.S. cybersecurity workforce, does not provide details on their sample size but estimated that in 2022, there were 1.1 million workers employed in cybersecurity and 755,743 open cybersecurity positions. CyberSeek builds on a data model from Lightcast, which combines job postings data with federal data from the Census Bureau, Department of Education, and BLS.

Timeliness

The range in timeliness of the data in these sources is wide. Job posting sites provide real-time information as jobseekers are made aware of new job postings and vice versa, but we do not know how up-to-date the data on the paid services of LinkedIn and Indeed are. CyberSeek provides data for the most recent 12-month period and is continuously updated.

Other sources publish annual, quarterly, or monthly reports or updates. For example, the most recent ClearanceJobs report contained 2022 data. ISC2 publishes its workforce report annually, and a new version for 2024 is set to be released. ZipRecruiter publishes updates on labor market trends for major industries monthly or quarterly, and ADP publishes a quarterly workforce report.

Conclusions and Recommendations for Survey Development

The review of 12 recommended data sources shows that they do not have the granularity, accessibility, reliability, timeliness, and coverage to fully capture the national cybersecurity workforce. Based on our analysis, a new data source to comprehensively capture the U.S. cybersecurity workforce is needed. To reinforce this need, interviewees who represented administrative data providers emphasized a need for a comprehensive, reliable, federally led data effort to better understand the national cybersecurity workforce. A pilot study and survey are needed to fully understand who comprises the cybersecurity workforce, including their demographics, pathways into the workforce, and experiences.

This administrative data currently fills a gap in understanding the workforce, partially due to the lack of an existing federal data source that comprehensively defines the workforce. Sources like CyberSeek and the ISC2 survey are frequently cited by industry professionals to understand the needs in the workforce, and sources like LinkedIn were the most frequently cited by participants in the CWDI supply and demand workshop. However, the main limitations of these sources are the lack of data availability or access, the often-missing alignment to existing taxonomies, the lack of granularity or focus on the cybersecurity workforce, or the focus on subgroups of the cybersecurity workforce. Although accessing raw data from job posting sites and proprietary data tools will help us better understand the cybersecurity workforce, they have their limitations. For example, job posting sites aggregate data from postings, but it is unclear if job postings are evergreen or duplicates, or if the skills and credentials match those sought by the hiring companies. In the next step in the CWDI, RTI will take a deeper dive into the high-priority administrative and nonfederal data cited in this report, including data from LinkedIn, ISC2, CyberSeek, and the NLx.

These existing administrative data tools are valuable for identifying important variables that a new data effort should include, such as demographics (age, gender, sex, race), geographic location, and educational attainment (including both degrees and certifications, in some cases). Additionally, they show the value of understanding career pathways, job titles, occupations, and cybersecurity work activities. Finally, there are surveys that capture barriers to success in the field, attrition and retention, and obstacles for different groups, including women, workers without 4-year college degrees, and other underrepresented groups in the cybersecurity workforce. These surveys reinforce many of the challenges and gaps identified in the interviews and workshops.

Data Source Summaries

Below we provide our findings by data source type. A detailed overview of each data source is found in table A-1 in the appendix. Within each subcategory (job posting sites, proprietary data tools, and surveys), sources are presented in alphabetical order.

Job Posting Sites

ClearanceJobs

ClearanceJobs is a large career network platform for professionals seeking jobs that require federal government security clearance. Jobseekers can search for jobs requiring varying levels of clearance, and employers can post positions and search for candidates that have the required clearances. As of August 9, 2024, the site had 65,124 active security clearance jobs from 2,042 prescreened hiring companies.

Relevance and Connection to Existing Frameworks

ClearanceJobs has low relevance, as it only includes data of employers requiring security clearances and of employees who work for them. There are no linkages to existing frameworks.

Granularity

ClearanceJobs provides salary information by education level and certification attainment. It also provides compensation level by experience level and clearance level, as well as by state.

Coverage and Sample Size

Reported data are based on 22,368 survey responses from 2022. Additionally, ClearanceJobs claims to have more than 1,660,000 candidates in its platform and to provide 54,243 job listings per month. All jobs posted require a security clearance, and the platform targets those who hold one. To become a candidate, one needs to be a U.S. citizen with active or current security clearance issued by the federal government.

Accessibility

Aggregated outputs are available on the website, and users can browse job postings. However, more detailed results require contacting ClearanceJobs.

Timeliness

Data reported publicly are presented for the most recent 12-month period for which data are available, and data are updated annually, though the last annual report is from 2022.

Links to Data

ClearanceJobs' The 2024 Security Clearance Compensation Report: The Year of the Breakthrough pdf: https://about.clearancejobs.com/hubfs/pdfs/2024SecurityClearanceCompensationSurveyReport.pdf

ClearanceJobs online Employers Dashboard: https://about.clearancejobs.com/employers/features/dashboard

Indeed

Indeed is a job search engine and employment site that compiles job listings. It allows users to search for jobs and post résumés and employers to post jobs.

Relevance and Connection to Existing Frameworks

Indeed is of medium relevance because, even though it provides a picture of job openings, it does not map to existing frameworks.

Granularity

Indeed collects age, race, and ethnicity of jobseekers, which is provided through Indeed Hiring Insights at an aggregate level (we currently do not have access). The same service also provides trends of credential requirements by job type, educational attainment of employees for certain employers, hiring trends by industry, and the most sought-after skills and certifications over time. Members without access to this paid service can only see job postings, which may include required skills, education, and experience; expected salary; and job location.

Coverage and Sample Size

The data cover users of the platform, which includes 225 million résumés and 25 million job postings worldwide. Researchers can use keywords to narrow the sample to cybersecurity jobseekers and job postings.

Accessibility

Paid access is required for Indeed Hiring Insights, but access is free to view specific job postings.

Timeliness

Data are updated in real time.

Links to Data

Indeed for employers Hiring Insights reports web page:
https://www.indeed.com/employers/hiring-insights

LinkedIn

LinkedIn is a job posting site that allows users to connect with other professionals for networking. It also allows users to apply for jobs, share professional content, and learn technical skills via online course offerings. LinkedIn also enables employers to recruit candidates for their companies.

Relevance and Connection to Existing Frameworks

LinkedIn is of medium relevance because, even though it provides a picture of job openings, it does not map to existing frameworks.

Granularity

LinkedIn collects users' gender, educational background, experience level, skills, and expertise. Paid data access provides these data, as well as information on job transition and promotions, career pathways, and industry-specific employment trends. Users can access job postings, which include job requirements, location, and sometimes salary ranges, for free.

Coverage and Sample Size

LinkedIn draws from more than 12 billion data points across its network. Data are collected from member profiles. For this project, the cybersecurity workforce is defined on LinkedIn by the researcher, as they restrict the cybersecurity workforce to members who have cybersecurity-related roles, skills, and educational backgrounds, as well as job postings related to cybersecurity.

Accessibility

Members can view other profiles and job postings for free and access additional data through a paid subscription to LinkedIn Talent Solutions. NSF has a data use agreement with LinkedIn.

Timeliness

Data are updated in real time.

Links to Data

LinkedIn Talent Solutions web page: https://business.linkedin.com/talent-solutions

LinkedIn Pressroom Data and Insights web page: https://news.linkedin.com/data-and-insights

NLx

The NLx is a partnership between the National Association of State Workforce Agencies (NASWA) and the DirectEmployers Association. It connects employers, state workforce agencies, and jobseekers with job openings.

Relevance and Connection to Existing Frameworks

The NLx is of high relevance, as it aggregates job listings from state job banks and private employers while deduplicating job postings. Keywords in its search engine are aligned to the NICE Framework. However, the site does not provide demographic data of users or jobseekers.

Granularity

The NLx provides information on educational requirements for specific job listings, as well as state-level and national-level reports on the entire U.S. labor force, not specific to cybersecurity. There is the potential to do searches by keywords and understand more data shared by state workforce boards in the NLx.

Coverage and Sample Size

The NLx includes more than 19,000 jobs with the "cybersecurity" keyword.

Accessibility

The NLx does not provide reports or surveys, but NASWA does. Reports and surveys are accessible but do not contain information specific to the cybersecurity workforce. NLx data are available through a data use agreement.

Timeliness

NASWA reports are released annually. These reports do not call out cybersecurity specifically.

Links to Data

The NLx About Us web page: https://usnlx.com/about

The NASWA 2023 State of the Workforce web page: https://www.naswa.org/reports/state-of-the-workforce-2023

ZipRecruiter

ZipRecruiter is a job posting platform that connects jobseekers with employers, similar to Indeed. Jobseekers can upload their résumé and apply to jobs, and employers can post open positions.

Relevance and Connection to Existing Frameworks

ZipRecruiter is of medium relevance. It is aligned to O*NET and SOC codes and can provide a datapoint of job openings; however, demographic information is kept confidential, and the sample size is unknown.

Granularity

ZipRecruiter collects the age, gender, race, ethnicity, and educational backgrounds of jobseekers for reports. However, individual-level information is not available.

Coverage and Sample Size

The sample size is unknown. It includes job postings categorized under cybersecurity.

Accessibility

Reports are available, but they do not provide information specific to the cybersecurity workforce.

Timeliness

Reports are released annually. ZipRecruiter also provides updates on labor market trends for major industries quarterly or monthly.

Links to Data

Zip Recruiter Economic Research’s Labor Market Outlook report web page: https://www.ziprecruiter-research.org/labor-market-outlook-report

Zip Recruiter Labor Market Insights web page: https://www.ziprecruiter.com/blog/datalab/

Payroll Data

ADP

ADP is a provider of human capital management solutions. Their Pay Insights Web page provides aggregate-level data on pay over time by characteristics (gender, age, industry, firm size, worker mobility).

Relevance and Connection to Existing Frameworks

ADP is of medium relevance. It provides highly relevant information on pay over time; however, the data are not aligned to existing taxonomies. Historical pay trends are publicly downloadable but grouped by overly broad industry classifications, such as “education and health services” or “financial activities.”

Granularity

ADP payroll data track salary, other types of pay (e.g., overtime and commissions), and demographics (e.g., gender and age) but do not have information on educational background or specific occupational codes. The information publicly available is at a granular level.

Coverage and Sample Size

The data cover workers who are employed by companies that use ADP as their human capital management platform, including more than 25 million workers in the United States. Surveys are also administered frequently on special topics—such as workers’ responses to the COVID-19 pandemic or how remote work is evolving with artificial intelligence—with the sample size often being a subset of ADP users. For instance, the last published report, *Today at Work*, leverages data from a survey of more than 550,000 workers in 29 countries.

Accessibility

Reports and pay levels by worker mobility (i.e., job stayer versus job changer), gender, age, industry, and firm size are publicly available. Individual-level data or cybersecurity-specific data are not available.

Timeliness

Data are updated continuously and are shown in ADP Pay Insights as of the last completed month.

Links to Data

ADP Research Pay Insights web page: https://workforcereport.adp.com/

Proprietary Data Model

CyberSeek

CyberSeek is a comprehensive data product developed by data provider Lightcast with the support of CompTIA and NICE, tracking cybersecurity workers and job openings across the United States. It is a frequently cited source of data on the workforce and compiles a mix of job postings data, employee profiles from job boards, and federal data from sources like BLS to model the size of the U.S. workforce and track trends over time, education level, and geography.

Relevance and Connection to Existing Frameworks

CyberSeek is highly relevant and looks nationally at the cybersecurity workforce, linking its data to the NICE Framework.

Granularity

Data are available at the national, state, and metropolitan statistical area levels in the public data tools, whereas additional, more granular data requires a paid subscription. Public data does not present demographic data but does present summary data on credential attainment and employment outcomes.

Coverage and Sample Size

The data are based on a model, and a sample size for the survey is not provided. CyberSeek estimates 1.1 million employed cybersecurity workers in the United States. Data model a national estimate of the entire workforce modeled from Lightcast definitions, public job postings, and modeling based on criteria from the NICE Framework.

Accessibility

Aggregated outputs are available on the website, but more detailed results require a paid subscription.

Timeliness

Data are presented for the most recent 12-month period for which data are available and are continuously updated.

Links to Data

CyberSeek's online interactive Cybersecurity Supply/Demand heat map:
https://www.cyberseek.org/heatmap.html

Surveys

CompTIA

CompTIA is a provider of professional IT certifications. It also provides training materials, a network of IT professionals, and industry research on labor force trends and technology adoption.

Relevance and Connection to Existing Frameworks

CompTIA is of medium relevance. It is aligned to NICE codes and provides salary information and job growth trends of certificate holders, but the number of certificates awarded is not publicly available.

Granularity

CompTIA collects age, race, and sexual orientation of members who take certification exams. The website also outlines potential career pathways that one can follow with each type of credential. Its survey of employers asks about the skills they need in new hires. Median salary and job growth trends of certificate holders are also accessible.

Coverage and Sample Size

The survey covers CompTIA certification program and exam participants, as well as employers hiring in cybersecurity. The sample size is unknown.

Accessibility

The annual report is available. However, there are no details on how many certificates are awarded by type of certificate or employment outcomes.

Timeliness

Data are updated annually.

Links to Data

CompTIA’s State of the Tech Workforce: Cyberstates 2024 report pdf: https://comptiacdn.azureedge.net/webcontent/docs/default-source/research-reports/comptia-state-of-the-tech-workforce-2024.pdf?sfvrsn=a8aa5246_2

CRA Taulbee Survey

The CRA Taulbee Survey is an organizational survey of PhD-granting departments in computer science, computer engineering, and information in the United States. The survey collects demographic information, as well as employment outcomes, of recent PhD recipients. It also collects salary and demographic information of faculty in the surveyed departments.

Relevance and Connection to Existing Frameworks

The CRA Taulbee Survey does not map to any existing taxonomy. It is of low relevance, as it only samples computer science, computer engineering, and information at U.S. PhD-granting institutions. It does not identify cybersecurity in its annual report.

Granularity

The survey collects information on gender, race, ethnicity, and residency status for new doctoral recipients and years of experience for faculty. Additionally, it collects the field of the PhD received and the employment industry and salary of new recipients.

Coverage and Sample Size

Of the 314 surveyed departments, 176 responded to the survey in 2023. Member departments include but are not limited to U.S. PhD-granting departments in computer science, computer engineering, and information.[4]

Accessibility

Annual reports are free to download, but raw data are unavailable.

Timeliness

Data are updated annually.

Links to Data

The CRA Taulbee Survey web page: https://cra.org/resources/taulbee-survey/

ISC2

ISC2 is the world's largest member association for cybersecurity professionals, encompassing nearly 675,000 members. ISC2 offers certifications and trainings and provides research on the cybersecurity workforce.

Relevance and Connection to Existing Frameworks

ISC2 is highly relevant. It models the size of the entire cybersecurity workforce and provides research on the cybersecurity workforce gap and the representation of women and minorities in the field, as well as tools for effective hiring, retention, and team building. Their data are not mapped to existing frameworks.

Granularity

ISC2 collects information on geographic location of members and chapters, age, gender, employment status, level of experience, certification received, and employment outcomes and wages based on certification. It also estimates U.S. workforce gaps based on federal surveys.

Coverage and Sample Size

ISC2 uses a mix of survey responses from its internal membership survey, as well as modeling from BLS's Quarterly Census of Employment and Wages, the Census Bureau's Statistics of U.S. Businesses, and the Census Bureau's County Business Patterns. The last workforce study—from 2023—surveyed 14,865 international cybersecurity practitioners and decision-makers.

Accessibility

The report is available to the public. The raw data are not.

Timeliness

ISC2 provides annual updates.

Links to Data

ISC2 Cybersecurity Research web page: https://www.isc2.org/research

SANS/GIAC

GIAC Certifications is the certification branch of SANS Institute, a private organization that offers information security training and certifications. GIAC offers more than 30 certifications aimed to upskill cybersecurity practitioners.

Relevance and Connection to Existing Frameworks

GIAC is of low relevance, as it does not appear to collect data on workers. It is, however, aligned to NICE codes. The GIAC Cyber Workforce Research Report asks human resource and cybersecurity managers about skills gaps and headcount gaps in their workforces.

Granularity

GIAC collects information on the number of companies that have trained with SANS and the number of GIAC alumni. It also surveys on the perceived effectiveness of employees, their experiences, and hiring challenges, from the point of view of human resource managers. No demographic data are available.

Coverage and Sample Size

The sample size is unknown. The survey covers human resource and cybersecurity managers of companies who responded to the survey and focuses on mid-level cybersecurity practitioners. The survey inquired about the top five NICE cybersecurity work roles.

Accessibility

The report is free to download, but the data presented are at an aggregate level.

Timeliness

Data are updated annually, with the most recent update in May 2024.

Links to Data

GIAC Certifications' 2024 SANS GIAC Cyber Workforce Research Report web page: https://www.giac.org/mlp/2024-attract-hire-retain-midlevel-cybersecurity-roles/

WiCyS/N2K

WiCyS is a nonprofit organization that aims to support women in the field and reduce the gender gap in cybersecurity. It hosts an annual conference, skill development programs, and mentorship programs, among other resources. N2K focuses on cybersecurity education and awareness and often collaborates with WiCyS.

Relevance and Connection to Existing Frameworks

WiCyS/N2K are relevant, as they help detail the experiences of women in cybersecurity, including the barriers and resources that may help close the headcount and retention gender gap. They are aligned to the NICE Framework.

Granularity

WiCyS/N2K collect information on gender, disability status, race, N2K certifications held, and structural barriers. N2K offers a Skills Diagnostics Dashboard, Benchmark and Comparisons, and other relevant reports not available to the public. It also appears to provide workforce trends on chief information security officers. WiCyS provides a Cyber Talent Study detailing the capabilities of its members, which is aligned with NICE standards.

Coverage and Sample Size

The WiCyS Cyber Talent Study, the only publicly available resource these organizations provide, surveys 7,999 women who are members of the organization. N2K studies survey cybersecurity professionals and employers, but the sample size is unknown.

Accessibility

Executive summaries of WiCyS reports, as well as the full annual report, are available. N2K reports are not available.

Timeliness

WiCyS reports are updated annually.

Links to Data

N2K Strategy Guide e-book web page: https://www.n2k.com/strategy-guide

Women in Cybersecurity State of Inclusion web page: https://www.wicys.org/initiatives/wicys-state-of-inclusion/

Appendix: Summary of Sources Reviewed

Table A-1

Detailed characteristics of data sources reviewed for analysis, by subcategory: 2024

(Characteristics)

Subcategory	Source	Relevance	Ability to map to existing taxonomies and frameworks	Granularity of demographic data	Ability to provide information on credential attainment	Ability to provide information on employment outcomes	Coverage and sample size	Coverage of cybersecurity workforce	Accessibility	Timeliness
Job posting site	ClearanceJobs	Low: no relevant data except of salaries of employers requiring security clearances	None	Age and gender	Salary by educational level of jobs that require security clearance, as well as salary by experience level and location	Salary information of certain IT and security occupations	Employee survey of 22,368 respondents with a job requiring a security clearance	Not specific to cybersecurity; just IT and "security"	Report is free to download; data are at an aggregate level	Annual update, though last one is from 2022
Job posting site	Indeed	Medium: complicated to map to codes and frameworks but can give a sense of job openings	No; based on job postings and profiles	Collects age, sex, race, ethnicity, and disability status of jobseekers (provided through Indeed Hiring Insights at an aggregate level, to which we do not currently have access)	Trends of credential requirements by job posting; educational attainment of employees from select companies	Hiring trends for specific industries, most sought-after skills and certifications over time	Has 225 million résumés and 25 million job postings worldwide	Data based on job title, descriptions, and required skills listed on postings related to cybersecurity	Paid access required to Indeed Hiring Insights; free to access specific job postings	Real-time updates; depend on how often users update
Job posting site	LinkedIn	Medium: complicated to map to codes and frameworks but can give a sense of job openings	No; based on job postings and profiles	Collects user's gender, educational background, location, experience level, and skills and expertise	Educational background, such as degrees earned and field of study, professional certifications and licenses (in LinkedIn Talent Insights, to which we currently do not have access)	Job transitions and promotions, career pathways, employment trends	Users of the website; draws from over 12 billion data points across the LinkedIn network	Data from public and private profile information from LinkedIn members who have specified cybersecurity-related roles, skills, and educational background; data also collected from job postings, company pages	Requires paid access to LinkedIn Talent Solutions; NSF has an existing data sharing agreement with LinkedIn	Real-time updates; depend on how often users update
Job posting site	National Labor Exchange	High: aggregates job listings from state job banks, private employers, and other job posting sites; job postings are deduplicated	Keywords aligned to NICE Framework	None	Provides information on educational requirements for specific job listings	State-level and national-level reports on the overall labor force but no information specific to cybersecurity	19,000 jobs with the "cybersecurity" keyword	Job postings from private company listings and state job banks	Report free to download; job listings free to browse; data sharing agreements exist	Listings updated in real time; NASWA reports updated annually

Subcategory	Source	Relevance	Ability to map to existing taxonomies and frameworks	Granularity of demographic data	Ability to provide information on credential attainment	Ability to provide information on employment outcomes	Coverage and sample size	Coverage of cybersecurity workforce	Accessibility	Timeliness
Job posting site	ZipRecruiter	Medium: can give a sense of job openings	Aligned to O*NET and SOC codes	Collects age, gender, race, and ethnicity for reports; individual demographic information kept confidential	One research survey provides information on respondents' college majors	Supply of cybersecurity jobs in financial services and in government	Unknown sample size; includes job postings categorized under cybersecurity	Based on job postings categorized under cybersecurity	Reports and surveys accessible but do not provide information for the cybersecurity workforce	Reports typically annual; also provide updates on labor market trends overall and for major industries (not cybersecurity) quarterly or monthly
Payroll data	ADP	Medium: high granularity of income data but no ability to map to taxonomies	None	Collects age, gender, race, ethnicity, and location for reports; individual demographic information kept confidential	None	Information on income trajectory, work stoppages and changes, ability to work remotely, industry, and firm size	25 million individuals who work for companies using ADP payroll services; surveys include a subset of this population	Based on individuals who have job titles that fall under cybersecurity; however, access to individual-level data is restricted	Reports and earning trends by gender, industry, firm size, worker mobility, and age are accessible but do not disaggregate data for the cybersecurity workforce	Data updated continuously; ADP Hiring Insights shows data for the most recent completed month
Proprietary data tool	CyberSeek	High: has data on supply and demand in cybersecurity; reports provide comparison of the number of available cybersecurity workers relative to employer demand in a particular location	Aligned to NICE Framework	Collects information on supply of workers by region; no demographic information (e.g., age, gender, race)	Number of certificate holders by certificate, as well as the openings requesting each type of certification; most commonly held job titles based on certifications attained; cybersecurity education and training providers by program type using IPEDS data	Current job roles by type of certification held, either by metro area or state; common career pathways based on certification held and initial job	National estimate of the national cybersecurity workforce; no specific data on sample size, but listed 1.1 million employed cybersecurity workers and 755,743 open cybersecurity positions in 2022	National estimate of the cybersecurity workforce, modeled from Lightcast definitions, public job postings, and modeling based on criteria from the NICE Framework	Outputs available on website, but raw data require special request	Data reference year is the most recent 12-month period for which data are available; continuously updated; heatmap data for the 12-month period May 2023–April 2024; career pathway data for the last 12 months from current date

Subcategory	Source	Relevance	Ability to map to existing taxonomies and frameworks	Granularity of demographic data	Ability to provide information on credential attainment	Ability to provide information on employment outcomes	Coverage and sample size	Coverage of cybersecurity workforce	Accessibility	Timeliness
Survey	CompTIA	Medium: useful for salary information and job growth trends; Need to contact them to access information on certificate numbers	Aligned to NICE Framework	Collects age, race, and sexual orientation of members who take certification exams	Potential career pathways with each credential; survey of employers and skills they need in new hires	Credential needed to achieve a role, median salary, job growth trends	Participants of CompTIA certification programs and exams, employers hiring in cybersecurity; unknown sample size	Cybersecurity analysts, security engineers, pen testers, incident responders, security consultants, network security administrators, security architects, vulnerability analysts, and compliance analysts	Annual reports available; unable to find CompTIA details on credential attainment	Annual updates
Survey	CRA Taulbee Survey	Low: only focuses on PhD-granting institutions on computer science, computer engineering, or information	None	Gender, race, ethnicity, residency status, experience years (of professors only)	Degree field of PhD recipients	Employment industry of PhD recipients and salaries	Lists 314 PhD-granting departments, but only 176 responded	Computer science, computer engineering, or information PhD-granting institutions	Report free to download; data are at an aggregate level	Annual updates
Survey	ISC2	High: models entirety of cybersecurity workforce and can be more useful if we are able to obtain their raw data; otherwise, can reference annual reports to relay survey findings on skills gaps, needs, and salaries by certification	No; based on self-reported definitions of cybersecurity job, based on ISC2 membership	Collects information on geographic location of members and of chapters, age, gender, employment status, department, hiring authority, time spent on security	Number of ISC2 certifications per credential, exams delivered worldwide, number of enrollments	Employment outcomes and wages based on ISC2 certification status, estimates of global and U.S. cybersecurity workforces, workforce gaps based on federal surveys	Mix of survey responses and modeling from BLS's Quarterly Census of Employment and Wages, the Census Bureau's Statistics of U.S. Businesses, and the Census Bureau's County Business Patterns; 2023 workforce study surveyed 14,865 international practitioners (2,400 of whom identified as women) and decision-makers and modeled the national workforce based on the data from the survey	International practitioners and decision-makers survey, member survey	Static data report available on website	Workforce study conducted April–May 2023; annual report published June 2024 with data collected through 2023; salary data from the workforce study; data updated annually

Subcategory	Source	Relevance	Ability to map to existing taxonomies and frameworks	Granularity of demographic data	Ability to provide information on credential attainment	Ability to provide information on employment outcomes	Coverage and sample size	Coverage of cybersecurity workforce	Accessibility	Timeliness
Survey	SANS Institute/GIAC Certifications	Low: no relevant data except perceived challenges of the cybersecurity workforce according to managers; can also use number of certificate holders if relevant	Aligned to NICE Framework	None	Number of companies that have trained with SANS and number of GIAC alumni	Roles of employees, perceived effectiveness, hiring challenges, and experience	Human resources and cybersecurity managers; unknown sample size	Managers of companies who responded to the survey; survey asks about top five NICE cybersecurity work role categories (Investigation, Implementation and Operation, Oversight and Governance, Design and Development, Protection and Defense)	Report free to download; data are at an aggregate level	Annual update; most recent one published May 2024
Survey	WiCyS/N2K	High (if able to access N2K data): WiCyS data can be relevant for detailing the experiences of women and barriers they face in cybersecurity	Aligned to NICE Framework	Collects gender, disability status, race, identification	Provides case studies detailing number of Security+ certification holders and growth over time; partnership or subscription required to access Cyber Talent Insights feature, including Skills Diagnostics Dashboard, Benchmark and Comparisons, and other relevant reports; WiCyS "Cyber Talent Study" executive summary identifies capabilities of members and aligns them with NICE standards	Structural barriers experienced by women in cybersecurity; appears to provide workforce trends on CISOs, but we do not have access	WiCyS: member survey of women, 7,999 members; N2K: cybersecurity professionals and employers (unknown sample size)	WiCyS reports include WiCyS members—women in cybersecurity; N2K data typically collected via surveys	Executive summaries of WiCyS reports, as well as full annual report, accessible; relevant N2K reports and data require unknown fee	WiCyS report data updated annually; N2K data require subscription

BLS = Bureau of Labor Statistics; CISO = chief information security officer; CompTIA = Computing Technology Industry Association; CRA = Computing Research Association; IPEDS = Integrated Postsecondary Education Data System; ISC2 = International Information System Security Certification Consortium; IT = information technology; NASWA = National Association of State Workforce Agencies; NSF = National Science Foundation; O*NET = Occupational Information Network; SOC = Standard Occupational Classification; WiCyS = Women in CyberSecurity.

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

Notes

[1] 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 the Cybersecurity Workforce Data Initiative web page, https://ncses.nsf.gov/about/cybersecurity-workforce-data-initiative; Federal Committee on Statistical Methodology (FCSM). 2020. *A Framework for Data Quality.* FCSM-20-04. Washington, DC: Office of Management and Budget. Available at the FCSM's A Framework for Data Quality report pdf web page, https://www.fcsm.gov/assets/files/docs/FCSM.20.04_A_Framework_for_Data_Quality.pdf. Accessed 8 August 2024.

[2] U.S. Securities and Exchange Commission (SEC). 2024. *Securities Topics: Cybersecurity*. Available at the U.S. Securities and Exchange Commission's Cybersecurity web page, https://www.sec.gov/securities-topics/cybersecurity. Accessed 26 August 2024.

[3] Although CRA comprises mainly U.S. research institutions, please note that the CRA member departments also include liberal arts colleges without graduate degrees, Canadian universities, and multiple departments from larger universities (e.g., Georgia Tech has four member departments; New York University [NYU] and NYU Tandon School of Engineering are both members). For more information, see the CRA Member List on the CRA's Members List web page.

[4] Ibid.