Research Report

SASHA ROMANOSKY, KAREN SCHWINDT, RYAN JOHNSON

Comparison of Public and Private Sector Cybersecurity and IT Workforces

Section 1652 of the fiscal year (FY) 2020 National Defense Authorization Act (NDAA) tasked the U.S. Department of Defense (DoD) with performing a zero-based review (ZBR) of its cybersecurity and information technology (IT) workforces. Part of the NDAA requirements was to compare DoD cybersecurity and IT manning with comparable industry organizations and determine whether DoD organizations are under- or over-resourced relative to the private sector (Pub. L. 116-92, 2019).

At the request of the DoD Chief Information Officer (CIO), RAND Corporation's National Defense Research Institute conducted research to support the DoD ZBR effort. This previous RAND research aimed to create a transparent, repeatable process for ensuring consistent data and analysis were available for the DoD ZBR. It focused on 25 work roles within the cybersecurity and IT functional areas of the DoD Cyber Workforce Framework (DCWF),[1] which are shown in Table 1.

RAND researchers produced five unpublished reports—one each for the four DoD services (the U.S. Air Force, Army, Marine Corps, and Navy) plus one for the Defense Information Systems Agency (DISA)—as well as a capstone report (hereafter referred to as the "Capstone Report"), which documented the transparent, repeatable ZBR process and provided a high-level summary of the findings across the organizations that participated in the ZBR.[2] Also in the

KEY FINDINGS

- Overall, the public sector emphasizes the allocation of computer and information technology (IT) support and administrative roles, while the private sector emphasizes the allocation of software development and testing roles.
- Not only is the public sector hiring more IT support workers (e.g., Computer User Support Specialists) relative to the private sector, but also it is paying these workers considerably more in annual salaries.
- The Information sector shows the greatest demand for Information Security Analysts: It hires most of these workers and is willing to pay them, on average, 20 percent more than other private sector industries and 50 percent more than the public sector.

TABLE 1
DCWF Cybersecurity and IT Work Roles

Cybersecurity Work Role	IT Work Role
Cyber Defense Forensics Analyst (212)	Technical Support Specialist (411)
Systems Security Analyst (461)	Database Administrator (421)
Cyber Defense Analyst (511)	Data Analyst (422)
Cyber Defense Infrastructure Support Specialist (521)	Knowledge Manager (431)
Cyber Defense Incident Responder (531)	Network Operations Specialist (441)
Vulnerability Assessment Analyst (541)	System Administrator (451)
Authorizing Official/Designating Representative (611)	Software Developer (621)
Security Control Assessor (612)	Systems Developer (632)
Secure Software Assessor (622)	Systems Requirements Planner (641)
Information Systems Security Developer (631)	Enterprise Architect (651)
Security Architect (652)	Research and Development Specialist (661)
Information Systems Security Manager (722)	System Testing and Evaluation Specialist (671)
Communications Security (COMSEC) Manager (723)	

SOURCE: Reproduces Table 1.1 from McIntosh et al., 2022.

NOTE: DCWF work role numbers are shown in parentheses.

Capstone Report, we compared the composition (or proportion) of current staffing among cybersecurity and IT work roles between DoD organizations and the private sector. Moreover, we compared private and public sector job opening data with unfilled positions in the organizations that participated in the DoD ZBR.

The Capstone Report found that most of the DoD organizations reported a gap in personnel between 15 percent and 30 percent for most work roles (McIntosh et al., 2022, p. 21). In other words, these organizations reported not having enough cybersecurity or IT personnel to meet all of their organization's requirements. Furthermore, work role gaps were not strongly correlated with the number of civilian requirements or personnel.[3] The Capstone Report also showed that DoD organizations have approximately 2.5 times the number of personnel allocated to IT functions relative to personnel in the private sector. Yet, DoD still experiences personnel gaps for these IT functions at higher percentages than the private sector does. And the private sector experiences *higher* rates of personnel gaps for cybersecurity positions relative to gaps observed in DoD (McIntosh et al., 2022, p. x). The Capstone Report noted in its conclusion that DoD organizations are still working to align their hiring practices with the DCWF taxonomy of cybersecurity and IT positions.

While the Capstone Report provided a preliminary look at available data, the authors were limited to examining the proportion of the civilian cybersecurity and IT workforce within select DoD organizations, not in DoD or the U.S. government as a whole. Additionally, the job opening data used from Burning Glass provided a snapshot of DoD and private industry vacancies in cybersecurity and IT work roles only at the time this previous research was conducted.

In this report, we update the research summarized in the Capstone Report with current job opening data to compare the civilian cybersecurity and IT workforces with those in the U.S. government and the private sector. We also extend the DoD-private industry comparison research summarized in the Capstone Report by further examining the *proportion* of workers across a common taxonomy of cyber work roles, *salaries* paid across work roles, and *demand* for these jobs. Thus, this report both updates and expands upon the research presented in the Capstone Report.

Creating a Common Taxonomy of Cyber Work Roles

As noted in the Capstone Report, direct workforce comparisons between DoD and the private sector are difficult to make for many reasons, such as the diversity of organizations' characteristics (e.g., mission, size, maturity of the workforce, management style and structure).[4] Moreover, the lack of a common taxonomy for cybersecurity and IT work roles makes comparisons problematic. While DoD has adopted the DCWF (based on the National Initiative for Cybersecurity Education [NICE] Workforce Framework for Cybersecurity) to describe and organize its cybersecurity and IT work roles,[5] the private sector has not uniformly adopted the DCWF. Instead, federal statistical agencies classify private sector work roles using the U.S. Bureau of Labor Statistics (BLS) Standard Occupational Classification (SOC) job code taxonomy.

Creating a mapping where no common taxonomy exists can be complicated. Knapp et al. (2021) analyzes the characteristics of DoD personnel who converted to a new DoD personnel system, the Cyber Excepted Service (CES) (hereafter referred to as the "CES Report").[6] The CES Report analyzed labor demand and supply for nine cyber work roles to inform the use of compensation flexibilities to support recruitment and retention.[7] The authors matched each of the nine work roles from the CES Report to private sector occupations to compare employee characteristics and pay between civilians in these DoD cyber work roles and their private sector counterparts.[8]

To enable this comparison, the CES Report used public and private sector cyber workforce data from two publicly available datasets: the American Community Survey (ACS) and the Occupational Information Network (O*NET).[9] A text clustering algorithm was developed to map the nine DCWF work roles to potential private sector job titles using common words and phrases found in job descriptions and the associated knowledge, skills, abilities, and tasks (KSATs). The results from the algorithmic mapping were validated by subject-matter experts with a practical understanding of both DoD and private sector cyber jobs. Of the nine DCWF work roles reviewed in the CES Report, the mapping exercise yielded four matches across all taxonomies, as displayed in Table 2.

Abbreviations

ACS	American Community Survey
BLS	U.S. Bureau of Labor Statistics
CES	Cyber Excepted Service
COMSEC	communications security
DCWF	DoD Cyber Workforce Framework
DISA	Defense Information Systems Agency
DoD	U.S. Department of Defense
DoD CIO	Department of Defense, Chief Information Officer
FY	fiscal year
IT	information technology
KSAT	knowledge, skills, abilities, and tasks
NAICS	North American Industry Classification System
NDAA	National Defense Authorization Act
NICE	National Initiative for Cybersecurity Education
O*NET	Occupational Information Network
OEWS	Occupational Employment and Wage Statistics
SOC	Standard Occupational Classification
ZBR	zero-based review

Additionally, in an effort to assess the current state and future needs of the federal cybersecurity workforce, Markow and Vilvovsky (2021) leveraged

TABLE 2

CES Report Mapping Matches

DCWF Work Role	BLS Job Role
Systems Security Analyst (461)	Information Security Analyst (15-1212)
Cyber Defense Analyst (511)	Information Security Analyst (15-1212)
Software Developer (621)	Computer Programmer (15-12521) Software Developer (15-1252)
System Testing and Evaluation Specialist (671)	Software Quality Assurance Analyst and Tester (12-1253)

SOURCE: Features information from Knapp et al., 2021.

NOTE: The authors mapped DCWF work roles to their private sector counterparts. DCWF work role numbers are shown in parentheses. In the right-hand column, BLS job codes are shown in parentheses.

historical job openings for federal cybersecurity positions using Burning Glass data, as well as career history data from the Integrated Postsecondary Education Data System from the National Center for Education Statistics, to project future cybersecurity workforce needs. Markow and Vilvovsky (2021, p. 11) also mapped cybersecurity jobs openings from Burning Glass to the NICE Framework using keyword searches to crosswalk common KSATs, as well as similarities in job titles, job opening keywords, and certifications, which produced both one-to-one and one-to-many matches (i.e., one job opening to many work roles).

The Capstone Report also mapped private sector (BLS) job codes with DCWF work roles, following the method used in Knapp et al. (2021): Its authors vetted algorithmic-mapped matches by subject-matter experts who examined and compared the descriptions of each work role. In our analysis, we followed an approach similar to what was used in Markow and Vilvovsky (2021), basing our mapping on a comparison of KSATs and keyword searches to identify similarities in job titles.

The taxonomy mapping approach discussed in this report is tailored to the data used in our analysis. We began by identifying BLS job codes in the computer and IT categories, which included 12 job codes across the 11-3020, 15-000, and 17-2060 SOC categories. While these BLS job codes remained mostly the same over the period of interest, many of the job codes changed in 2018. For example, codes and descriptions for database- and software-related jobs changed and additional categories were included in some years. To address this, we reviewed and aggregated all affected computer and IT BLS job codes into two broad categories. For example, Database Administrator (15-1141 and 15-1242) and Database Administrator and Architect (15-1245) were combined into the single work role of Database Administrator and Architects. In addition, job codes relating to software development and programming (i.e., 15-1131, 15-1132, 15-1133, 15-1251, 15-1252, 15-1256) were combined into the single work role of Software Developer and Programmer.

A summary of the BLS job codes and their variations over the years is shown in Table 3.

TABLE 3

BLS Job Codes, by Work Role (2012–2021)

BLS Job Code	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Computer and Information Research Scientist										
15-1111	X	X	X	X	X	X	X			
15-1221								X	X	X
Computer and Information Systems Manager										
11-3021	X	X	X	X	X	X	X	X	X	X
Computer Network Architect										
15-1143	X	X	X	X	X	X	X			
15-1241								X	X	X
Computer Network Support Specialist										
15-1152	X	X	X	X	X	X	X			
15-1231								X	X	X
Computer Systems Analyst										
15-1121	X	X	X	X	X	X	X			
15-1211								X	X	X
Computer User Support Specialist										
15-1151	X	X	X	X	X	X	X			
15-1232								X	X	X
Data Scientist										
15-2051										X

Table 3—Continued

BLS Job Code	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Database Administrator										
15-1141	X	X	X	X	X	X	X			
15-1242										X
Database Administrator and Architect										
15-1245								X	X	
Information Security Analyst										
15-1122	X	X	X	X	X	X	X			
15-1212								X	X	X
Network and Computer Systems Administrator										
15-1142	X	X	X	X	X	X	X			
15-1244								X	X	X
Software Developer										
15-1252										X
Software Developer and Software Quality Assurance Analyst and Tester										
15-1256								X	X	
Software Developer, Applications										
15-1132	X	X	X	X	X	X	X			
Software Developer, Systems Software										
15-1133	X	X	X	X	X	X	X			
Computer Programmer										
15-1131	X	X	X	X	X	X	X			
15-1251								X	X	X

SOURCE: Features information from BLS, undated-a.

NOTE: An X indicates the presence of that job code in the given year.

Because of the variation in BLS job codes over the years analyzed, we consolidated BLS job codes into the 11 job roles listed in Table 4. This enabled us to match DCWF work roles more accurately to their corresponding BLS *role* rather than the specific *code* (i.e., SOC). Doing so also circumvented the issue of some job codes being consolidated in different years, such as Software Developer and Software Quality Assurance Analyst and Tester, which were later divided into two distinct job codes in 2021.

To develop these 11 consolidated job roles, we relied on the BLS job code descriptions for each year, which we accessed from the 2018 BLS SOC webpage (BLS, undated-a). After consolidating the BLS job codes across the years analyzed, we then mapped the 11 consolidated job roles to DCWF work roles. To conduct this mapping, we relied on subject-matter experts' reviews of BLS job codes and DCWF work roles, using keyword searches related to the work role title, key tasks, and responsibilities. A detailed summary of this process is included in the appendix. The final result was the mapping shown in Table 4. These 11 cybersecurity and IT job roles are the focus of the analysis discussed in the remainder of this report.

Data Collection and Analysis

Leveraging data and methods from the Capstone Report, we used data primarily from two sources: BLS and CyberSeek.[10]

To examine the *proportion* and *salaries* of workers across cybersecurity and IT positions, we used BLS Occupational Employment and Wage Statistics (OEWS) data between 2012 and 2021 (BLS, undated-b), which were the most recent data available at the time of this writing. For each job role, we examined the total number of employees and mean annual salary. We looked at all private sector firms and

TABLE 4

Mapping Between BLS Job Roles and DCWF Work Roles

Consolidated BLS Job Role	BLS Job Code	DCWF Work Role
Computer and Information Research Scientist	15-1111 15-1221	661
Computer and Information Systems Manager	11-3021	431 611 722 723
Computer Network Architect	15-1143 15-1241	441 651
Computer Network Support Specialist	15-1152 15-1231	521
Computer Systems Analyst	15-1121	641 671
Computer User Support Specialist	15-1151 15-1232	411
Data Scientist	15-2051	422
Database Administrator and Architect	15-1141 15-1242 15-1245	421
Information Security Analyst	15-1122 15-1212	212 461 511 531 541 612 622 631 652
Network and Computer Systems Administrator	15-1142 15-1244	451
Software Developer and Programmer	15-1131 15-1132 15-1133 15-1251 15-1252 15-1256	621 632

NOTE: The first column contains the consolidated BLS cybersecurity and IT job roles that we used in our analysis. By combining related BLS job codes, we were able to most accurately match specific DCWF work roles to their corresponding consolidated BLS job role instead of mapping DCWF work roles to BLS job codes, many of which changed year to year.

all government (i.e., local, state and federal) agencies identified in the BLS North American Industry Classification System (NAICS), where private sector firms are coded as 000001 and all government organizations are coded as 999001. We also focused in on three technology-related industry sectors: Information (NAICS code 51), Finance and Insurance (NAICS code 52), and Professional, Scientific, and Technical Services (NAICS code 54), which we have abbreviated as "Professional Services."[11]

In addition, we collected national job opening data from CyberSeek.[12] These data enable comparisons of job openings for the public and private sectors. Using these data, we identified the total number of job openings both by NICE Framework category—Analyze, Collect and Operate, Investigate, Operate and Maintain, Oversee and Govern, Protect and Defend, and Securely Provision—and by each DCWF work role (NICCS, 2022).

Proportion of Cyber Workers Across Work Roles

First, we examine the most recent year's employment data, 2021, from BLS. Unless otherwise noted, the figures in this section depict the results of our analysis of BLS OEWS data (BLS, undated-b).

The proportion of cybersecurity and IT workers across the 11 consolidated job roles is shown in Figure 1. These data show that, overall, government organizations hire proportionally *fewer* Software Developer and Programmers compared with private sector industries (12 percent versus 38 percent). On the other hand, government organizations hire proportionally *more* Computer User Support Specialists compared with private sector industries (26 percent versus 14 percent). Furthermore, government organizations hire proportionally *more* Network and Computer Systems Administrators (13 percent versus 7 percent) and, to a lesser extent, Computer Systems Analysts (16 percent versus 12 percent), which are two entry-level computer support roles that typically require fewer credentials and experience.

> Government organizations hire proportionately more . . . entry-level computer support roles that typically require fewer credentials and experience.

We further examine the variation in the proportion of worker allocation across three technology-related industry sectors, as shown in Figure 2.

We observe how, overall, these 11 cybersecurity and IT job roles have similar proportions of workers

FIGURE 1

Proportion of Cyber Workers in Government Organizations and in All Private Sector Industries, by Consolidated Job Role (2021)

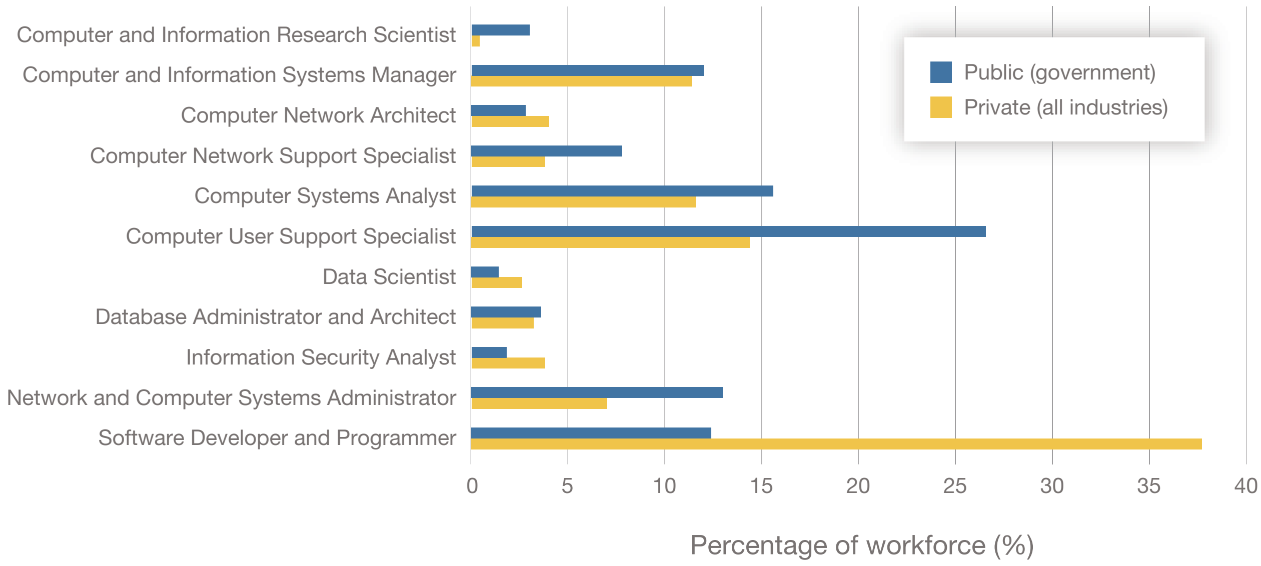
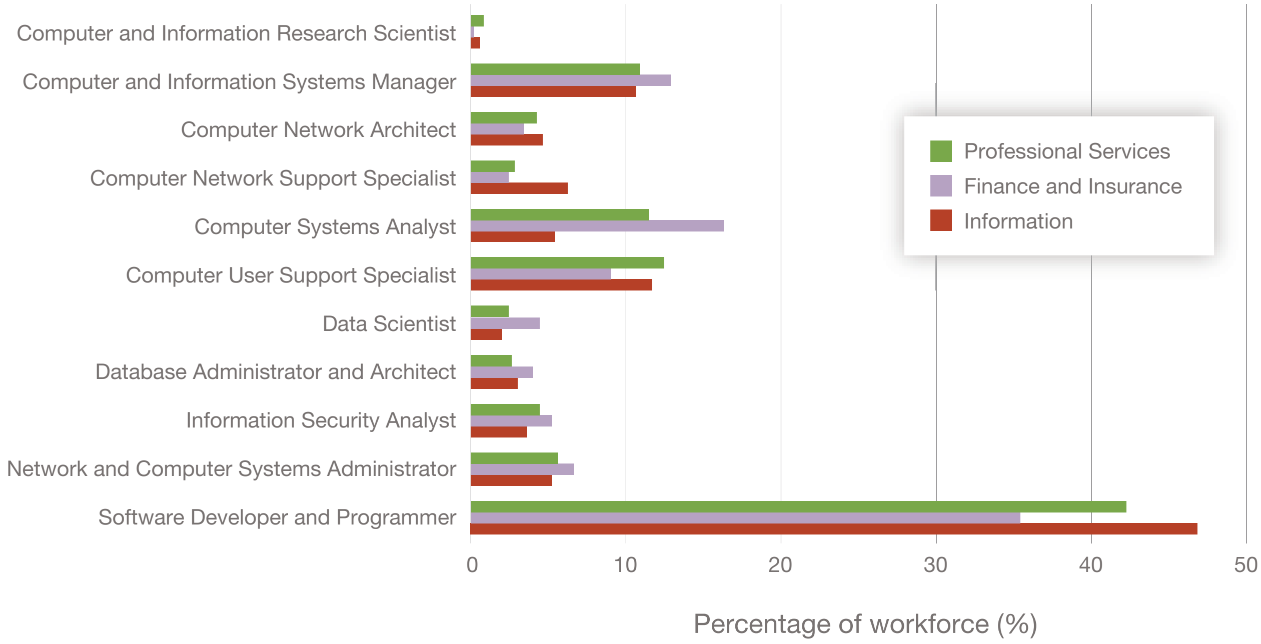


FIGURE 2

Proportion of Cyber Workers in Private Sector Industries, by Consolidated Job Role (2021)



across the three sectors. The Finance and Insurance sector shows slightly more uniformity across work roles, relative to the other sectors, while the largest differences exist with respect to the Software Developer and Programmer role: The Information sector employs 47 percent of these workers and the Finance and Insurance sector employs 35 percent of these workers.

Next, we explore how worker allocation across BLS job codes has changed from 2012 to 2021.[13] For brevity, we do not discuss each of the 11 consolidated BLS job codes but instead focus in on the more prominent findings. Results for all of the consolidated job roles are included in the appendix.

Overall, we find that government organizations hire proportionally *more* workers in entry-level cyber job roles, such as the Computer User Support Specialist (top chart) and the Network and Computer System Administrator (bottom chart) job roles, as shown in Figure 3.

Computer User Support Specialists typically compose 25 percent or more of cybersecurity and IT staff in government organizations, whereas this same group represents 15 percent or fewer of cybersecurity and IT personnel across private sector industries. Similarly, Network and Computer Systems Administrators represent 14 percent of cybersecurity and IT staff across government organizations in 2012, while this group employed between 7 percent and 10 percent of cybersecurity and IT staff in the private sector. Furthermore, employment of this group of workers has been declining steadily within the private sector to between 5 percent and 8 percent in 2021.

In addition to hiring proportionally more workers in the basic computer roles, government organizations also hire more than twice as many Computer and Information Research Scientists, and this proportion has been increasing over time, as shown in Figure 4.

One of the most prominent differences between cybersecurity and IT staff in the private sector and government organizations concerns the Software Developer and Programmer role, as shown in Figure 5. Software Developers and Programmers make up between 30 percent and 50 percent of all cybersecurity and IT staff within private sector firms but only about 15 percent of this workforce in government organizations, which has also been decreasing over the past decade.

FIGURE 3

Proportion of Computer User Support Specialists and Network and Computer System Administrators, by Sector

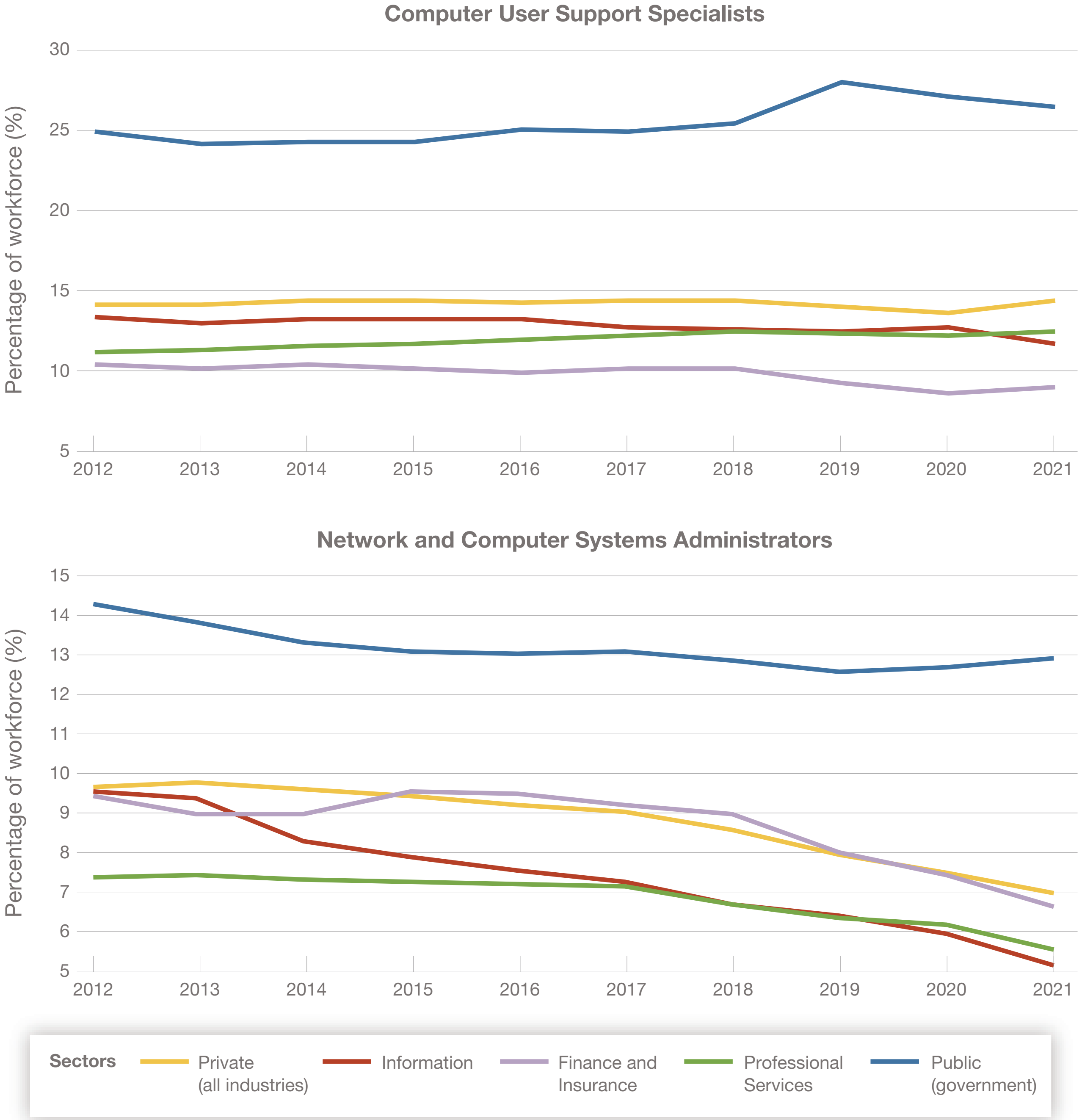


FIGURE 4

Proportion of Computer and Information Research Scientists, by Sector

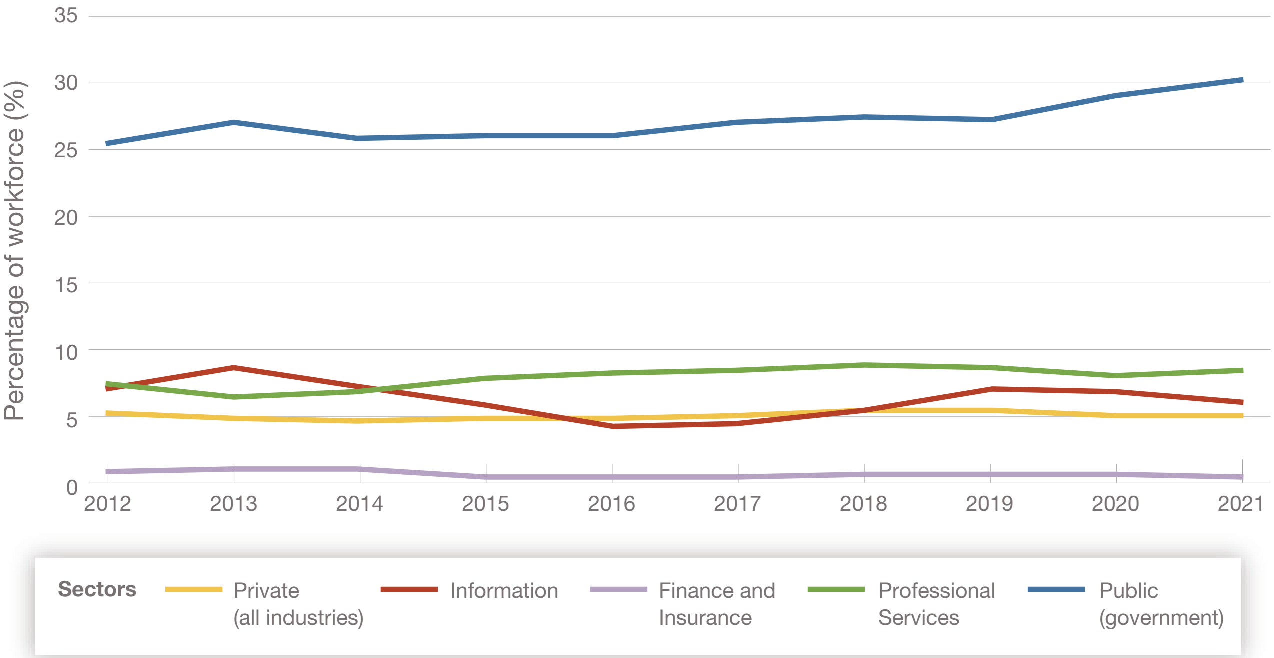
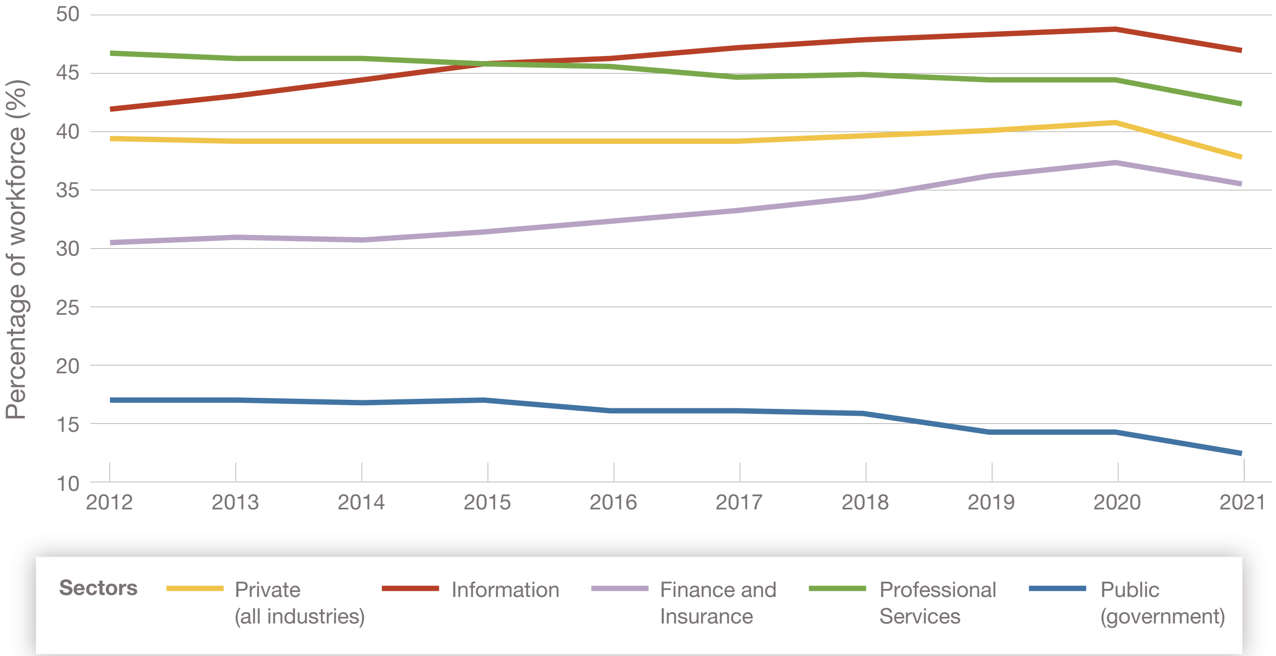


FIGURE 5

Proportion of Software Developers and Programmers, by Sector



Salaries of Cyber Workers

Next we examine the most recent year's salary data (2021). Figure 6 shows variation in salaries across the 11 consolidated job roles between the public (i.e., government) and private sectors.[14]

These data show how private sector companies typically offer salaries between 20 percent and 35 percent *higher* than public sector salaries, on average, and as high as 47 percent more for a Computer and Information Research Scientist ($109,000 on average for the public sector compared with $160,000 on average for the private sector). However, the one exception is with the Computer User Support Specialist role where mean salaries in the *government* cybersecurity and IT workforce are 6 percent higher than those paid by private sector firms ($60,000 versus $57,000, respectively).

We further examine the variation in mean salaries across three technology-related industry sectors, as shown in Figure 7.

Overall, firms in each of the Information, Finance and Insurance, and Professional Services sectors offer similar mean salaries within each work role, although the Information sector generally offers slightly higher mean salaries compared with firms in the other two sectors. One notable exception occurs with Computer and Information Research Scientists for which the Professional Services and Information sectors offer salaries exceeding $160,000 on average, while the Finance and Insurance sector offers less than $120,000, on average, for this work role.

> Private sector companies typically offer salaries between 20 percent and 35 percent higher than public sector salaries, on average, and as high as 47 percent more for a Computer and Information Research Scientist.

FIGURE 6

Mean Salaries, by Consolidated Job Role (2021)

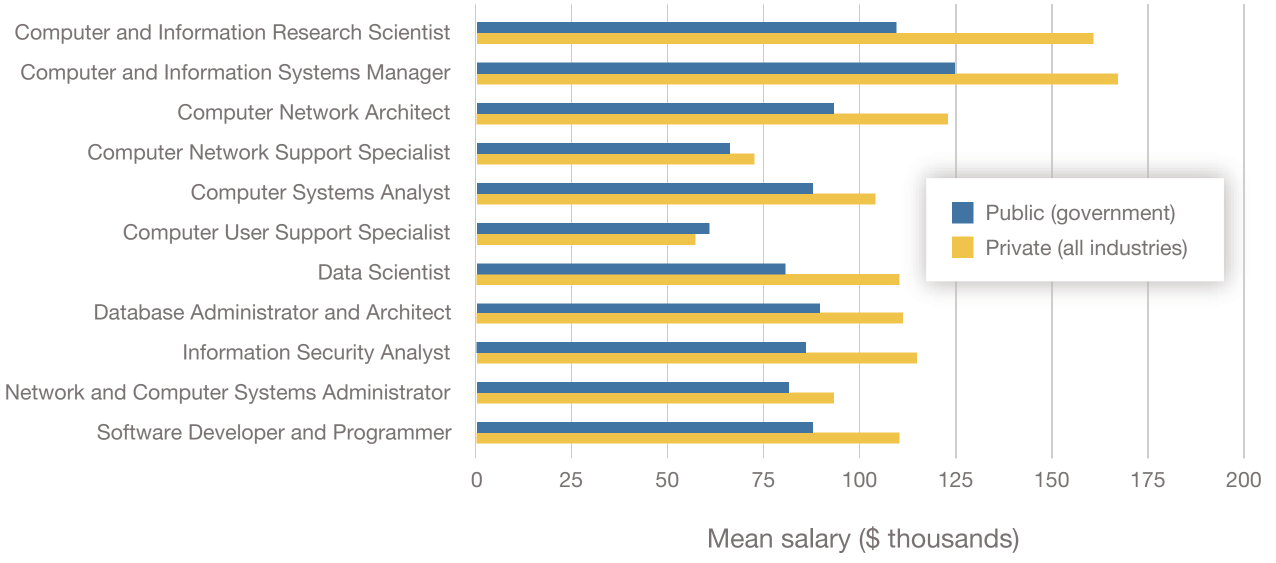
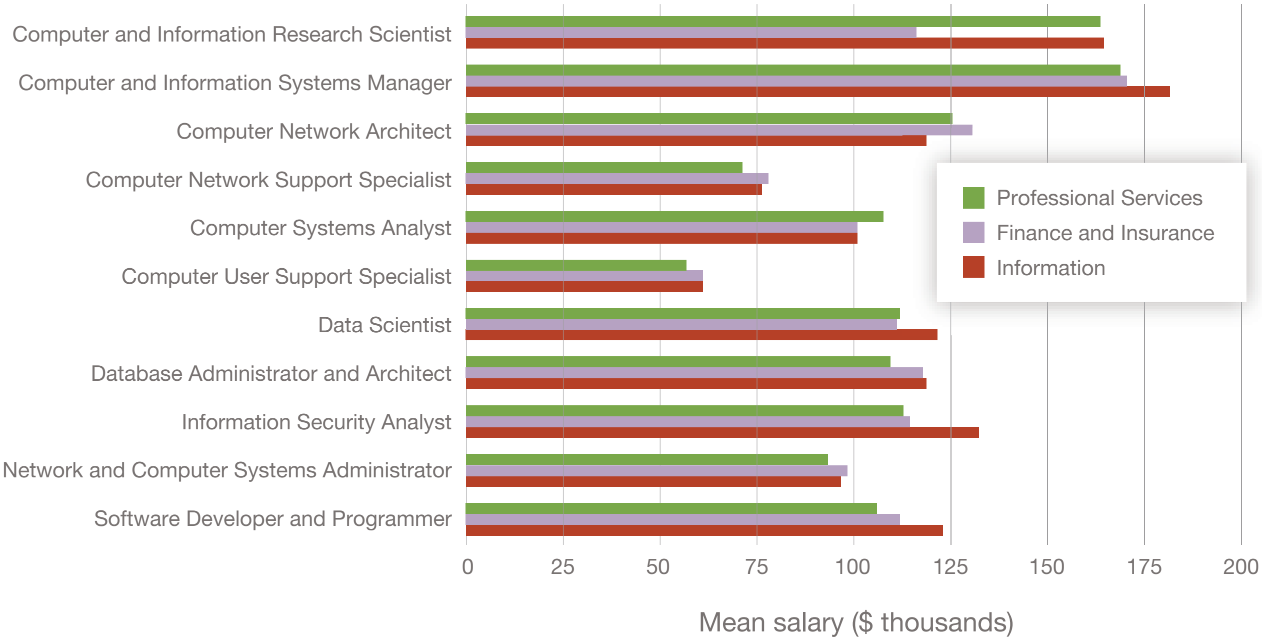


FIGURE 7

Mean Salaries, by Consolidated Job Role and Sector (2021)



Next, we examine mean salaries, adjusted for inflation, from 2012 to 2021. Figures showing results for DCWF cybersecurity and IT work roles (across all sectors and years) are available in the appendix. We only discuss the more prominent findings below.[15]

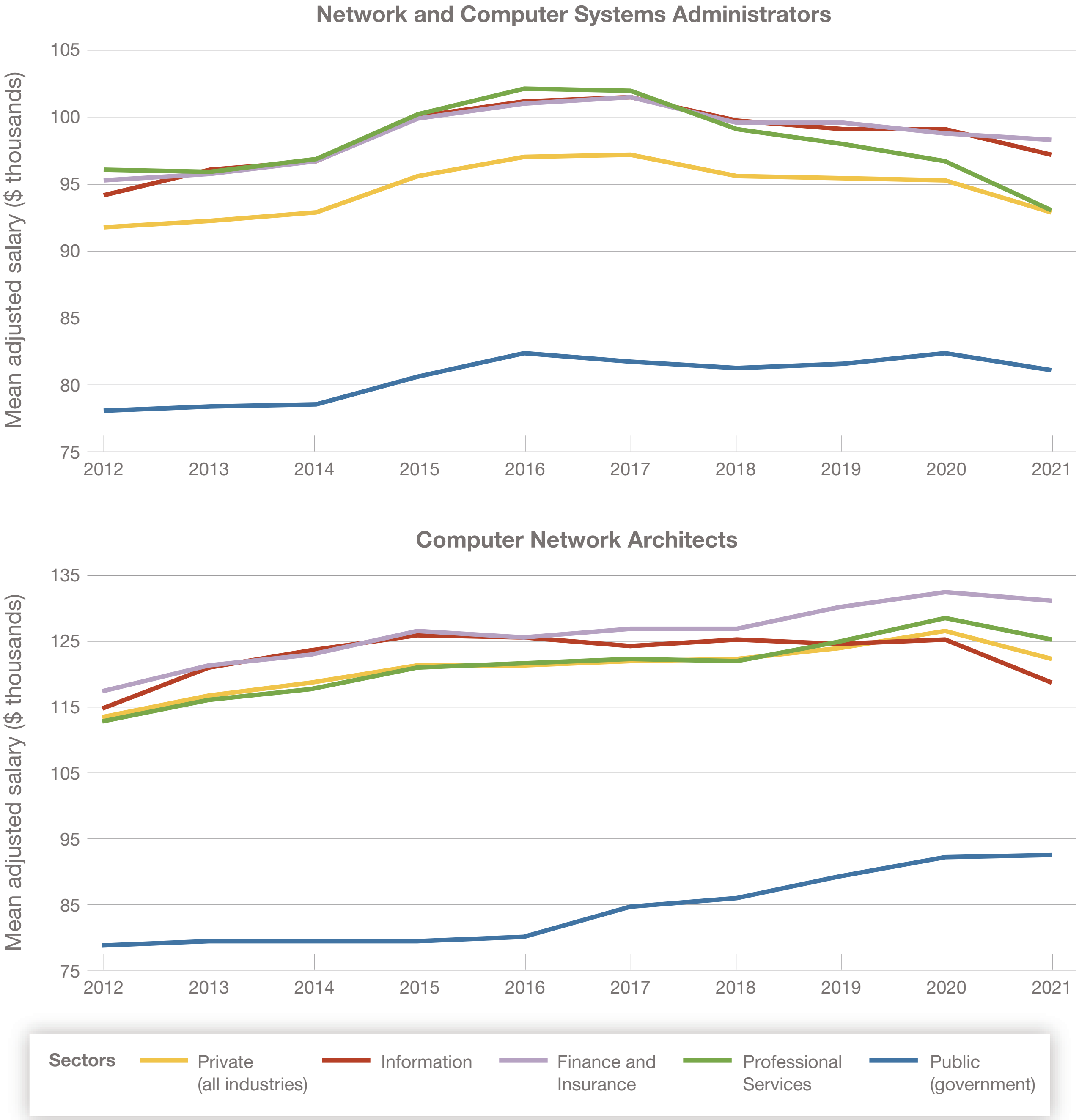
Using OEWS data, we observe how adjusted mean salaries are systematically lower for cyber workers in government organizations relative to those working in the private sector, as shown in Figure 8.[16] The top chart compares adjusted mean salaries between all private industry sectors and government organizations for Network and Computer Systems Administrators, while the bottom chart shows adjusted mean salaries for Computer Network Architects. For workers in both of these roles, for example, mean salaries in government organizations are between approximately $20,000 and $30,000 *less* than those paid by private sector companies.

That being said, *government* adjusted mean salaries for the Computer User Support Specialist job role lagged private sector adjusted mean salaries by $10,000–$15,000 annually. However, in 2018, government adjusted mean salaries increased dramatically, reaching and then surpassing private sector adjusted mean salaries in 2020, as shown in Figure 9. On the other hand, private sector adjusted mean salaries for this job role have been declining since around 2016. This dramatic increase in government mean salaries is unique among all job roles that we examined.

Adjusted mean salaries are systematically lower for cyber workers in government organizations relative to those working in the private sector.

FIGURE 8

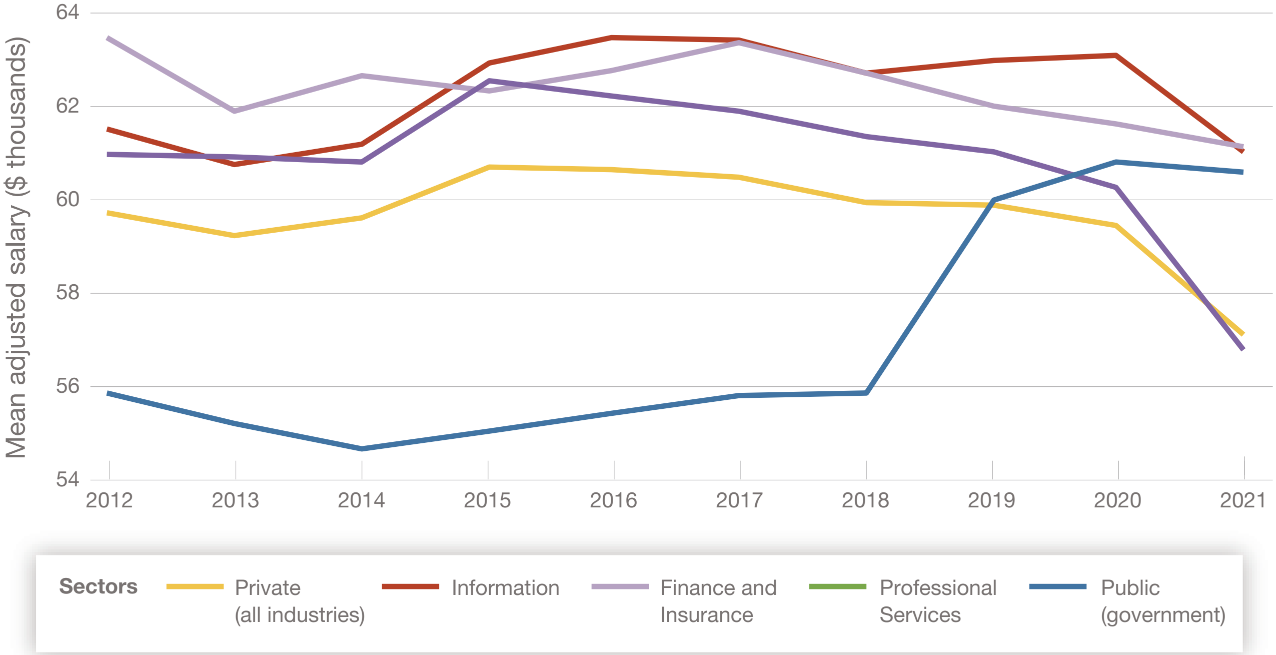
Adjusted Mean Salaries for Network and Computer Systems Administrators and Computer Network Architects, by Sector


Network and Computer Systems Administrators

Computer Network Architects

FIGURE 9

Adjusted Mean Salaries for Computer User Support Specialists, by Sector



When looking across the Finance and Insurance, Information, and Professional Services sectors, we generally see that job roles have equivalent mean salaries, with a few notable exceptions. For example, Figure 10 shows mean salaries for the Software Developer and Programmer (top chart) and the Information Security Analyst (bottom chart) job roles. In 2012, mean salaries for Software Developers and Programmers were similar across these private industry sectors. However, starting in 2018, mean salaries for this job role in the Information sector increased from about $117,000 to almost $125,000 by 2021, whereas mean salaries for this job role in the other private industry sectors *decreased* from about $115,000 in 2018 to $110,000 in 2021.

Moreover, mean salaries for the Information Security Analyst job role were generally equivalent across the private industry sectors until mean salaries for this job role in the Information sector increased dramatically in 2019, climbing from less than $110,000 to $130,000 by 2021.

Demand for Cyber Workers

Next, we explore demand for cyber workers as captured in job opening data collected by CyberSeek. This online tool allows users to filter cybersecurity supply and demand data by public and private sectors. The tables and figures in this section depict the results of our analysis using CyberSeek supply/demand heat map data (CyberSeek, undated-b).

We categorized the total estimated number of both public and private sector workers employed in cybersecurity and IT-related jobs, as well as the number of public and private sector cybersecurity and IT job openings, according to the categories outlined in the NICE Framework, which we mapped to the 11 consolidated BLS job roles. Cybersecurity and IT job openings for each of the 11 consolidated BLS job roles in both the private and public sectors are shown in Table 5 and Figure 11.

According to these data, both private and public sectors are seeking to fill cybersecurity and IT positions at proportionally similar amounts. The great-

FIGURE 10

Adjusted Mean Salaries for Software Developers and Programmers and Information Security Analysts, by Sector

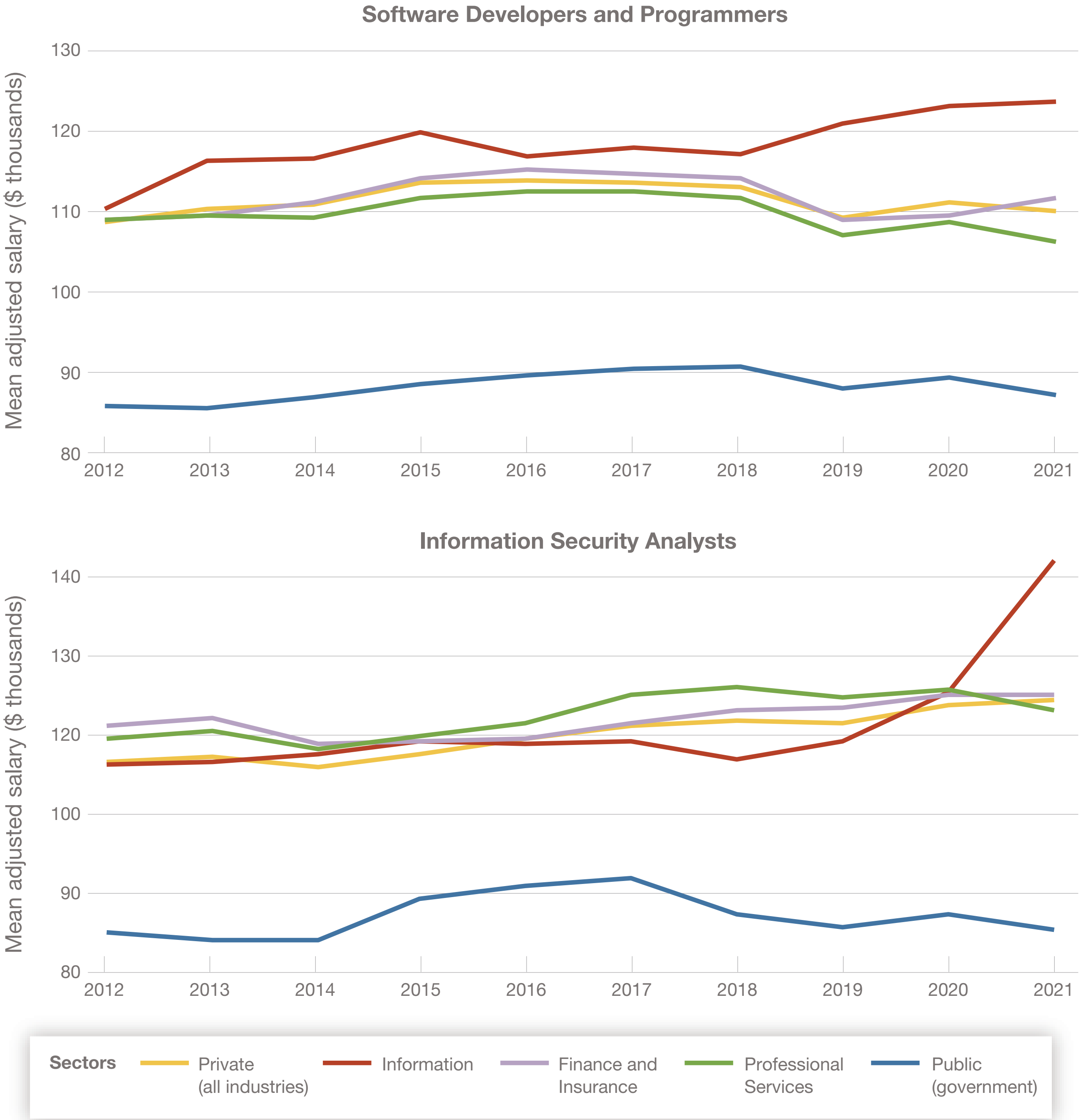


TABLE 5

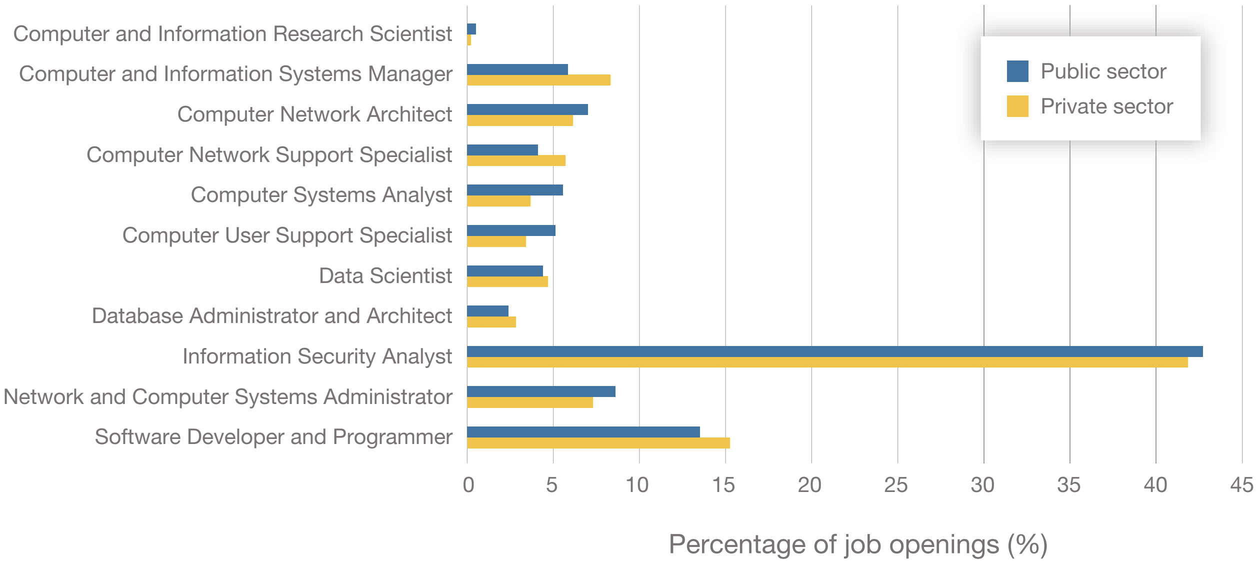
Private and Public Sector Cybersecurity and IT Job Openings, by Consolidated Job Role

	Number of Job Openings		Percentage of Job Openings		
Consolidated BLS Job Role	Private Sector	Public Sector	Private Sector	Public Sector	Difference
Computer and Information Research Scientist	3,384	672	0.2%	0.5%	–0.3%
Computer and Information Systems Manager	161,922	7,432	8.4%	5.9%	2.5%
Computer Network Architect	120,441	8,849	6.2%	7.1%	–0.9%
Computer Network Support Specialist	110,936	5,166	5.8%	4.1%	1.7%
Computer Systems Analyst	72,326	7,031	3.7%	5.6%	–1.9%
Computer User Support Specialist	66,949	6,405	3.5%	5.1%	–1.6%
Data Scientist	91,403	5,539	4.7%	4.4%	0.3%
Database Administrator and Architect	53,578	2,959	2.8%	2.4%	0.4%
Information Security Analyst	806,875	53,449	41.8%	42.7%	–0.9%
Network and Computer Systems Administrator	142,710	10,913	7.4%	8.7%	–1.3%
Software Developer and Programmer	294,871	17,037	15.3%	13.6%	1.7%
Total	**1,925,395**	**125,452**	**99.8%**	**100.1%**	

NOTE: Percentage totals do not sum to 100 because of rounding.

FIGURE 11

Proportion of Private and Public Sector Cybersecurity and IT Job Openings, by Consolidated Job Role



est portion of job openings for both sectors is for the Information Security Analyst job role (just over 40 percent of job openings), followed by the Software Developer and Programmer job role (approximately 15 percent of job openings).

Furthermore, these data show that the public sector is looking to hire proportionally more people with basic technical IT skills—i.e., Network and Computer Systems Administrators, Computer User Support Specialists, and Computer Systems Analysts—than the private sector. This finding is consistent with results shown in Figures 1 and 3: That is, the proportion of workers in the Computer User Support Specialist and the Network and Computer System Administrator job roles is greater in government organizations compared with all other sectors. Additionally, Figure 3 highlights that while the proportion of workers in the Network and Computer Systems Administrator job role has decreased slightly in all other sectors, the proportion has remained relatively stable in the public (government) sector, decreasing only a small amount over the same period.

In addition, these data show there is greater demand (as reflected by job openings) for the Software Developer and Programmer job role in the private sector than in the public sector, which is consistent with the results shown in Figure 1, where the proportion of Software Developers and Programmers is higher in all other sectors compared with the proportion of these workers in government organizations.

Findings and Limitations

Comparing DoD cybersecurity and IT positions with comparable positions in the private sector is a challenging task. In this report, we examine additional data to help create a clearer picture of the DoD cybersecurity and IT workforce as it evaluates and addresses its supply and demand gaps.

Overall, we find that the public sector emphasizes what might be considered support and administrative roles (e.g., Network and Computer Systems Administrator, Computer User Support Specialist, and Computer Network Support Specialist), while the private sector emphasizes software development and testing roles (Computer Systems Analyst and Software Developer and Programmer).[17] Indeed, this finding is also supported by job opening data that shows the public sector is looking for relatively more workers in entry-level IT positions (e.g., Network and Computer Systems Administrator, Computer Systems Analyst, and Computer User Support Specialist), while the private sector is looking for more Software Developers and Programmers, Computer and Information Systems Managers, and Computer Network Support Specialists.

Furthermore, among all job roles, the Computer User Support Specialist and Information Security Analyst job roles stand out in two unique ways. First, despite the proportion of workers holding steady across sectors (and the public sector supporting almost twice as many of these workers as the private sector), the public sector has increased average annual salaries of Computer User Support Specialists by about 20 percent since 2018, at the same time as salaries for these same workers in private sector firms have been decreasing. The implication seems to be that the public sector sees more value in these employees, relative to the public sector, and is willing to pay them more to maintain this workforce.

Secondly, the Information sector seems to find more value in Information Security Analysts relative to other private sector industries and the public sector. The data we analyzed show that the Information sector seeks to hire more Information Security Analysts and is willing to pay them, on average, 20 percent more than other private sector industries and 50 percent more than the public sector.

Limitations

In regard to limitations of this research, we acknowledge that the mapping between private and public sectors, as manifested through BLS SOC and the DCWF and NICE Framework work roles, is imperfect. However, we trust that our methodology is sufficiently transparent for readers to understand the decisions and assumptions that we made.

As demand for cyber talent continues to increase and the diversity and specialization of work roles create more jobs, both public and private sectors would benefit from the use of a common taxonomy.

In addition, because both private and public sectors contract out some cybersecurity and IT functions to third parties, job openings data may undercount the total number of gapped positions and disproportionately undercount gapped positions across job roles or sectors. In addition, a job title included in the CyberSeek job opening data could represent multiple work roles within the DCWF, which may also affect our count data. That is, a single job opening may cover multiple DCWF work roles and therefore may show up as two or more datapoints in the CyberSeek data.

Furthermore, the demand for cybersecurity and IT roles may vary disproportionately across public and private sectors. And so while comparing public and private sector workforce data is useful for analysis, large differences between these groups may be a function of mission requirements or other group characteristics rather than hiring difficulties. On the other hand, if the public and private sectors do have comparable demand for a given position but only the private sector is hiring for this position (or hiring at a significantly greater rate), then this could create a challenge for the public sector to address.

Recommendation

Our findings are consistent with past RAND research highlighting the challenges in comparing DoD and private sector cybersecurity and IT workforces because of different cyber personnel taxonomies (e.g., McIntosh et al., 2022).

Specifically, we found that multiple private sector positions mapped to a single DCWF work role, and vice versa, which created confusion and ambiguity of the true nature of the work being performed. This made a strict one-to-one comparison infeasible, requiring consolidation among cyber workforce taxonomies (e.g., BLS SOC and the DCWF).

That aside, our comparisons show that there are significant differences between U.S. government and private sector classification and organization of cybersecurity and IT positions. Furthermore, there are noticeable variations across job roles in salary, staffing across roles, and changes in staffing proportions. As demand for cyber talent continues to increase and the diversity and specialization of work roles create more jobs, both public and private sectors would benefit from the use of a common taxonomy.

To remedy this, we recommend that DoD engage BLS to encourage the adoption of the DCWF as the industry standard taxonomy used for classifying cybersecurity and IT work roles. Although not all DCWF work roles are applicable to the private sector (e.g., private sector cyber workforce personnel will not perform all source analysis or exploitation analysis), the DCWF provides a more complete partitioning of cyber-related work responsibilities and will aid in future private-public sector comparisons. Furthermore, adopting a uniform framework and methodology of classifying work roles will enable greater transparency and allow the federal government to assist with workforce planning and identify talent gaps more accurately.

Adopting the DCWF approach also allows for modularity and scalability as the industry evolves over time. As seen from 2012 to 2021, numerous BLS job codes had evolved: Some were consolidated and others split up into new codes. One benefit of the DCWF is instead of purely relying on the work performed and the skills, education, and training needed to perform the work, work roles are hierarchically structured with seven broad categories, 33 specialty areas, and 54 work roles (DoD CIO, undated). This structure would allow future cyber and IT jobs to be nested in the current structure without requiring a complete overhaul of classifications.

Appendix

DCWF Work Roles

Table A.1 provides descriptions for all the DCWF cybersecurity and IT work roles.

TABLE A.1

DCWF Work Role Descriptions, by NICE Framework Category

DCWF Work Role	Description
Investigate	Investigates cybersecurity events or crimes related to IT systems, networks, and digital evidence.
Cyber Defense Forensics Analyst (212)	Investigates cybersecurity events or crimes related IT systems, networks, and digital evidence.
Operate and Maintain	Provides the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security.
Technical Support Specialist (411)	Provides technical support to customers who need assistance using client-level hardware and software in accordance with established or approved organizational process components.
Database Administrator (421)	Administers databases and data management systems that allow for the storage, query, and utilization of data.
Data Analyst (422)	Examines data from multiple disparate sources with the goal of providing new insight. Designs and implements custom algorithms, flow processes, and layouts for complex, enterprise-scale datasets used for modeling, data mining, and research purposes.
Knowledge Manager (431)	Responsible for the management and administration of processes and tools that enable the organization to identify, document, and access intellectual capital and information content.
Network Operations Specialist (441)	Plans, implements, and operates network services/systems, including hardware and virtual environments.
Systems Administrator (451)	Installs, configures, troubleshoots, and maintains hardware and software, and administers system accounts.
Systems Security Analyst (461)	Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.
Protect and Defend	Identifies, analyzes, and mitigates threats to internal IT systems and networks.
Cyber Defense Analyst (511)	Uses data collected from a variety of cyber defense tools (e.g., IDS [Intrusion Detection System] alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.
Cyber Defense Infrastructure Support Specialist (521)	Tests, implements, deploys, maintains, and administers infrastructure hardware and software.
Cyber Defense Incident Responder (531)	Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.
Vulnerability Assessment Analyst (541)	Performs assessments of systems and networks within the network environment or enclave and identifies where those systems or networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.
Authorizing Official/ Designating Representative (611)	Acts as a senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation (CNSSI 4009, 2022).
Security Control Assessor (612)	Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an IT system to determine the overall effectiveness of the controls (as defined in NIST, 2018).

Table A.1—Continued

DCWF Work Role	Description
Software Developer (621)	Develops, creates, maintains, and writes or codes new (or modifies existing) computer applications, software, or specialized utility programs.
Secure Software Assessor (622)	Analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results.
Information Systems Security Developer (631)	Designs, develops, tests, and evaluates information system security throughout the systems development life cycle.
Systems Developer (632)	Designs, develops, tests, and evaluates information systems throughout the systems development life cycle.
Systems Requirement Planner (641)	Consults with customers to evaluate functional requirements and translate functional requirements into technical solutions.
Enterprise Architect (651)	Develops and maintains business, systems, and information processes to support enterprise mission needs; develops IT rules and requirements that describe baseline and target architectures.
Security Architect (652)	Designs enterprise and systems security throughout the development life cycle; translates technology and environmental conditions (e.g., law and regulation) into security designs and processes.
Research and Development Specialist (661)	Conducts software and systems engineering and software systems research to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.
Systems Testing and Evaluation Specialist (671)	Plans, prepares, and executes tests of systems to evaluate results against specifications and requirements, as well as analyzes and reports test results.
Information Systems Security Manager (722)	Responsible for the cybersecurity of a program, organization, system, or enclave.
COMSEC Manager (723)	Manages the COMSEC resources of an organization (CNSSI 4009, 2022).

SOURCE: Adapted from DoD CIO, undated.

Mapping the DCWF Work Roles to BLS Job Roles

After consolidating BLS job codes into the 11 distinct job roles listed in Table 4, we matched corresponding DCWF work roles with similar responsibilities using a one-to-many relationship. That is, one BLS job code can be associated with many DCWF work roles. No DCWF work roles were matched to multiple BLS job codes. For readers' convenience, we reproduce that mapping information here as Table A.2.

For example, the BLS job description for the Computer and Information Systems Manager job role is to "plan, direct, or coordinate activities in such fields as electronic data processing, information systems, systems analysis, and computer programming" (BLS, 2022). Using this description, we matched this BLS job role with the following DCWF work roles: Knowledge Manager (431), Authorizing Official/Designating Representative (611), Information Systems Security Manager (722), and COMSEC Manager (723). Tables A.3–A.13 provide the descriptions of DCWF work roles that correspond to the BLS consolidated job roles, with justifications for their mapping in bold type, based on our analysis of the DCWF (DoD CIO, undated).

TABLE A.2

Mapping Between BLS Job Roles and DCWF Work Roles

Consolidated BLS Job Role	BLS Job Code	DCWF Work Role
Computer and Information Research Scientist	15-1111 15-1221	661
Computer and Information Systems Manager	11-3021	431 611 722 723
Computer Network Architect	15-1143 15-1241	441 651
Computer Network Support Specialist	15-1152 15-1231	521
Computer Systems Analyst	15-1121	641 671
Computer User Support Specialist	15-1151 15-1232	411
Data Scientist	15-2051	422
Database Administrator and Architect	15-1141 15-1242 15-1245	421
Information Security Analyst	15-1122 15-1212	212 461 511 531 541 612 622 631 652
Network and Computer Systems Administrator	15-1142 15-1244	451
Software Developer and Programmer	15-1131 15-1132 15-1133 15-1251 15-1252 15-1256	621 632

NOTE: The first column contains the consolidated BLS cybersecurity and IT job roles that we used in our analysis. By combining related BLS job codes, we were able to most accurately match specific DCWF work roles to their corresponding consolidated BLS job role instead of mapping DCWF work roles to BLS job codes, many of which changed year to year.

TABLE A.3

DCWF Match for Computer and Information Research Scientist

DCWF Work Role	DCWF Description
Research and Development Specialist (661)	Conducts **software** and systems engineering and **software systems** research in order to develop **new capabilities**, ensuring cybersecurity is fully integrated. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.

TABLE A.4

DCWF Matches for Computer and Information Systems Manager

DCWF Work Role	DCWF Description
Knowledge Manager (431)	Responsible for the **management** and administration of **processes and tools** that enable the organization to identify, document, and access intellectual capital and information content.
Authorizing Official/ Designating Representative (611)	Acts as senior official or executive with the authority to formally assume **responsibility** for operating an **information system** at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation (CNSSI 4009, 2022).
Information Systems Security Manager (722)	Analyzes the security of new or existing computer applications, software, or specialized utility programs and **provides actionable results**.
COMSEC Manager (723)	**Manages** the COMSEC resources of an organization (CNSSI 4009, 2022).

TABLE A.5

DCWF Matches for Computer Network Architect

DCWF Work Role	DCWF Description
Network Operations Specialist (441)	Plans, implements, and operates **network** services and systems, including hardware and virtual environments.
Enterprise Architect (651)	**Develops** and maintains business, systems, and **information processes** to support enterprise mission needs; develops IT rules and requirements that describe baseline and target architectures.

TABLE A.6

DCWF Match for Computer Network Support Specialist

DCWF Work Role	DCWF Description
Cyber Defense Infrastructure Support Specialist (521)	Tests, implements, deploys, maintains, and administers the **infrastructure hardware** and software.

TABLE A.7

DCWF Matches for Computer Systems Analyst

DCWF Work Role	DCWF Description
Systems Requirements Planner (641)	Consults with customers to **evaluate functional requirements** and translate functional requirements into technical solutions.
System Testing and Evaluation Specialist (671)	Plans, prepares, and executes **tests of systems** to evaluate results against specifications and requirements, as well as analyzes and reports test results.

TABLE A.8

DCWF Match for Computer User Support Specialist

DCWF Work Role	DCWF Description
Network Operations Specialist (411)	Plans, implements, and operates **network services and systems**, including hardware and virtual environments.

TABLE A.9

DCWF Match for Data Scientist

DCWF Work Role	DCWF Description
Data Analyst (422)	Examines **data** from multiple disparate sources with the goal of providing **new insight**. Designs and implements custom algorithms, flow processes, and layouts for complex, enterprise-scale datasets used for modeling, data mining, and research purposes.

TABLE A.10

DCWF Match for Database Administrator and Architect

DCWF Work Role	DCWF Description
Database Administrator (421)	Administers **databases** and/or **data management systems** that allow for the storage, query, and utilization of data.

TABLE A.11

DCWF Matches for Information Security Analyst

DCWF Work Role	DCWF Description
Cyber Defense Forensics Analyst (212)	Analyzes **digital evidence** and investigates computer **security** incidents to derive useful information in support of system and network vulnerability mitigation.
Systems Security Analyst (461)	Responsible for the analysis and development of the integration, testing, operations, and maintenance of **systems security**.
Cyber Defense Analyst (511)	Uses data collected from a variety of **cyber defense tools** (e.g., IDS [Intrusion Detection System] alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of **mitigating threats**.
Cyber Defense Incident Responder (531)	Investigates, analyzes, and responds to **cyber incidents** within the network environment or enclave.
Vulnerability Assessment Analyst (541)	Performs assessments of systems and networks within the network environment or enclave and identifies where those systems and networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of **defense-in-depth architecture** against known vulnerabilities.
Security Control Assessor (612)	Conducts independent **comprehensive assessments** of the management, operational, and technical security controls and control enhancements employed within or inherited by an IT system to determine the overall effectiveness of the controls (as defined in NIST, 2018).
Secure Software Assessor (622)	Analyzes the **security** of new or existing computer applications, software, or specialized utility programs and provides actionable results.
Information Systems Security Developer (631)	Designs, develops, tests, and evaluates **information system security** throughout the systems development life cycle.
Security Architect (652)	Designs **enterprise** and **systems security** throughout the development life cycle; translates technology and environmental conditions (e.g., law and regulation) into security designs and processes.

TABLE A.12

DCWF Match for Network and Computer Systems Administrator

DCWF Work Role	DCWF Description
System Administrator (451)	Installs, configures, troubleshoots, and maintains hardware, software, and **administers** system accounts.

TABLE A.13

DCWF Matches for Software Developer

DCWF Work Role	DCWF Description
Software Developer (621)	Develops, creates, maintains, and **writes or codes new** (or modifies existing) computer applications, **software**, or specialized utility programs.
Systems Developer (632)	Designs, develops, tests, and evaluates **information systems** throughout the systems development life cycle.

Proportion of Workers, by Consolidated Job Role and Sector

Figure A.1 shows the proportion of cybersecurity and IT workers for each BLS consolidated job role, between 2012 and 2021, for government organizations and all private sector companies, as well as three technology-related industry sectors. We do not include a figure for Data Analysts because this role was newly introduced in 2021 and no trend data exist.

Adjusted Mean Salaries of All Consolidated Job Roles

Figure A.2 shows the inflation-adjusted mean salaries for cyber and IT workers across all consolidated job roles, between 2012 and 2021, for government organizations, all private sector companies, and the three technology-related industry sectors. We do not include a figure for the Data Analyst job role because it was only introduced in 2021 and no trend data exist.

FIGURE A.1

Proportion of Workers, by Consolidated Job Role and Sector

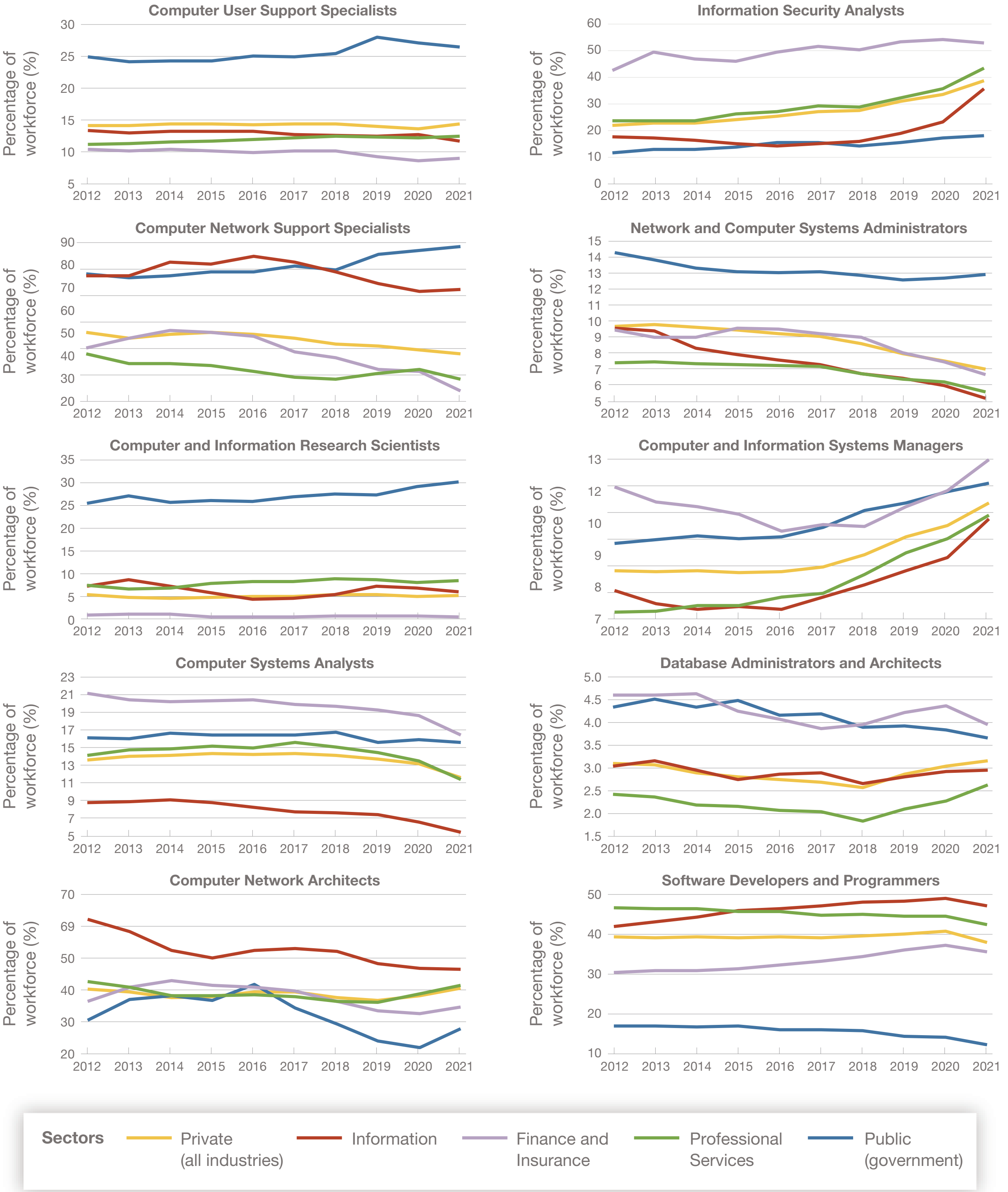
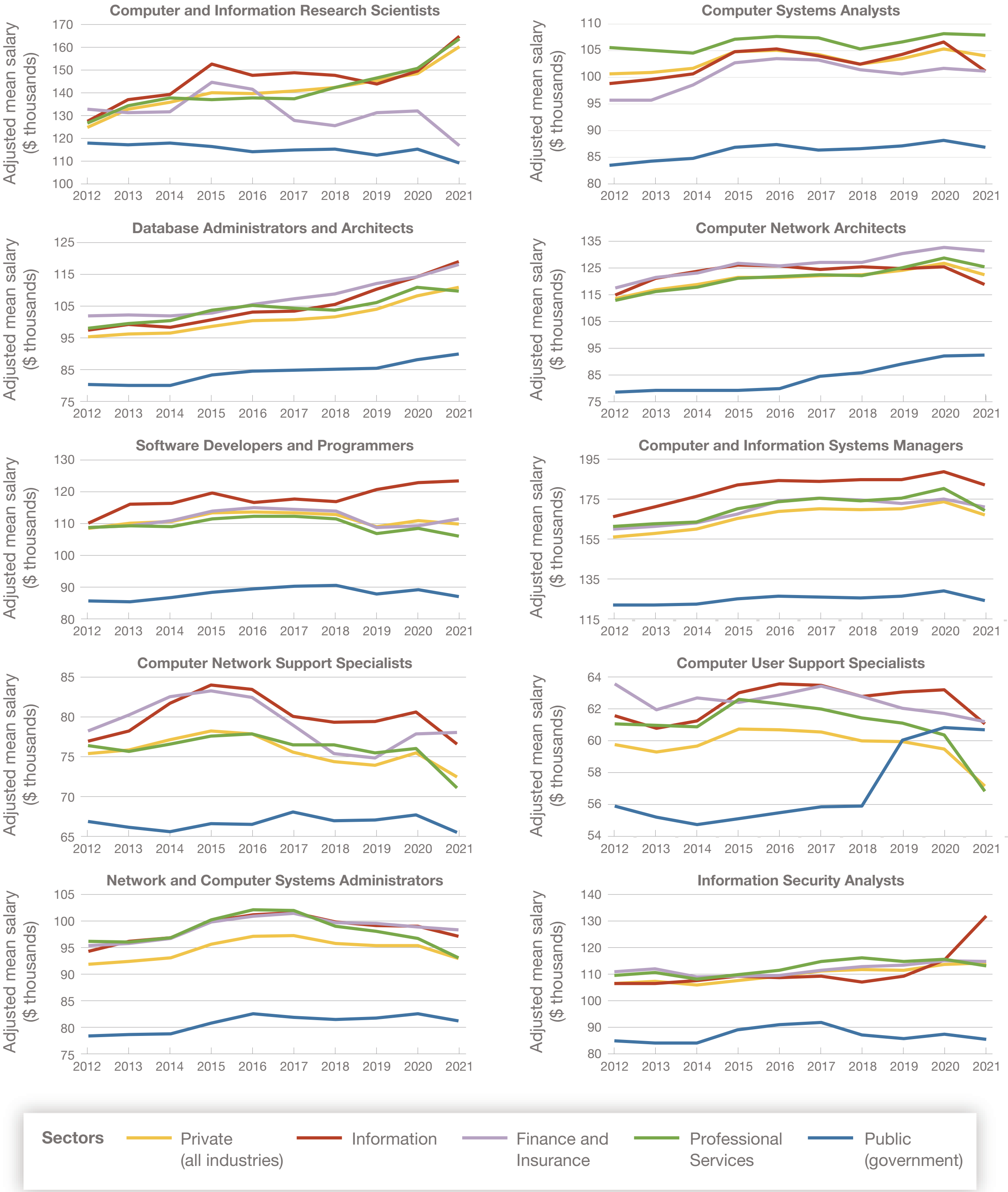


FIGURE A.2

Adjusted Mean Salaries, by Consolidated Job Role and Sector



Employee Counts for All Consolidated Job Roles

For reference, Table A.14 shows the number of employees, by sector, for 2021.

CyberSeek Job Opening Data for DCWF Cybersecurity and IT Work Roles

For completeness, Table A.15 provides job opening data for each DCWF cybersecurity and IT work role.

TABLE A.14

BLS Count of Employees, by Sector (2021)

Consolidated Job Role	Private Sector (All Industries)	Information Sector	Finance and Insurance Sector	Professional Services Sector	Public Sector (Government)
Computer Network Architect	158,860	28,260	14,810	64,830	9,970
Computer Network Support Specialist	148,430	38,030	10,160	44,640	27,770
Computer Systems Analyst	450,030	32,680	69,760	177,830	55,130
Computer User Support Specialist	560,840	70,810	38,180	195,220	93,470
Computer and Information Research Scientist	20,170	3,680	210	13,150	10,670
Computer and Information Systems Manager	442,480	65,300	55,240	169,870	42,710
Data Scientist	101,170	12,130	18,850	37,160	4,810
Database Administrator and Architect	123,360	17,860	16,930	41,200	12,950
Information Security Analyst	150,810	21,620	22,420	67,500	6,410
Network and Computer Systems Administrator	271,170	31,180	28,190	86,570	45,590
Software Developer and Programmer	1,473,070	285,010	151,150	660,770	43,720

SOURCE: Features information from BLS, undated-b.

NOTE: The second column represents private sector firms (coded as 000001 by BLS) and the sixth column represents all government organizations (coded as 999001 by BLS). Columns two through five report on three technology-related industry sectors: Information (NAICS code 51), Finance and Insurance (NAICS code 52), and Professional, Scientific, and Technical Services (NAICS code 54), which we abbreviate as “Professional Services.”

TABLE A.15

CyberSeek Job Opening Data for DCWF Cybersecurity and IT Work Roles

	Number of Job Openings		Percentage of All Job Openings	
DCWF Work Role	Private Sector	Public Sector	Private Sector	Public Sector
Cybersecurity				
Cyber Defense Forensics Analyst (212)	27,681	4,838	1.4%	3.9%
Systems Security Analyst (461)	206,207	14,896	10.7%	11.9%
Cyber Defense Analyst (511)	50,193	2,296	2.6%	1.8%
Cyber Defense Infrastructure Support Specialist (521)	110,936	5,166	5.8%	4.1%
Cyber Defense Incident Responder (531)	75,935	4,208	3.9%	3.4%
Vulnerability Assessment Analyst (541)	120,268	8,154	6.2%	6.5%
Authorizing Official/Designating Representative (611)	33,123	1,331	1.7%	1.1%
Security Control Assessor (612)	109,296	5,153	5.7%	4.1%
Secure Software Assessor (622)	38,603	4,021	2.0%	3.2%
Information Systems Security Developer (631)	61,738	3,978	3.2%	3.2%
Security Architect (652)	116,954	5,905	6.1%	4.7%
Information Systems Security Manager (722)	55,835	2,181	2.9%	1.7%
COMSEC Manager (723)	2,201	472	0.1%	0.4%
IT				
Technical Support Specialist (411)	66,949	6,405	3.5%	5.1%
Database Administrator (421)	53,578	2,959	2.8%	2.4%
Data Analyst (422)	91,403	5,539	4.7%	4.4%
Knowledge Manager (431)	70,833	3,448	3.7%	2.7%
Network Operations Specialist (441)	112,583	8,734	5.8%	7.0%
System Administrator (451)	142,710	10,913	7.4%	8.7%
Software Developer (621)	175,094	9,155	9.1%	7.3%
Systems Developer (632)	119,777	7,882	6.2%	6.3%
Systems Requirements Planner (641)	43,015	4,479	2.2%	3.6%
Enterprise Architect (651)	7,858	155	0.4%	0.1%
Research and Development Specialist (661)	3,384	672	0.2%	0.5%
System Testing and Evaluation Specialist (671)	29,311	2,552	1.5%	2.0%
Total	**1,925,465**	**125,492**	**99.8%**	**100.1%**

SOURCE: Features information from CyberSeek, undated-b.
NOTE: Percentages do not total to 100 because of rounding.

Notes

[1] The DCWF is the DoD cyber taxonomy based on the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework and DoD Joint Cyberspace Training and Certification Standards.

[2] The five unpublished reports outlined organization-specific findings that could be used to support individual ZBR submissions. The Capstone Report aggregates the results and findings of these five reports (McIntosh et al., 2022).

[3] The Capstone Report separated civilian data from active-duty military data. Results from the military cybersecurity work role gap analysis showed that there were fewer military cybersecurity personnel and requirements compared with their civilian counterparts partly because of limited data from some organizations. Interestingly, even these small differences between personnel and requirements still produced large gaps in military cybersecurity and IT manning (McIntosh et al., 2022, p. 21).

[4] Although a variety of industry sectors have cybersecurity and IT personnel, in this report, we focus on comparing cybersecurity- and IT-focused industry sectors primarily within the U.S. Bureau of Labor Statistics (BLS) Standard Occupational Classification (SOC) job codes within the 15-000 Computer and Mathematical Occupations series, which provides a better comparison with the public sector cybersecurity and IT workforce. We also examined job codes within the 11-000 Management Occupations series to capture relevant cybersecurity and IT managerial positions that are also represented in DCWF. Relative to the other BLS SOC categories, the Management Occupations and the Computer and Mathematical Occupations series provide a better benchmark for comparison with the public sector cybersecurity and IT workforce.

[5] The Workforce Framework for Cybersecurity, or NICE Framework, was originally developed by the U.S. Department of Homeland Security, with input from both the private and other government agencies (see NIST, 2022). DCWF was developed specifically for DoD in 2010 and used the NICE Framework as its foundation, and the two frameworks are therefore interchangeable.

[6] In 2016, Congress created a distinct personnel system, the CES Report, and granted DoD flexibilities in setting compensation aimed at the recruitment and retention of personnel considered critical to the DoD cyber mission. See DoD Directive 8140.01, 2020; U.S. Code, Title 10, Section 1599f, 2016; and Pub. L. 114-92, Sec. 1107, 2015.

[7] Although the CES Report predates the DCWF, we leveraged the DCWF's predecessor, the NICE Framework, because it provided a consistent cybersecurity classification and established a set of work roles and required knowledge, skills, abilities, and tasks (KSATs) for cyber and related work. The nine priority work roles in the CES Report were (1) Cyber Defense Analyst, (2) Cyber Operator, (3) Exploitation Analyst, (4) Security Control Assessor, (5) Software Developer, (6) System Test and Evaluation Specialist, (7) System Security Analyst, (8) Authorizing Official, and (9) Cyber Defense Incident Responder.

[8] See Knapp et al., 2021.

[9] O*NET is a database of KSATs considered necessary for specific jobs based on surveys of analysts and industrial and organizational psychologists. Both the ACS and O*NET map occupations and associated KSATs to SOC job codes. The authors used KSATs listed in O*NET to map the DCWF work roles to their private sector counterparts (denoted with BLS job codes) found in the ACS.

[10] The CyberSeek project provides a web-based tool supported by NICE (see CyberSeek, undated-a).

[11] NAICS codes 51, 52, and 54 are official NAICS codes, while 000001 and 999001 are specific BLS coding schemes used to identify all private sector firms and all government organizations, respectively.

[12] We used public and private sector supply and demand data from the CyberSeek heat map (see CyberSeek, undated-b).

[13] Because the Data Scientist job code (15-2051) only appears in 2021, time trend analysis is not possible for this job role.

[14] These results are robust to analysis of the median data, and so we only present the mean salary data.

[15] As before, a time trend analysis for the Data Scientist job code (15-2051) is not possible.

[16] For reference, the underlying sample size used by BLS for 2021 is shown in Table A.13 in the appendix.

[17] For support and administrative roles, the public sector employs approximately 47 percent of such workers versus 29 percent in the private sector. In regard to software development and testing roles, the private sector employs approximately 48 percent of such workers versus 28 percent in the public sector.

References

BLS—*See* U.S. Bureau of Labor Statistics.

CNSSI—*See* Committee on National Security Systems Instruction.

Committee on National Security Systems Instruction 4009, *Committee on National Security Systems (CNSS) Glossary*, March 2, 2022.

CyberSeek, homepage, undated-a. As of October 1, 2022:
https://www.cyberseek.org/

CyberSeek, "Cybersecurity Supply/Demand Heat Map," webpage, undated-b. As of June 28, 2022:
https://www.cyberseek.org/heatmap.html

Department of Defense, Chief Information Officer, "The DoD Cyber Workforce Framework (DCWF)," webpage, undated. As of October 1, 2022:
https://dodcio.defense.gov/Cyber-Workforce/DCWF.aspx

Department of Defense Directive 8140.01, *Cyberspace Workforce Management*, U.S. Department of Defense, October 5, 2020.

DoD CIO—*See* Department of Defense, Chief Information Officer.

DoD Directive—*See* Department of Defense Directive.

Knapp, David, Sina Beaghley, Karen Schwindt, and Daniel Schwam, *Employee Conversions to the Cyber Excepted Service: Assessing Factors and Characteristics to Personnel Conversion Decisions*, RAND Corporation, 2021. As of [accession date]:
https://www.rand.org/pubs/research_reports/RRA730-2.html

Markow, William, and Nomi Vilvovsky, *Securing a Nation: Improving Federal Cybersecurity Hiring in the United States*, Burning Glass Technologies, March 2021.

McIntosh, Molly F., Sasha Romanosky, Thomas Deen, Samantha E. DiNicola, Christopher Ferris, Jonathan Fujiwara, Priya Gandhi, Henry Hargrove, Kirsten M. Keller, Maria C. Lytell, Mace Moesner IV, Isabelle Nazha, Zhan Okuda-Lim, Nina Ryan, Karen Schwindt, and Amanda Wicker, *Support to the DoD Cyber Workforce Zero-Based Review: Developing a Repeatable Process for Conducting ZBRs Within DoD*, RAND Corporation, RR-A660-6, 2022. As of September 19, 2022:
https://www.rand.org/pubs/research_reports/RRA660-6.html

National Initiative for Cybersecurity Careers and Studies, "Workforce Framework for Cybersecurity (NICE Framework)," Cybersecurity and Infrastructure Security Agency, webpage, June 30, 2022. As of October 1, 2022:
https://niccs.cisa.gov/workforce-development/nice-framework

National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, SP 800-37, rev. 2, December 2018.

National Institute of Standards and Technology, "NICE Framework Resource Center: History," webpage, August 4, 2022: As of October 1, 2022:
https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/history

NICCS—*See* National Initiative for Cybersecurity Careers and Studies.

NIST—*See* National Institute of Standards and Technology.

Public Law 116-92, National Defense Authorization Act for Fiscal Year 2020, Section 1652, Zero-Based Review of Department of Defense Cyber and Information Technology Personnel, December 20, 2019.

U.S. Bureau of Labor Statistics, "2018 Standard Occupational Classification System," webpage, undated-a. As of October 1, 2022:
https://www.bls.gov/soc/2018/major_groups.htm

U.S. Bureau of Labor Statistics, "Occupational Employment and Wage Statistics," webpage, undated-b. As of October 1, 2022:
https://www.bls.gov/oes/tables.htm

U.S. Bureau of Labor Statistics, "Occupational Employment and Wage Statistics, May 2021: 11-3021 Computer and Information Systems Managers," webpage, March 31, 2022. As of October 1, 2022:
https://www.bls.gov/oes/current/oes113021.htm

U.S. Code, Title 10, Section 1599f, United States Cyber Command Recruitment and Retention, January 3, 2016.

Acknowledgments

We are grateful to Walter Spears and Hali Sparks of DoD CIO and to our RAND colleagues Molly F. McIntosh, Daniel Ginsberg, Igor Mikolic-Torreira, Lisa Abraham, and Jim Powers.

About This Report

In the fiscal year 2020 National Defense Authorization Act (NDAA), the U.S. Department of Defense (DoD) was tasked with performing a *zero-based review* (ZBR)—a detailed review rather than a simple comparison with previous size or budget—of its cyber and information technology (IT) personnel. The NDAA requires that DoD departments, components, and agencies complete ZBRs for their cyber and IT workforces and that those ZBRs be submitted to the Principal Cyber Advisor, DoD Chief Information Officer (DoD CIO), and the Under Secretary of Defense for Personnel and Readiness.

DoD CIO asked the RAND Corporation's National Defense Research Institute to produce a transparent and repeatable process for validating and ensuring the consistency of data and analysis used for the ZBR. In this report, we extend that previous research by collecting and analyzing additional cyber workforce data to further compare the private and public sector cyber workforces.

The research reported here was completed in December 2022 and underwent security review with the sponsor and the Defense Office of Prepublication and Security Review before public release.

RAND National Security Research Division

This research was sponsored by the Principal Advisor for Cybersecurity, Strategy, Planning, and Oversight in the Office of the DoD CIO and conducted within the Forces and Resources Policy Program of the RAND National Security Research Division (NSRD), which operates the National Defense Research Institute (NDRI), a federally funded research and development program sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense intelligence enterprise.

For more information on the RAND Forces and Resources Policy Program, see www.rand.org/nsrd/frp or contact the director (contact information is provided on the webpage).

For more information on this publication, visit www.rand.org/t/RRA660-7.

www.rand.org

RR-A660-7