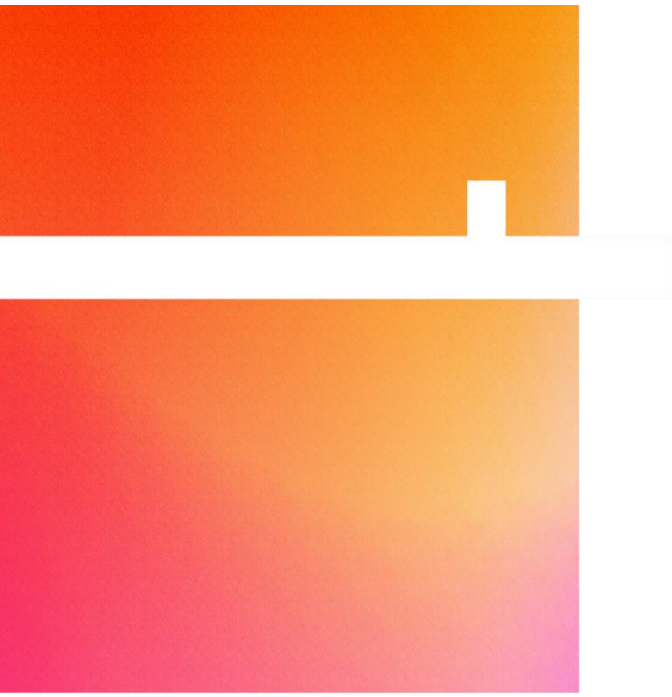
Cybersecurity Workforce Analysis & Strategy

Maryland and DC



MARCH 2024

TEDCO
LEADING INNOVATION TO MARKET

Lightcast

About Lightcast

Lightcast is the world's leading authority on job skills, workforce talent, and labor market dynamics, providing expertise that empowers businesses, education providers, and governments to find the skills and talent they need and enabling workers to unlock new career opportunities. Headquartered in Boston, Massachusetts, and Moscow, Idaho, Lightcast is active in more than 30 countries and has offices in the United Kingdom, Italy, New Zealand, and India. The company is backed by global private equity leader KKR.

Lightcast
232 N Almon Street
Moscow, ID 83843
lightcast.io

Acknowledgements

Lightcast gratefully acknowledges the support of TEDCO (the Maryland Technology Development Corporation) and Cyber Maryland. Special thanks to Alex Choi, TEDCO Government Relations & Research Director, and Mindy Lehman, TEDCO Chief Government Relations & Policy Officer, for project management support. This report is prepared by Lightcast. The content is solely the responsibility of the authors and does not necessarily represent the views of TEDCO or Cyber Maryland. Proper acknowledgement of Lightcast should be included in publications, presentations, or other developed materials.

Introduction

Digital technologies permeate our lives and our infrastructure now more than ever. In this environment, the cybersecurity landscape has never been more important or more challenging. The Maryland and DC region is at the forefront of safeguarding access to these technologies and protecting against their misuse.

A large and healthy cybersecurity workforce is critical to delivering on that important mission. But while the cybersecurity workforce in Maryland and DC is large, it is pulled tight by severe talent shortages.

Cybersecurity training is particularly difficult because the threat landscape evolves so rapidly. Lessons taught in the classroom must be bolstered with practical experience. Practical experience requires access to data systems that are often classified. And by the time curricula are updated and alternative data systems set up for practicums, new and different threats have emerged.

Protecting the technological infrastructure in the Maryland and DC region also means developing a deep understanding of legacy data systems, modern data systems, and future data systems, and serving as the bridge between them. The public sector often relies on legacy data systems, and updating those systems will require the work of the same cybersecurity professionals who are tasked with safeguarding them. Upkeep, updates, and upgrades of these systems are each monumental responsibilities, and cybersecurity professionals must see to all of them.

Fortunately, there is momentum behind growing the cybersecurity workforce. Executive Orders from the White House consistently emphasize enhancing the nation's cybersecurity capabilities. The President's Management Agenda (PMA) names cybersecurity a pillar of modern, effective government. Cybersecurity is also prioritized at the local level. Maryland Governor Wes Moore is developing the Maryland

Cybersecurity Task Force. Cyber Maryland is an existing advisory board of cybersecurity professionals from industry, education, and workforce development, that advise the state on cybersecurity strategy. The state legislature has secured funding from the federal State and Local Cybersecurity Grant Program. The state invests in the EARN Maryland program to advance IT and cybersecurity education and training. There are many local and national resources to bring to bear on expanding the cybersecurity talent pipeline.

This report explores the causes of the cybersecurity talent gaps in the Maryland and DC region and offers some solutions.

Approach

Defining Cybersecurity

In 2010, cybersecurity skills were requested in just five percent of information technology job postings – by 2023, that figure had increased more than twofold to 13 percent. In the Maryland and DC region, nearly a quarter (24 percent) of information technology job postings request cybersecurity skills. The relatively static taxonomies of publicly available labor market information have not kept up with the rise of cybersecurity jobs. The occupation-level data provided by the Bureau of Labor Statistics and Census is limited to a single occupation, Information Security Analysts, which accounts for less than a fifth of cybersecurity supply and demand. Given these limitations, Lightcast leveraged novel datasets, new models, and a more up-to-date taxonomy to provide Cyber Maryland and TEDCO with intelligence on the local cybersecurity labor market.

Using proprietary web scraping technology, Lightcast collects over three million unique job postings daily from over 60,000 sources. Additionally, Lightcast maintains a dataset of work histories pulled from the user profiles on professional networking sites. Lightcast uses text analytics to extract job titles, skills, certifications, employer names, descriptions of education and experience, and more from these documents.

The granular data captured by Lightcast through job postings and social profiles enables the creation of up-to-date taxonomies that are critical in scoping the cybersecurity labor market. The first of these taxonomies is the Lightcast Occupational Taxonomy.[1] This taxonomy goes deeper than more traditional government occupational classifications

[1] Lightcast provides additional information on this taxonomy here: https://kb.lightcast.io/en/articles/7215917-lightcast-occupation-taxonomy-lot

(such as SOC or O*NET) and is updated on an annual basis to ensure that it captures the ever-changing landscape of the US labor market. The second taxonomy is the Lightcast Open Skills Taxonomy.[2] Using a combination of machine learning and rules-based classifiers, Lightcast identifies and standardizes common skills, technical skills, and certifications requested by employers in the text of job postings. This taxonomy allows for nuanced analyses of the employer requirements. The taxonomy is key to scoping the cybersecurity sector because cybersecurity responsibilities have expanded beyond traditional occupation-level or job-title-level scoping.

The third taxonomy used for this report was Lightcast Sectors.[3] Lightcast sectors aim to capture emerging fields which are not sufficiently covered by existing industry classifications (such as the NAICS system). Lightcast sectors include green jobs, artificial intelligence, and cybersecurity, among others. The Lightcast sector for cybersecurity was developed in collaboration with the National Institute of Standards and Technology (NIST) and CompTIA, a leader in IT and cybersecurity credentialing. The collaboration between Lightcast and CompTIA is featured in the website CyberSeek.org, the most granular and up-to-date authority on the national cybersecurity workforce.

As further validation of the Lightcast cybersecurity job-posting classification, Lightcast is using this taxonomy to provide regular readouts to the White House about the state of the cybersecurity workforce nationally. A 2023 press release regarding the White House National Cybersecurity Workforce and Education Strategy explains, “Lightcast will provide quarterly data announcements on the size of the cyber talent needs, providing a more comprehensive, up-to-date picture of the cyber labor market.” In this way, this report on the Maryland and DC cybersecurity workforce is working from the same dataset that is setting the agenda at the federal level.

---

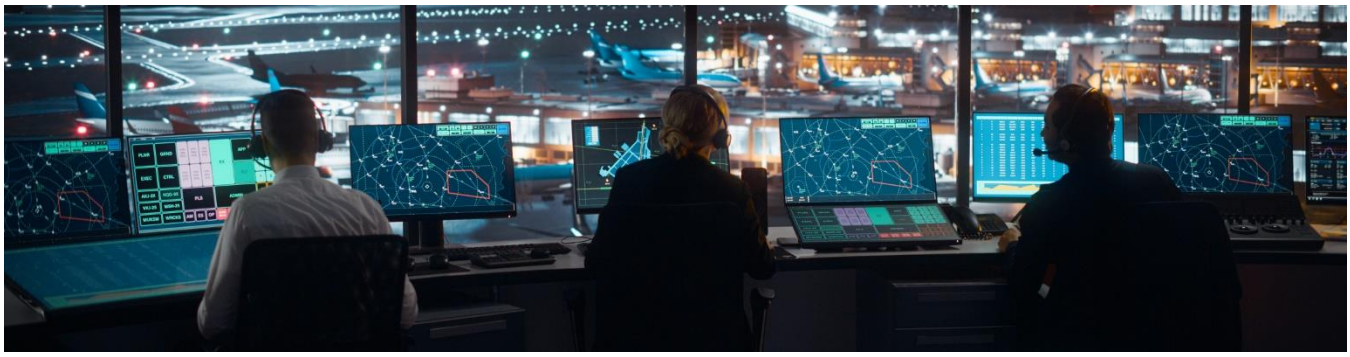
[2] Lightcast provides additional information on this taxonomy here: https://lightcast.io/open-skills

[3] Lightcast provides additional information on this taxonomy here: https://kb.lightcast.io/en/articles/7960247-lightcast-sectors

Leveraging the taxonomies above, Lightcast used occupations, skills, and certifications to classify job postings and social profiles into three categories:

- **Cybersecurity-Forward Roles** are those central to the creation, analysis, and management of cybersecurity technologies.[4]
- **Downstream Cybersecurity Implementers** are other IT roles that use the tools or strategies developed by cyber-forward occupations.[5]
- **Diffuse Cybersecurity Roles** include all other, non-IT roles that employ cybersecurity skills or tools in the performance of their responsibilities.[6]

Because these categories are defined at the job posting or social profile level, Lightcast can differentiate between cybersecurity and non-cybersecurity roles within the same occupation. For example, Lightcast tags a Software Engineer debugging a video game as a non-cybersecurity role and a Software Engineer developing communication software at the Top Secret/Sensitive Compartmented Information level as a cybersecurity role.



[4] Cybersecurity-Forward Roles are occupations including Chief Information Security Officer, Cyber Security Analyst, Cyber Security Engineer, Cyber Security Architect, Cyber Security Consultant, Cyber Security Manager / Administrator, Cyber Security Product Manager, Cyber Crime Analyst / Investigator, Cyber Security Specialist / Technician, Security / Defense Intelligence Analyst, Vulnerability Analyst / Penetration Tester, Incident Analyst / Responder, IT Auditor, Security Manager, Security Officer, and Security Supervisor, when these roles (job postings or social profiles) use cybersecurity skills.

[5] Downstream Cybersecurity Implementers are occupations that fall within the Lightcast Occupation Taxonomy career area Information Technology and Computer Science when these roles (job postings or social profiles) use cybersecurity skills. For example, a Software Engineer whose code must comply with the Department of Defense's Zero Trust Strategy falls within this category.

[6] Diffuse Cybersecurity Roles are occupations outside of the Lightcast Occupation Taxonomy career area Information Technology and Computer Science when those roles (job postings or social profiles) use cybersecurity skills. For example,

Modeling Supply-Demand Gaps for Cybersecurity

Lightcast combines trend data from job postings and social profiles with publicly available labor market information in order to accurately model the supply of and demand for cybersecurity talent.

A supply-demand gap is best measured during a relatively tight increment of time. Over a long enough period, a single position could be listed as a vacancy, filled, vacated, and relisted, which would thus appear in demand-side datasets twice times over that period. Similarly on the supply side, jobseekers find employment over a long enough horizon, so the measurement window should be constrained within the typical job search period. When modeling the supply-demand gap for cybersecurity, Lightcast used the most recent two-month period for which data was available: December 2023 to January 2024. This date range provides the most up-to-date account of supply and demand for cybersecurity.

On the demand side, vacancies are calculated as the sum of job postings that were open at any point during the above time range. On the supply side, the estimate is a sum of individuals who are unemployed and qualified for a given occupation and individuals who are undergoing job changes into that same occupation. The unemployment estimate is calculated using data produced at the state-level and occupation group-level from the Bureau of Labor Statistics. The estimate of supply due to occupational transitions uses a matrix of occupation-to-occupation movement captured in social profile data at the national level. The sum of these two measures is the total supply for a given occupation. To subset these occupation-level estimates to the cybersecurity workforce, Lightcast uses historical job posting data, under the assumption that past hiring activity is indicative of current staffing patterns. The historical posting set includes job postings from the Maryland and DC region over the five-year period of 2019 to 2023. The model is illustrated in the following example: historical postings data for Network Engineers / Architects show cybersecurity skills requested in 52 percent of observations, so we estimate that a similar share of the available supply for this occupation in the cybersecurity workforce.

Lightcast further segments supply and demand for cybersecurity talent into industry buckets: public sector, private sector, and government contractors. Lightcast classifies private sector industries according to the North American Industry Classification System (NAICS). Job postings and social profiles are classified according to the employer. For example, a vacancy posted by Google is tagged to the Information sector (NAICS code 51). For the public sector, Lightcast uses both the NAICS system and a set of keywords that commonly appear in public sector employer names (such as “State of…,” “District of…,” and more). Lightcast also implemented a methodology to identify government contractors within the job posting dataset: Government contractors are identified using the Federal Procurement Data System from usaspending.gov for the prior five fiscal years (2019-2023).

Estimating Supply from the Postsecondary System

Postsecondary education systems are an important component of the supply pipeline for cybersecurity talent. Lightcast analyzed two sources of postsecondary education: the college and university system, including certificate programs, two-year programs, four-year programs, and advanced programs; and the adult education or non-profit education system, which often targets older or nontraditional learners and offers non-degree credentials.

Lightcast referred to several sources to inventory Maryland's education and training assets. For the college and university system, Lightcast used data from the National Center for Education Statistics (NCES), specifically the Integrated Postsecondary Education Data System (IPEDS). Lightcast mapped completers from colleges and universities to the cybersecurity sector if they graduated from a set of cybersecurity-aligned degree programs, defined according to Classification of Instructional Programs (CIP) codes.[7] Lightcast estimates annual completions in the Maryland and DC region by calculating the average annual completions from these programs in the region over the previous five years.

Program-level completions are then mapped to occupations using a proportional crosswalk derived from historical job postings (2019-2023). For example, if 20 percent of postings that reference a degree in the CIP code for Cybersecurity Defense Strategy/Policy are hiring for Cyber Security Analysts, then 20 percent of completions from this program are assigned to that occupation. To avoid degree-occupation mismatches and to limit the long tail of potential degree-occupation pairs, Lightcast only considers CIP-SOC pairs that have been validated by a proprietary Lightcast CIP-SOC

[7] The CIP codes that qualify as cybersecurity-aligned include the following: Artificial Intelligence; Computer and Information Sciences and Support Services, Other; Computer and Information Sciences, General; Computer and Information Sciences, Other; Computer and Information Systems Security/Information Assurance; Computer Engineering, General; Computer Engineering, Other; Computer Hardware Engineering; Computer Science; Computer Software Engineering; Critical Infrastructure Protection; Cyber/Computer Forensics and Counterterrorism; Cyber/Electronic Operations and Warfare; Cybersecurity Defense Strategy/Policy; Information Resources Management; Information Technology Knowledge Management; Management Information Systems and Services, Other; Management Information Systems, General

crosswalk. This crosswalk was developed by economists at Lightcast and takes into account feedback from users of Lightcast's flagship web applications, many of whom are education professionals.

Lightcast also measures the talent migration of graduates from postsecondary institutions. Lightcast measures the in-migration of cybersecurity talent graduating from institutions outside of the Maryland and DC region, as well as the out-migration of cybersecurity talent graduating from institutions within the Maryland and DC region. Because the labor shed also includes part of Northern Virginia, Lightcast also performed the migration calculations inclusive of the section of Northern Virginia in the national capital region metropolitan statistical area. Measurement of retention, attraction, and attrition of cybersecurity talent in the Maryland and DC region was done using social profile data. Social profiles include a user-identified current location, which can be compared against the location of the postsecondary institution also listed on the social profile.

The education and training system outside of colleges and universities includes non-profits, adult education providers, and other skills training organizations. To inventory assets at these providers, Lightcast compiled training programs from organizations promoted on CyberSeek, training institutions listed as Cyber / IT in the EARN Maryland program, and organizations surfaced during desktop research into cybersecurity training in the Maryland and DC region. Lightcast identified 53 training organizations with cybersecurity programming. Lightcast estimated student throughput at these organizations by simulating that a class of 25 students graduates from each location each year. This average class size comports with target class sizes of training organizations that Lightcast engaged during stakeholder interviews, though because of class attrition it serves as an upper-bound estimate of throughput from these organizations. Lightcast then mapped the above programs to cybersecurity and information technology occupations by reviewing the training offerings and educational pathways detailed on the provider's website or in informational brochures.

Expert Engagement

Lightcast worked with experts in the cybersecurity workforce at Cyber Maryland to pressure test and validate the narratives in this report and to generate recommendations. Cyber Maryland is an all-volunteer advisory board comprising industry, education, and workforce development stakeholders from across the cybersecurity ecosystem. Lightcast presented preliminary and interim findings to the board and held a number of focus groups with board members.

The Epicenter of Cybersecurity Talent

The National Capital Region Has the Largest and Most Concentrated Cybersecurity Workforce in the U.S.

The National Capital Region is the epicenter for cybersecurity talent. Compared to other states, the combined Maryland and DC agglomeration ranks fourth in terms of cybersecurity employment and second in terms of active demand for cybersecurity talent. Combined with Virginia, the Maryland-DC-Virginia agglomeration tops even much larger states like California and Texas in terms of the size of the cybersecurity workforce and the demand for cybersecurity talent.

Tables 1 – 2. Cybersecurity Employment and Active Cybersecurity Demand, Top 20 States

State Name	Cybersecurity Employment (2024)
California	166,648
Texas	125,506
Virginia	108,403
Maryland and DC	87,555
Florida	77,209
New York	73,619
Georgia	53,005
Illinois	47,902
North Carolina	46,141
Pennsylvania	42,735
Colorado	41,381
Ohio	38,935
Washington	37,585
New Jersey	37,307
Massachusetts	35,189
Michigan	30,293
Arizona	29,636
Missouri	23,063
Alabama	22,671
Minnesota	20,222

State Name	Active Cybersecurity Demand (Dec. 2023 – Jan. 2024)
Virginia	13,448
Maryland and DC	9,781
California	9,238
Texas	8,843
Florida	5,282
Illinois	5,242
New York	4,238
Colorado	3,848
Pennsylvania	3,678
Georgia	3,669
Massachusetts	3,252
North Carolina	3,165
Ohio	2,954
New Jersey	2,469
Arizona	2,418
Alabama	2,338
Michigan	2,283
Washington	2,130
Missouri	1,968
Minnesota	1,410

Location quotients (LQs) are often used to gauge regional specialization and comparative advantage. To calculate LQ, a region's percent employment in a given sector is measured and divided by the U.S. national percent employment in that sector. A regional LQ of 1.1, then, means that the sector is 1.1 times more concentrated (or 10% more concentrated) in that region than the national average. This calculation can also be performed on the demand side, using job openings rather than employment.

The LQ for the cybersecurity workforce in the Maryland and DC region is 2.69, meaning that the region has 2.69 times more workers employed in cybersecurity than the national average, controlling for the size of the region. Virginia's location quotient is similarly high, at 2.84. Combined, the three-state agglomeration has a cybersecurity sector 2.78 times more concentrated than the national average.

The concentration of demand is even higher for the region. The LQ for cybersecurity demand in the Maryland and DC region is 3.09 and for Virginia is 3.66. Combined, the three-state agglomeration has 3.42 times more demand than the national demand for a region of that size.

Tables 3 – 4. LQ of Cybersecurity Employment and LQ of Active Cybersecurity Demand, Minimum LQ = 1.0

State Name	LQ of Cybersecurity Employment (2024)
Virginia	2.84
Maryland and DC	2.69
Idaho	2.31
Colorado	1.51
Hawaii	1.49
New Mexico	1.17
Georgia	1.17
Alabama	1.16
Alaska	1.15
Rhode Island	1.12
Washington	1.11
Wyoming	1.05
Utah	1.05
Montana	1.04
Massachusetts	1.02
North Carolina	1.02
Vermont	1.01
Delaware	1.01
Arizona	1.00
Virginia	2.84

State Name	LQ of Active Cybersecurity Demand (Dec. 2023 – Jan. 2024)
Virginia	3.66
Maryland and DC	3.09
Idaho	2.06
Hawaii	1.74
Colorado	1.35
Alabama	1.32
Vermont	1.24
Delaware	1.12
Rhode Island	1.12
Georgia	1.08
New Mexico	1.04
North Carolina	1.02
Texas	1.01
Utah	1.00

The federal government is a large reason for the concentration of cybersecurity talent and demand in the national capital region. The region is home to the federal government agencies responsible for national cybersecurity and national defense, including the Department of Defense (DoD), the National Security Agency (NSA), the Department of Homeland Security (DHS), as well as others. These government agencies have also given rise to a large ecosystem of defense contractors, cybersecurity firms, and technology companies that provide cybersecurity services or have their own cybersecurity demands. Additionally, the region is a key location for the development of cybersecurity policy and legislation, which attracts professionals not only skilled in the technical aspects of cybersecurity but also in areas related to policy, regulation, and compliance.

With such concentration of cybersecurity talent, Maryland and DC could benefit from a higher number of cyber-aligned graduates from postsecondary institutions. The Maryland and DC region is seventh in cyber-aligned completions at the sub-bachelor's level, tenth in bachelor's completions, and fifth in advanced degree completions.

Tables 5 – 6. Average Annual Completers from Cyber-Aligned Programs at the Sub-Bachelor's (Sub-BA), Bachelor's (BA), and Master's and Above MA/MA+ Levels, Top 10 states, 2019-2023

State Name	Avg. Annual Sub-BA Completions (2019-2023)
North Carolina	4,521
Kentucky	3,778
California	3,456
Texas	3,296
Florida	2,317
Virginia	1,805
Maryland and DC	1,690
Arizona	1,649
New York	1,609
Utah	1,175

State Name	Avg. Annual BA Completions (2019-2023)
California	11,905
Texas	7,058
New York	6,907
Florida	5,470
Pennsylvania	4,570
Massachusetts	3,856
Georgia	3,758
Utah	3,709
Virginia	3,659
Maryland and DC	3,647

State Name	Avg. Annual MA/MA+ Completions (2019-2023)
California	5,274
New York	5,039
Georgia	2,945
Massachusetts	2,860
Maryland and DC	2,664
Texas	2,540
Illinois	2,353
Pennsylvania	2,244
Utah	2,101
Arizona	1,799

It is noteworthy that the Maryland and DC region falls within the top ten states for production of cyber-aligned completers across all levels of education. The University of Maryland falls within the top 20 institutions graduating cyber-aligned completers. The Naval Academy is a top producer of grads from very-highly-aligned cybersecurity programs including Cyber/Computer Forensics and Counterterrorism and Cyber/Electronic Operations and Warfare. But despite these bright spots, the region will struggle to address its talent shortage without increasing the number of cyber-aligned grads produced by the postsecondary system.

The National Capital Region Also Has the Largest Supply-Demand Gap for Cybersecurity Workers in the U.S.

The cybersecurity talent shortage in Maryland and DC is severe. Lightcast calculates the cybersecurity talent gap as active demand minus available supply, where available

supply represents likely jobseekers. Lightcast estimates that over 6,500 cybersecurity positions were unfilled and unable to be filled over the Dec. 2023 – Jan. 2024 period. Only Virginia has a higher count, at 8,500. The state with the next-largest gap is only contending with 40 percent of the gap in Maryland and DC. Further, measuring the share of active demand that can be met by available supply, the Maryland and DC ranks sixth to last compared to other states. A cybersecurity talent gap is felt in most states, but Maryland and DC can only fill a third of the gap with available supply, compared to states like Massachusetts, California, and Texas, which can generally fill more than half of the openings with available supply.

Tables 7 – 8. Cybersecurity Talent Gap (Active Demand Minus Available Supply) and Share of Cybersecurity Demand Met by Available Supply, Top 20 States by Talent Gap and Bottom 20 States by Share of Demand Met, Dec. 2023 – Jan. 2024

State Name	Cybersecurity Talent Gap (Dec. 2023 – Jan. 2024)
Virginia	8,503
Maryland and DC	6,513
Illinois	2,625
Colorado	1,870
Massachusetts	1,595
Alabama	1,474
Pennsylvania	1,458
Florida	958
Missouri	922
Ohio	902
New York	729
Michigan	707
Minnesota	684
New Mexico	670
Arizona	658
Hawaii	635
Nebraska	571
Wisconsin	563
North Carolina	540
Georgia	518

State Name	Share of Cybersecurity Demand Met by Available Supply (Dec. 2023 – Jan. 2024)
Vermont	23%
Alaska	24%
Rhode Island	30%
North Dakota	32%
Nebraska	33%
Maryland and DC	33%
South Dakota	33%
Wyoming	34%
Hawaii	35%
New Mexico	35%
Virginia	37%
Alabama	37%
Montana	40%
Iowa	44%
Arkansas	48%
Illinois	50%
Massachusetts	51%
Colorado	51%
Minnesota	51%
Wisconsin	52%

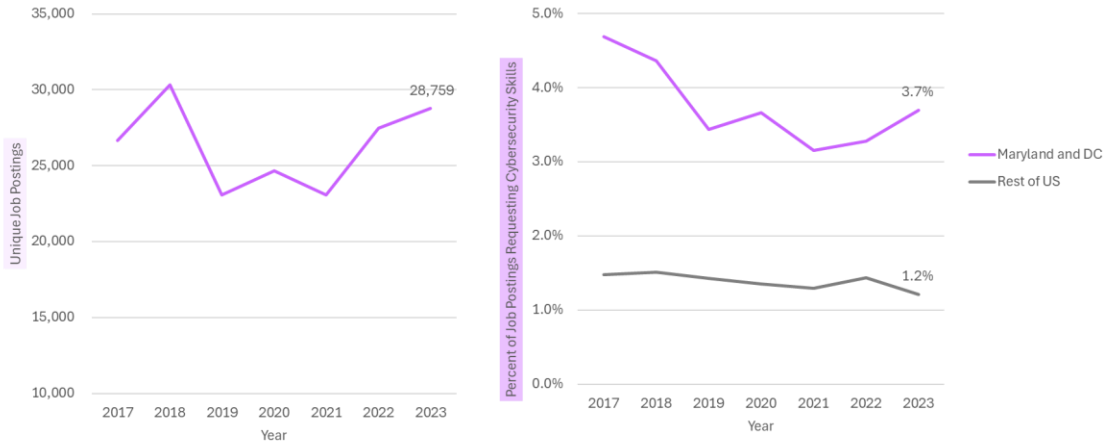
Despite the large cybersecurity workforce in Maryland and DC, demand for cybersecurity workers outstrips supply. The glut of unmet demand is due to several factors. The pace

of hiring for cybersecurity jobs is slower in the Maryland and DC region compared to other markets. Security clearances, bureaucratic hiring procedures, and uncertain staffing budgets contribute to a lengthy hiring process. In the Maryland and DC region, job postings in the information technology career area were kept online on average one additional day when requesting cybersecurity skills compared to when they do not, which ranks seventh compared to other states in the added duration when hiring for cybersecurity skills. The delay increases to 1.5 days on average when security clearances are also required, which ranks third in added duration compared to other states.

The labor market for cybersecurity talent is also tighter than other comparable labor markets in the Maryland and DC area. Compared to tech firms more broadly,[8] the cybersecurity workforce employs nine workers for every job posting compared to twelve workers at other tech firms.

The talent shortage in the Maryland and DC region does not seem to be dampening the overall demand for cybersecurity talent in the region. Despite a dip in demand during the Covid-19 pandemic, the count of job postings hiring for cybersecurity skills in the region is approaching all-time highs.

Figures 1 – 2. Unique Job Postings for Cybersecurity and Cybersecurity Share of All Postings in Maryland Compared to the Rest of the U.S., 2017-2023

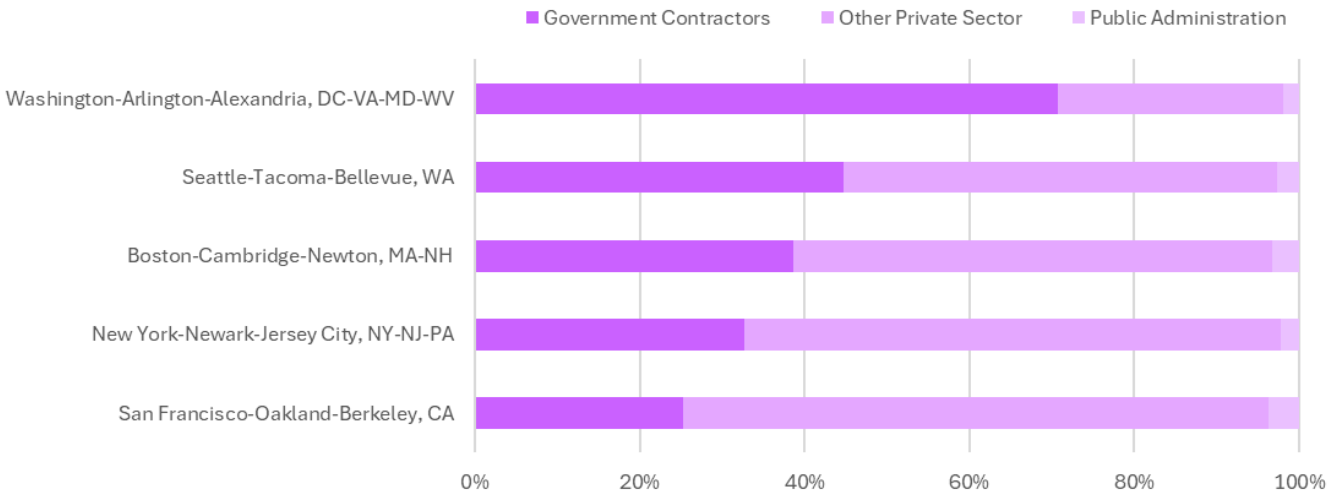


[8] Defined according to NAICS 51: Information, which includes software publishers, data processing and storage, and telecommunications firms among others.

Unique Employer Profile

The national capital region has a unique workforce composition, with its combination of public sector agencies, government contractors, and security ecosystem. This workforce has a significant influence on the dynamics of the cybersecurity labor market. Compared to peer regions such as the Bay Area, New York, Boston, and Seattle, the national capital region has between 1.5 to 2.8 times as many government contractors.

Figure 3. Distribution of Cybersecurity Job Postings Across Government Contractors, Other Private Sector, and Public Administration, Top Tech Metros, 2023



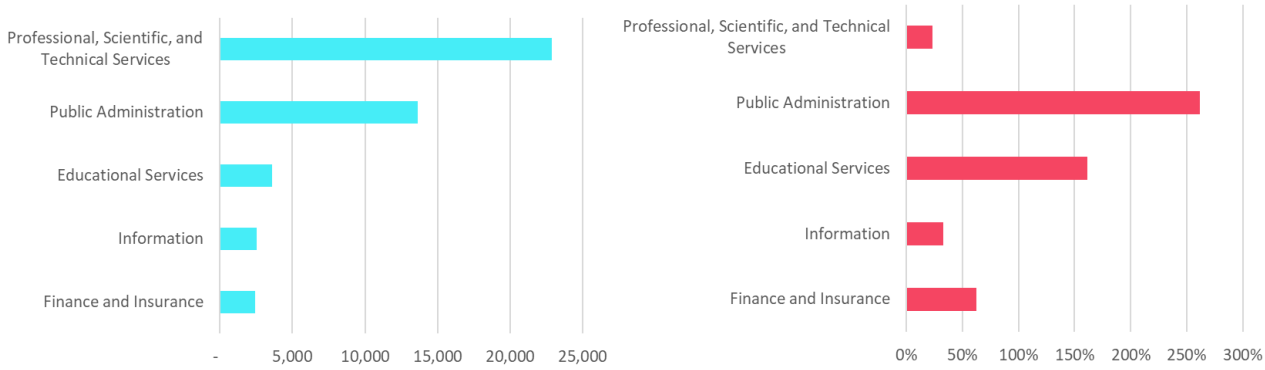
Seattle's cybersecurity sector is dominated by Amazon, Boeing, and Microsoft, none of which are top ten employers by demand in the DC metropolitan region. The Boston and New York metropolitan regions have a greater concentration of demand in banking, but none of the top ten employers by demand for cybersecurity in the DC metropolitan region are banks.

Investigating Cybersecurity Talent Gaps

Sizing Cybersecurity Talent and Demand in the Public Sector, Private Sector, and at Government Contractors

As discussed above, the cybersecurity workforce in the Maryland and DC region is highly concentrated in public sector agencies and government contractors. The five largest sectors by employment of cybersecurity professionals are Professional, Scientific, and Technical Services (which houses many consulting firms); Public Administration (government agencies and publicly owned institutions); Educational Services (including universities); Information (home to software publishers, data processing and storage, and telecommunications); and Finance and Insurance.

Figures 4 – 5. Cybersecurity Employment and Share of Cybersecurity Demand Met by Available Supply, by Industry, Maryland and DC, 2024

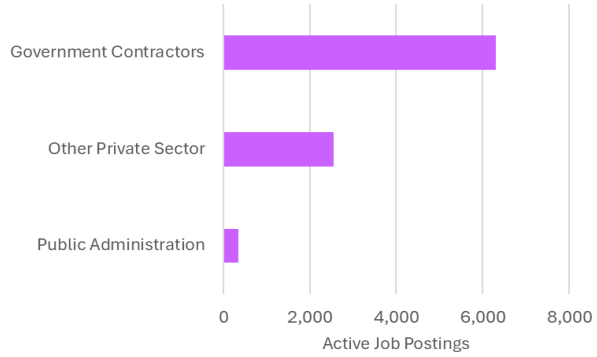


The supply-demand gap for these sectors can be measured by the share of active demand that can be met by available supply. In the Public Administration and Educational Services sectors, cybersecurity demand is satisfied with the existing talent supply. In the sector primarily driven by government contractors – Professional, Scientific, and Technical Services – only 23 percent of active demand can be met by available supply (as of Jan. 2024). That share is slightly higher in the other private sector

industries, Information (33 percent) and Finance and Insurance (62 percent). On the whole, the talent shortage is driven predominantly by cybersecurity demand at government contractors.

Lightcast aggregated active demand into three employer categories: government contractors, other private-sector employers, and public administration. Government contractors account for 68 percent of total active demand and 71 percent of private sector demand. The public sector only accounts for four percent of active demand.

Figure 6. Active Demand, by Sector, Maryland and DC, Dec. 2023 – Jan. 2024



The government contractors with the greatest demand for cybersecurity talent include Leidos, General Dynamics, Booz Allen Hamilton, CACI International, and Northrop Grumman. These employers can be prime targets for workforce development partnerships. This opportunity is discussed in greater detail in the recommendations section of the report.

The distribution of demand across occupations is very different at government contractors compared to the public sector. This finding points to the types of occupations that are underrepresented in the public sector because government agencies are outsourcing the work of these occupations to government contractors. The most prominent role that remains within the public sector is IT Specialist / Engineer. This entry-level occupation accounts for nearly a quarter (23 percent) of demand within the public sector. Meanwhile, the top occupations with cybersecurity demand at government contractors include Cyber Security Engineer and Cyber Security Analyst. With less in-house demand for higher-level cybersecurity occupations, the career pathways for cybersecurity professionals in the public sector are limited.

Tables 9 – 10. Distribution of Active Demand Across Occupations at Government Contractors compared to Public Sector Employers, 2023

Occupation Name	Share of Cyber Demand at Government Contractors
Cyber Security Engineer	8%
Cyber Security Analyst	7%
Network Engineer / Architect	5%
Software Developer / Engineer	4%
Systems Engineer	3%
Cyber Security Manager	3%
Systems Administrator	3%
Help Desk Technician / Analyst	2%
Other Occupations	65%

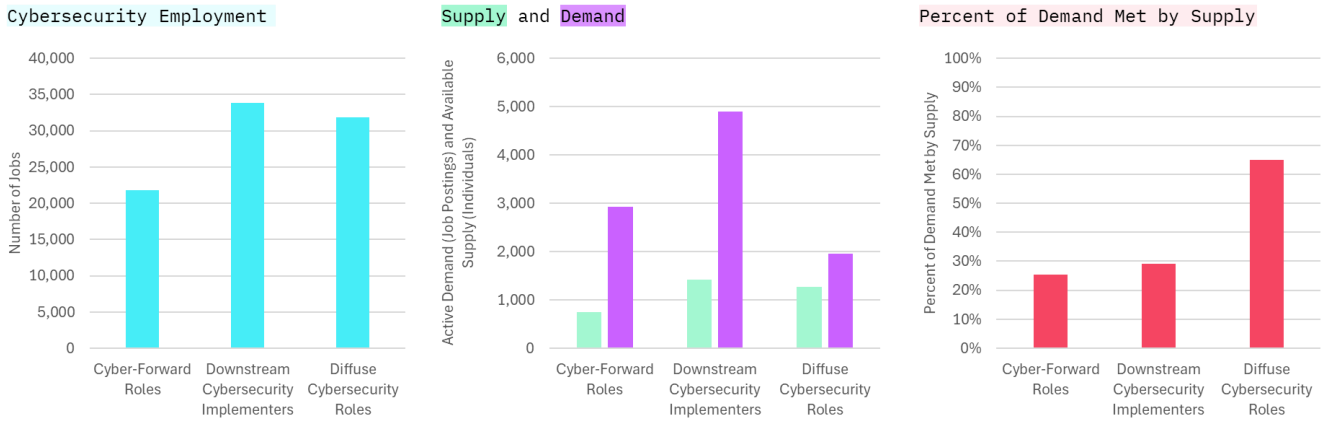
Occupation Name	Share of Cyber Demand in Public Sector
IT Specialist / Engineer	23%
IT Manager	6%
Cyber Security Analyst	4%
Cyber Security Technician	4%
Cyber Security Manager	4%
Cyber Security Engineer	3%
Security / Defense Intel. Analyst	3%
Contracts Analyst	2%
Other Occupations	50%

Cybersecurity Skills Exacerbate Talent Gaps in IT Jobs

Lightcast classified occupations according to how central cybersecurity skills are to the performance of the role. In Cybersecurity-Forward Roles, cybersecurity skills are definitional. Occupations classified as Downstream Cybersecurity Implementers are IT positions that follow cybersecurity protocols in their regular work but may not engage these requirements daily. Finally, Diffuse Cybersecurity Roles cover non-IT positions that nevertheless have cybersecurity responsibilities.

The more significant cybersecurity skills are to the role, the greater the supply-demand gap. Diffuse Cybersecurity Roles have the greatest supply of labor available to fill active demand but can still fill only 65 percent of demand. Downstream Cybersecurity Implementers can only fill 30 percent of active demand. Cyber-Forward Occupations can only fill 25 of active demand, the most acute supply shortage.

Figures 7, 8, 9. Employment, Supply and Demand, and Percent of Demand that can be Met by Available Supply, by Cybersecurity Category, Maryland and DC, Jan. 2023 – Dec. 2024

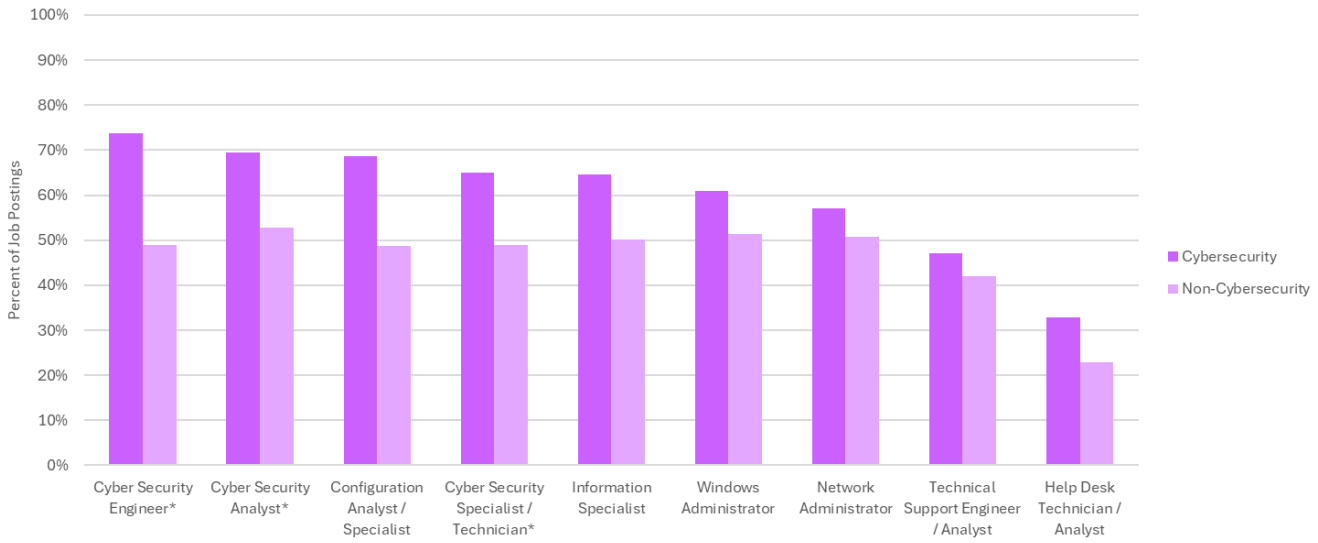


Degree Inflation in Cybersecurity Roles Contributes to Talent Gaps

The cybersecurity workforce tends to require higher levels of education than otherwise similar occupations that are not focused on cybersecurity. The figure below shows this for certain key cybersecurity occupations. When job postings reference cybersecurity

skills, the average level of education increases, even relative to other job postings with the same job title or overall occupation.

Figure 10. Share of Job Postings Requesting a Bachelor's Degree or Higher, When Hiring for Cybersecurity Jobs or Non-Cybersecurity Jobs, Maryland and DC, 2023



* The starred occupations only ever reference cybersecurity skills, as their job title suggests. For these occupations, an alternative non-cyber occupation was used for the comparison: Cyber Security Engineer used IT Specialist / Engineer, Cyber Security Analyst used ERP Analyst, and Cyber Security Specialist / Technician also used IT Specialist / Engineer.

There are many reasons for degree inflation. Cybersecurity roles often require a deep theoretical understanding of computer systems, networks, and security principles, and a degree program provides a structured curriculum that covers that wide range of topics. This educational foundation can be helpful for understanding the complexity of cybersecurity.

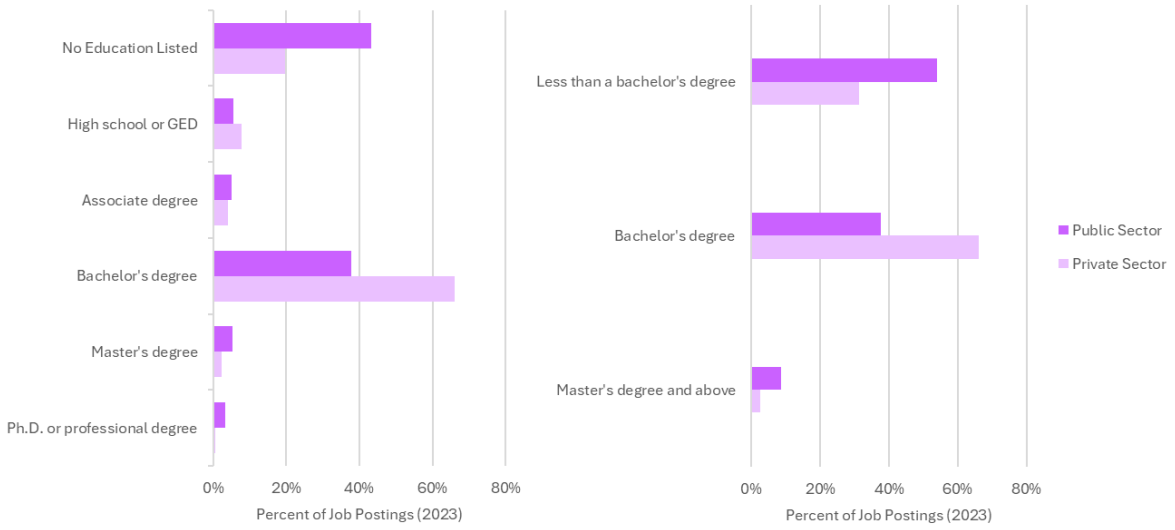
There are also already high levels of education within the incumbent cybersecurity workforce. The Current Population Survey from Census reports that 69 percent of Information Security Analysts – the occupation in the Census taxonomy that best aligns to cybersecurity – have a bachelor's degree or higher, including 42 percent with a bachelor's degree, 25 percent with a master's degree, and 2 percent with a doctoral degree. The level of education is even higher among managers, who are often in charge of the hiring process: 74 percent of Computer and Information Systems Managers have a bachelor's degree or higher, including 45 percent with a bachelor's degree, 26 percent with a master's degree, and 3 percent with a doctoral degree. High levels of degree

attainment in the incumbent workforce helps to explain high degree expectations in the cybersecurity workforce.

Finally, some hiring managers still use a college degree as a proxy for strong critical thinking and problem-solving abilities. These abilities are particularly important in cybersecurity, a field where professionals frequently encounter complex new problems that require innovative solutions.

The public sector tends to have lower expected levels of education for cybersecurity roles. A bachelor's degree is required in 30 percent of job postings from public sector employers, compared to 66 percent in the private sector. In fact, 43 percent of cybersecurity job postings in the public sector make no reference to a minimum education requirement at all, compared to only 20 percent in the private sector. Interestingly, despite the lower average level of education requested in public sector job postings, the share asking for a master's degree or doctoral degree is higher – nine percent in the public sector compared to three percent in the private sector.

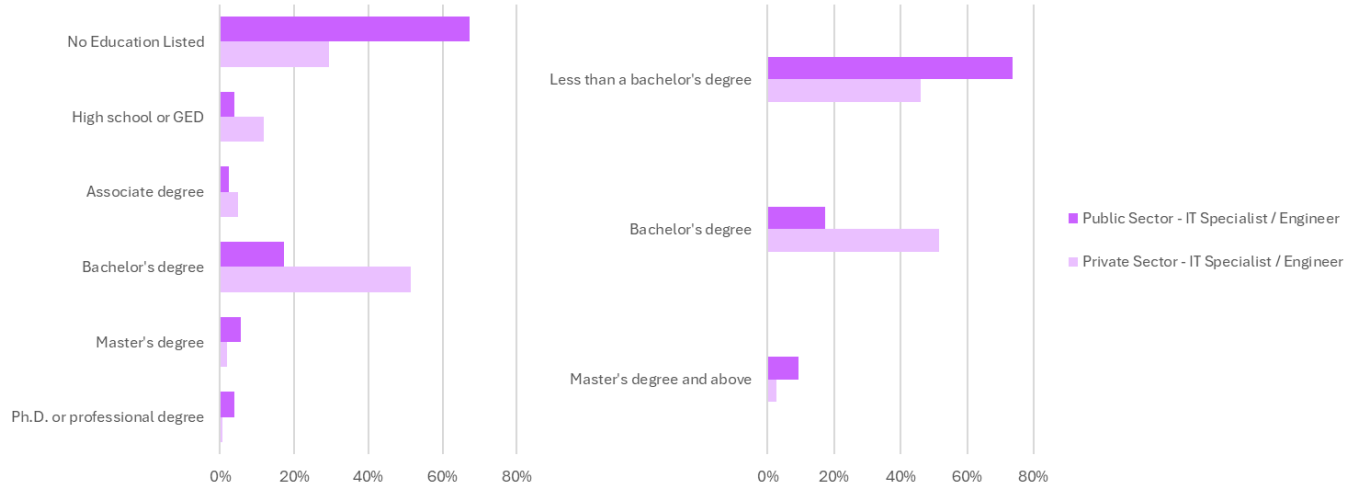
Figure 11. Minimum Levels of Education Requested on Cybersecurity Job Postings in the Public and Private Sectors, Maryland and DC, 2023



Part of the differing educational requirements is driven by the public sector and private sector hiring for different occupations, but degree inflation in the private sector is consistent even across similar occupations. The occupation driving demand in the

public sector is IT Specialist / Engineer, which often requires less than a bachelor's degree. Among public sector employers, 74 percent of demand for this role is at the sub-bachelor's level. In the private sector, however, the expectation of a bachelor's degree is the norm even for this role, with 54 percent of job postings requesting a bachelor's degree or higher. Even when controlling for occupations, the private sector has higher degree expectations.

Figure 12. Minimum Levels of Education Requested on Cybersecurity Job Postings in the Public and Private Sectors, IT Specialist / Engineer, Maryland and DC, 2023



The public sector has made meaningful efforts to move away from degree-based career pathways in the public sector. As early as 2011, the U.S. Office of Personnel Management (OPM) released a competency model for public sector cybersecurity professionals.[9] This competency model included certifications and pathways for skill acquisition within the sector, and it did not make advancement contingent on degree acquisition.

The competency model was updated in 2020, when the National Institute of Standards and Technology (NIST) released the NICE Workforce Framework for Cybersecurity (NICE Framework),[10] which included even more details on competency-based pathways

[9] The February 2011 memorandum can be read here: https://www.chcoc.gov/content/competency-model-cybersecurity

[10] The NICE Framework can be explored here: https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center

through OPM-defined occupations. The NICE framework has become the gold standard for public sector cybersecurity workforce planning, and it focuses on competencies rather than degrees. In 2023, the OPM published additional guidance on how competency models can replace degree requirements.[11]

The state of Maryland has also made efforts to reduce the reliance on degrees in public sector hiring. In 2022, Governor Hogan announced an effort to remove bachelor's degree requirements from many state government roles.[12] This policy is intended to impact a wide range of jobs, including information technology jobs.

The Tension Between Degrees and Certifications in Cybersecurity

Degree requirements are not the only signal that employers seek to indicate jobseeker readiness – certifications are another common signal. The cybersecurity sector also has robust, career-based certification pathways. These certification pathways include but are not limited to the following:

- CompTIA[13] has a cybersecurity certification pathway that includes CompTIA Security+, CompTIA Cybersecurity Analyst (CySA+), CompTIA PenTest+, and CompTIA Advanced Security Practitioner (CASP+).
- Cisco[14] has a cybersecurity certification pathway that begins with the Cisco Certified Support Technician (CCST) certification and advances to the Cisco Certified CyberOps Associate certification.

---

[11] The September 2023 press release can be read here: https://www.opm.gov/news/releases/2023/09/release-opm-releases-new-federal-workforce-competency-initiative-to-support-agencies-with-skills-based-hiring/. It builds on a May 2022 press release that can be read here: https://www.opm.gov/news/releases/2023/09/release-opm-releases-new-federal-workforce-competency-initiative-to-support-agencies-with-skills-based-hiring/

[12] Read more about this announcement here: https://hechingerreport.org/the-new-labor-market-no-bachelors-required/

[13] More information about this pathway can be found here: https://www.comptia.org/blog/the-comptia-cybersecurity-career-pathway-employable-skills-found-here

[14] More information about this pathway can be found here: https://www.netacad.com/careers/pathways-and-certifications

- The Information Systems Audit and Control Association (ISACA)[15] has a cybersecurity certification pathway that runs from the Certified Information Systems Auditor (CISA) credential to the Certified Information Security Manager (CISM) credential and includes other specialty credentials as well.
- (ISC)2[16] has a cybersecurity certification pathway that begins with CC (Certified in Cybersecurity) and has a number of specialized certifications including CISSP (Cybersecurity Leadership), SSCP (Security Operations), CCSP (Cloud Security), CGRC (Governance, Risk, and Compliance), and others.
- The EC-Council[17] cybersecurity certification pathway has beginner, core, advanced, and expert certifications across a range of specialties, including Cyber Forensics, Network and Security, Vulnerability Assessment and Penetration Testing, and more.
- GIAC[18] has a cybersecurity certification pathway that begins with GIAC Security Professional (GSP) and continues on to GIAC Security Expert (GSE).
- The Department of Defense (DoD)[19] has combined some of the above certifications into a DoD-specific pathway matrix that enables workers to level up in two categories: Information Assurance Technical (IAT) and Information Assurance Management (IAM).

Certifications are often presented as a more skills-based substitute for degree requirements. The argument is that certifications are more aligned with a specific set of skills or aligned to a specific occupation, whereas two-year and four-year degree programs include instruction on a much wider range of subjects. Because certifications are more focused, they also take less time to complete and can cost less.

---

[15] More information about this pathway can be found here: https://www.isaca.org/credentialing/certifications

[16] More information about this pathway can be found here: https://www.isc2.org/certifications/cc

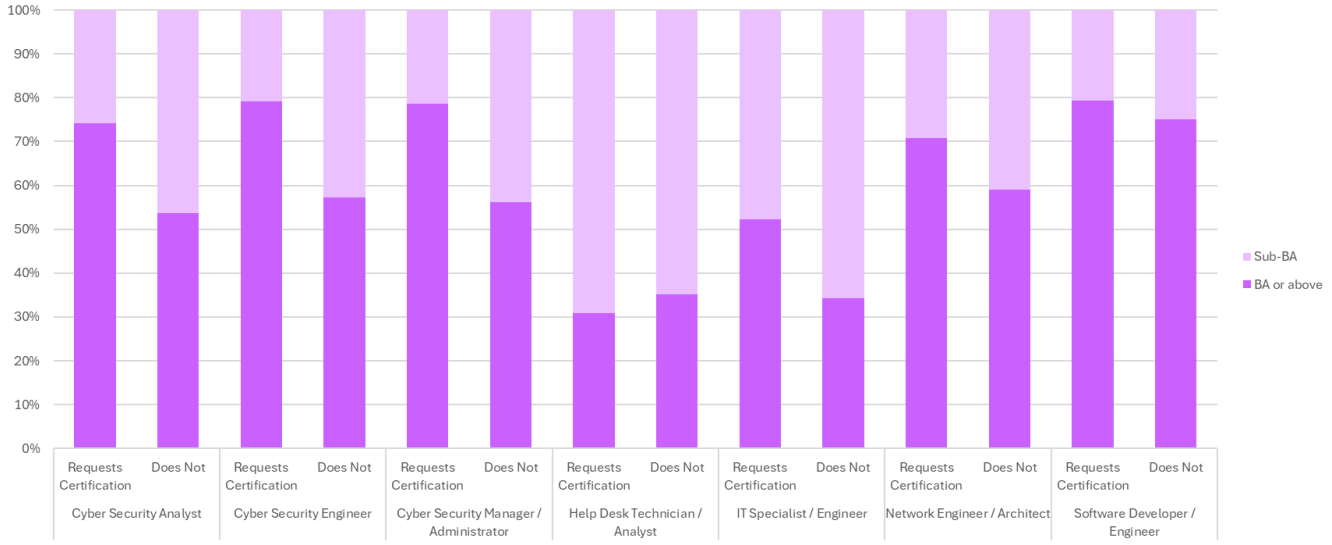
[17] More information about these options can be found here: https://docs.netcomlearning.com/EC-Council-Roadmap.pdf

[18] More information about this pathway can be found here: https://www.giac.org/get-certified/giac-portfolio-certifications/?msc=main-nav

[19] More information about the pathway credential matrix can be found here: https://public.cyber.mil/wid/dod8140/dod-approved-8570-baseline-certifications/

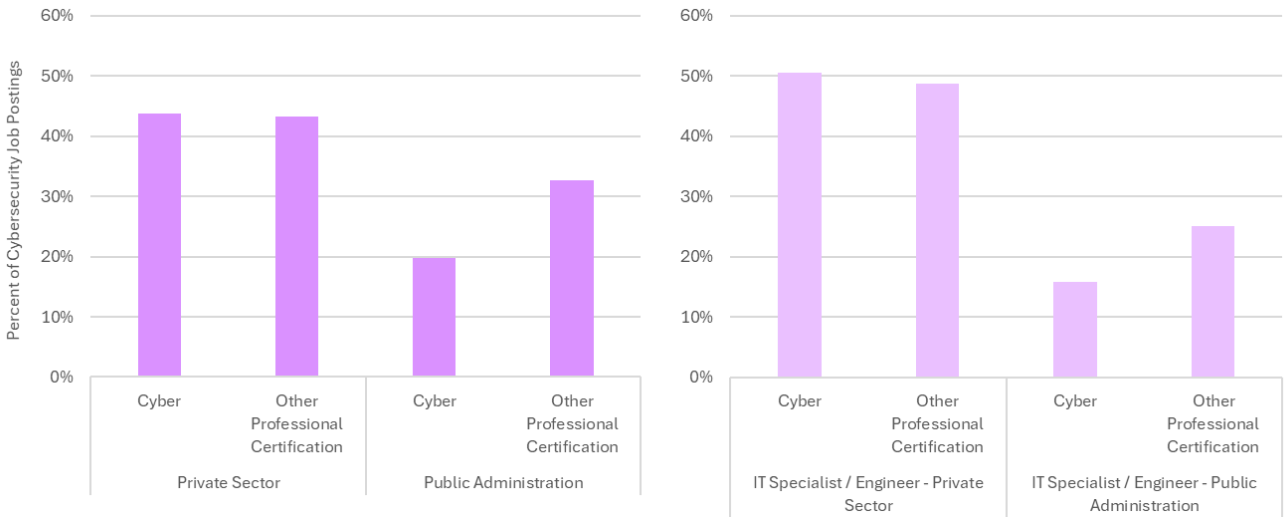
However, in the cybersecurity sector in the Maryland and DC region, the relationship between certifications and degrees appears to be additive rather than substitutional. Cybersecurity job postings that request a certification are more likely to also require a degree at the bachelor's level or higher. The figure below shows some of the occupations in highest demand in the cybersecurity sector. For all but one occupation, Help Desk Technician, the percentage of job postings that request a bachelor's degree or more is higher when the postings are also co-requesting a skills-based credential.

Figure 13. Education Requested in Job Postings, Disaggregated by Whether the Job Posting Requests a Certification, Maryland and DC, 2021-2023



In the public sector specifically, there is another issue with accepting certifications as a meaningful indication of skills-readiness: government agencies in Maryland and DC are not requesting certifications in job postings as often as their peers in the private sector. In the public sector, 20 percent of cybersecurity job postings reference a cybersecurity certification, compared to 44 percent in the private sector. The issue applies to other professional certifications as well, where the public sector requests other professional certifications in 33 percent of cybersecurity postings compared to 43 percent in the private sector.

Figures 14 – 15. Share of Cybersecurity Job Postings Requesting a Cybersecurity Certification or Other Professional Certification, Private Sector vs. Public Sector and Among IT Specialist Postings in the Private Sector vs. Public Sector, Maryland and DC, 2023



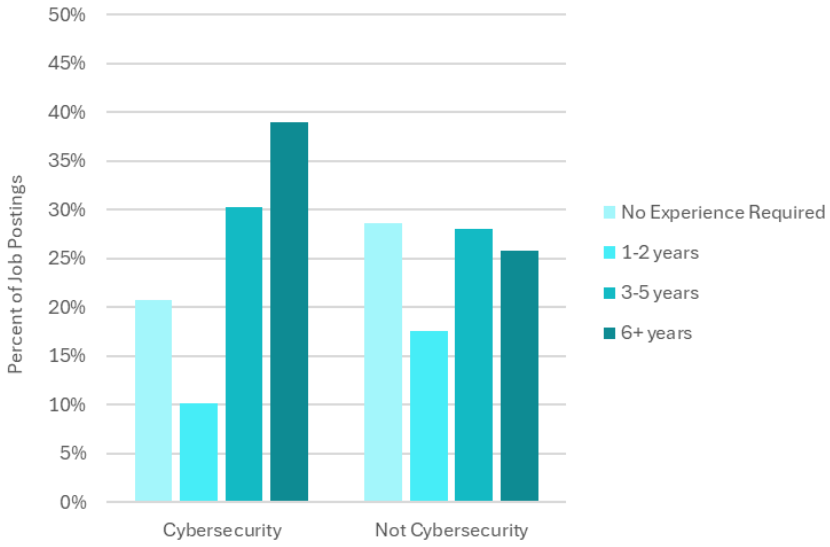
The issue is not driven by differences in the occupations in highest demand in the private sector compared to the public sector. As seen in the above figure, even for the most in-demand occupation in the public sector, IT Specialist / Engineer, public sector postings are less likely to list a certification than private sector postings for the same role.

Experience is the Truest Measure of Readiness But the Most Difficult to Acquire

Focus group participants highlighted prior work experience as the ultimate measure of cybersecurity readiness. Per focus group participants, work experience is crucial for cybersecurity jobs because of the practical, hands-on nature of the work and the importance of trust and reliability in the workplace. Focus group participants shared that theoretical knowledge is necessary but insufficient and that prior work experience is evidence of the ability to apply that knowledge in real-world scenarios, under pressure, and with the nuance of actual systems. Work experience also demonstrates that the individual has previously been trusted with sensitive information and important responsibilities.

Labor market data reinforces the opinions voiced by focus group participants. Only 21 percent of cybersecurity job postings in Maryland and DC are looking for a candidate with no experience, compared to 29 percent in non-cybersecurity jobs. And just 10 percent of cybersecurity job postings are looking for someone with 1-2 years of experience, compared to 18 percent in non-cybersecurity jobs. Combining these two experience buckets, less than a third (31 percent) of cybersecurity job postings could be considered entry-level, or requesting less than two years of experience. In non-cybersecurity job postings, close to half (47 percent) of job postings are in that entry-level range.

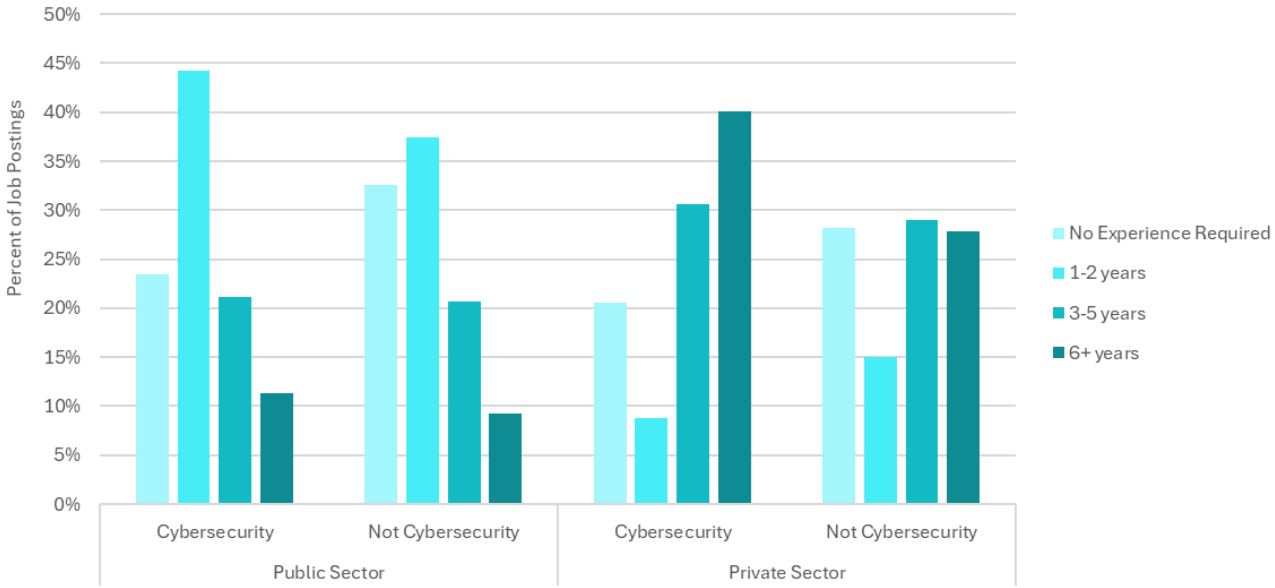
Figure 16. Level of Experience Requested in Job Postings, Cybersecurity vs. Not Cybersecurity, Maryland and DC, 2021-2023

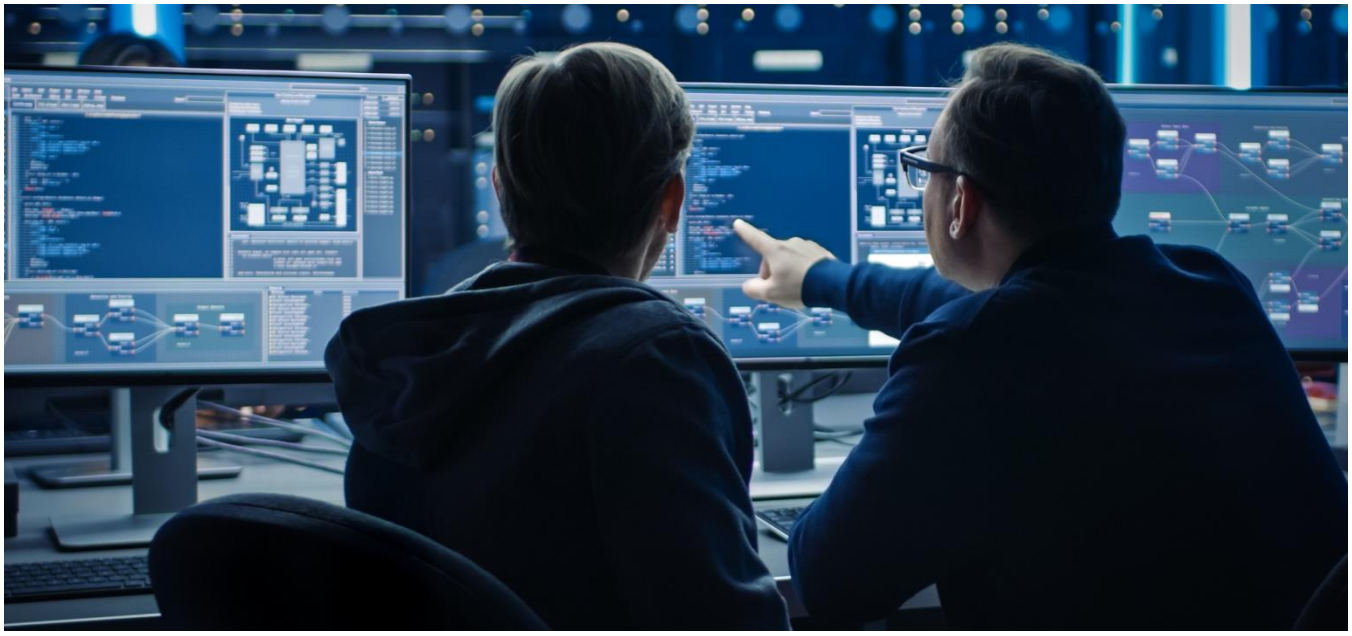


There are notable differences in the levels of experience requested in the public sector compared to the private sector. Similar to requested levels of education, the public sector is far more open to entry-level cybersecurity jobseekers with minimal experience. In the public sector, 44 percent of cybersecurity job postings are open to jobseekers with 1-2 years of experience, compared to just 9 percent in the private sector. The share of job postings open to jobseekers with no prior experience is similarly low across both sectors: 23 percent in the public sector and 21 percent in the private sector. In the private sector, fully 40 percent of job postings are looking for an individual with six or more years of experience. Without reducing those expectations, any interventions to increase the

talent pipeline into cybersecurity will be forestalled by many years as the new cybersecurity workers gain the relevant experience.

Figure 17. Level of Experience Requested in Job Postings, Cybersecurity vs. Not Cybersecurity, by Sector, Maryland and DC, 2021-2023

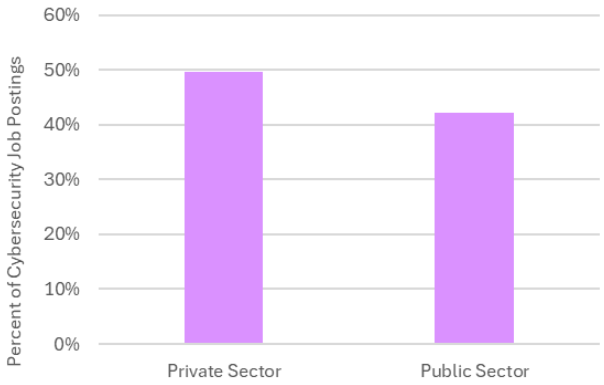




Security Clearances Present Barriers in Both the Public Sector and Private Sector

Security clearances are an important feature of cybersecurity work in the Maryland and DC ecosystem. Security clearances are required in the public sector and in the private sector, commonly via government contractors. Security clearances are required in close to half of all active cybersecurity postings in the Maryland and DC region overall, including 42 percent in the public sector and 50 percent in the private sector.

Figure 18. Percent of Cybersecurity Job Postings Requesting a Security Clearance, Public Sector vs. Private Sector, Maryland and DC, Dec. 2023 – Jan. 2024



Lightcast tracks three levels of security clearance in job postings: Secret Clearance, Top Secret Clearance, and Top Secret-Sensitive Compartmented Information (TS/SCI) Clearance. In all cases, individuals need employer sponsorship from a government agency, they must provide information about their personal, financial, and employment histories, and they must undergo a background check. The duration and stringency of these steps differ by level. The General Services Administration (GSA) approximates 1-2 months to acquire a Secret Clearance, 6-8 months for a Top Secret Clearance, and 8-15 months for a TS/SCI Clearance.[20]

Table 11. Demand for Security Clearances, by Level, Maryland and DC, Dec. 2023 – Jan. 2024

Security Clearance Level	Approximate Duration to Acquire	Percent of Active Cybersecurity Job Postings (Dec. 2023 – Jan. 2024)
Secret	1-2 months	15%
Top Secret	6-8 months	9%
Top Secret-Sensitive Compartmented Information (TS/SCI)	8-15 months	33%

[20] The relevant GSA site is here: https://handbook.tts.gsa.gov/general-information-and-resources/business-and-ops-policies/top-secret/

The most in-demand security clearance level is also the level that takes the longest to acquire. Thirty-three percent of active demand for cybersecurity workers requires TS/SCI Clearance. The next-most in-demand level is Secret Clearance, which is more accessible.

Focus group participations cited the lengthy process to receive a Top Secret Clearance and TS/SCI Clearance as a reason why individuals who would quality for the clearance never seek it. Focus group participants added that, due to the lengthy process and uncertain outcome for Top Secret Clearance and above, employers are reluctant to hire someone who is not already cleared. Clearance requirements were also cited as an impediment to setting up job training programs, such as internships or apprenticeships.

Occupation-Level Gaps are Largest in Technical Roles, Smallest in Managerial Roles

The Cyber-Forward Roles that face the greatest talent shortage are analysts, engineers, and specialists / technicians. These are also some of the largest occupations. Cyber-Forward Roles that involve the management of cybersecurity technologies have less acute talent gaps, though gaps are present.

Figure 19. Employment and Percent of Active Demand Met by Available Supply, by Occupation among Cyber-Forward Roles, Maryland and DC, Dec. 2023 – Jan. 2024

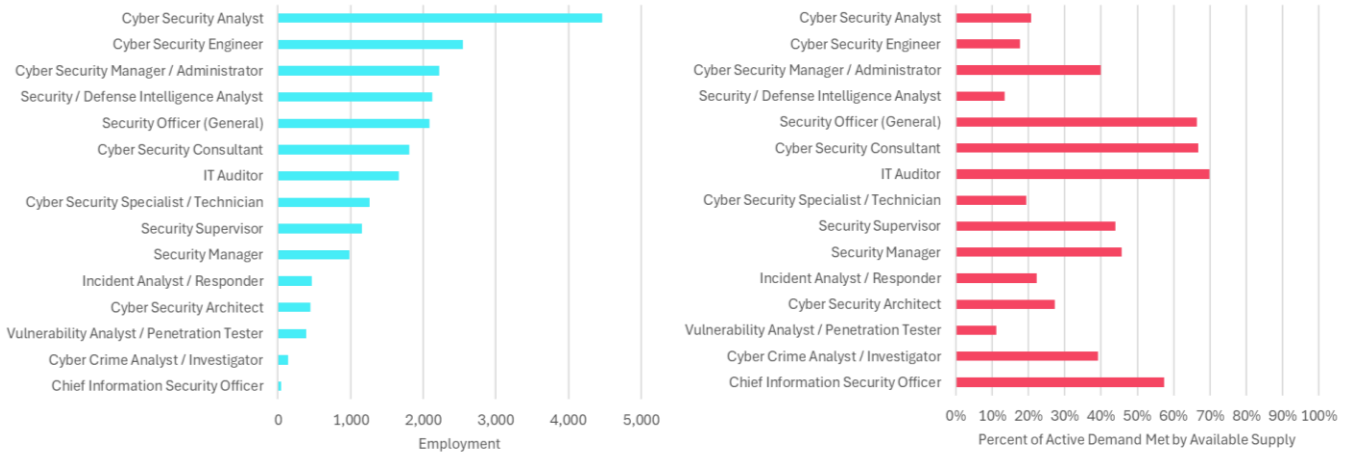
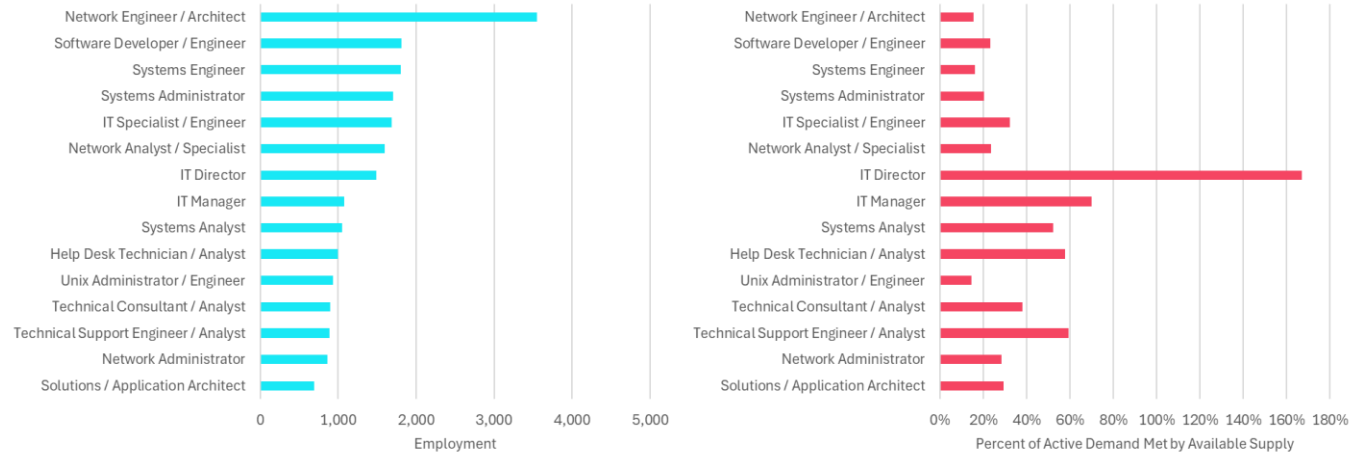


Figure 20. Employment and Percent of Active Demand Met by Available Supply, by Occupation among Downstream Cybersecurity Implementers, Maryland and DC, Dec. 2023 – Jan. 2024

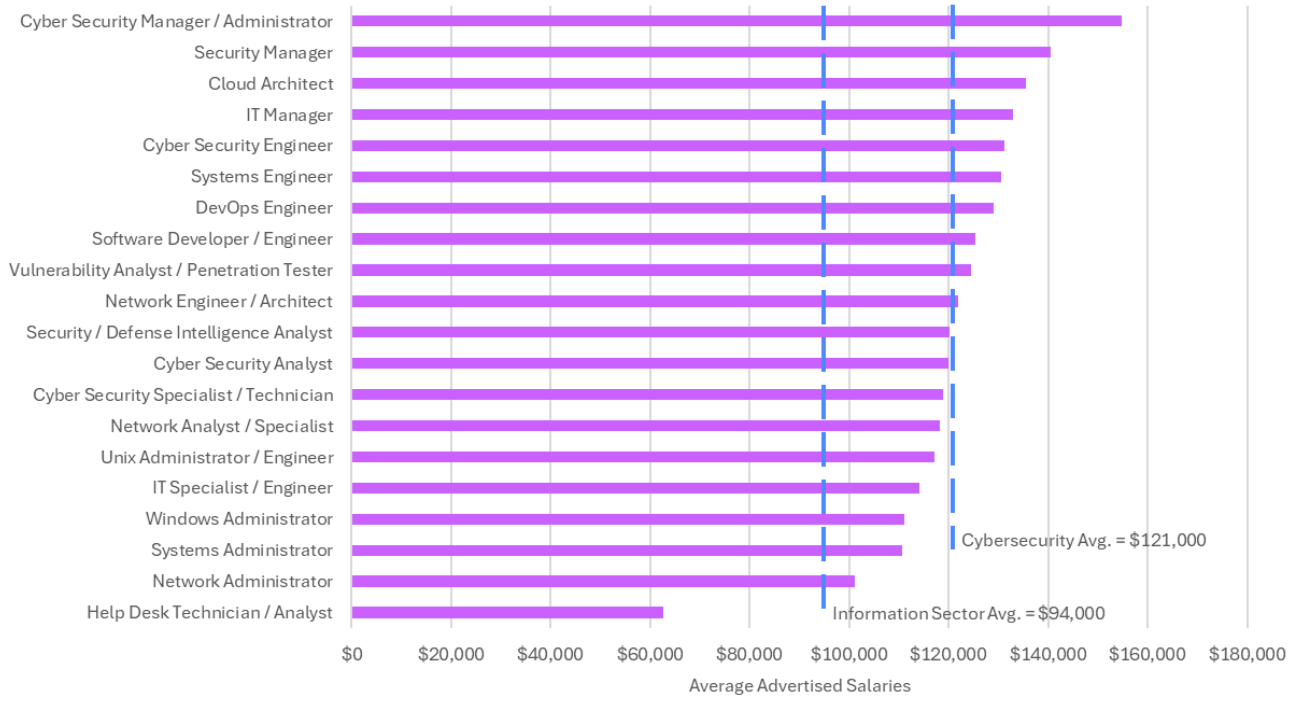


The dynamics of supply and demand for Downstream Cybersecurity Implementers are similar to those of Cyber-Forward Occupations. More technical roles, such as engineers, developers, architects, and administrators have the lowest percentage of current demand that can be met by available supply. Management roles tend to have higher available supply to meet demand. Only one occupation, IT Director, has sufficient supply to meet active demand.

Cybersecurity Skills Command Salary Premia, But Salaries Are Lower in Maryland and DC than in Peer Markets

Advertised salaries on job postings for cybersecurity roles are on average $121,000 compared to $94,000 for the benchmark Information sector (home to software publishing firms and data processing companies). There is a significant management premium in cybersecurity roles. The occupations with the highest advertised salaries are Cyber Security Manager / Administrator and Security Manager, at $155,000 and $141,000, respectively. IT Managers are also in the top five occupations with the highest advertised salaries on job postings, at $132,000. Other occupations that command a high salary on job postings are Cloud Architect, Cyber Security Engineer, Systems Engineer, DevOps Engineer, and Software Developer.

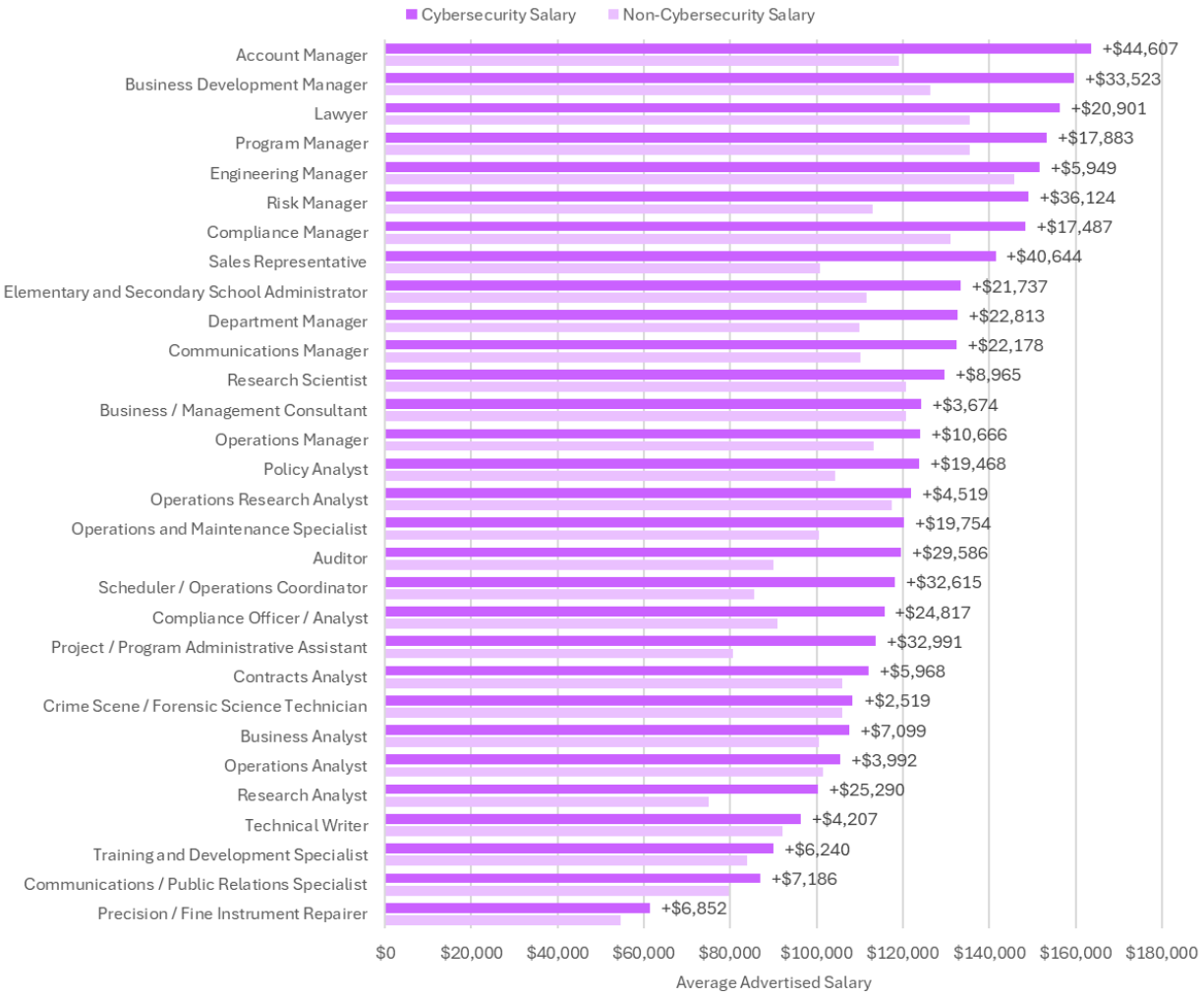
Figure 21. Average Advertised Salary in Cybersecurity Job Postings, by Occupation, Top 20 Occupations by Demand, Maryland and DC, 2021-2023



There can be sizeable salary boosts for incorporating cybersecurity skills into non-tech roles. Lightcast classified non-tech positions with cybersecurity responsibilities as Diffuse Cybersecurity Roles. The salary premia for these cyber-enabled occupations can

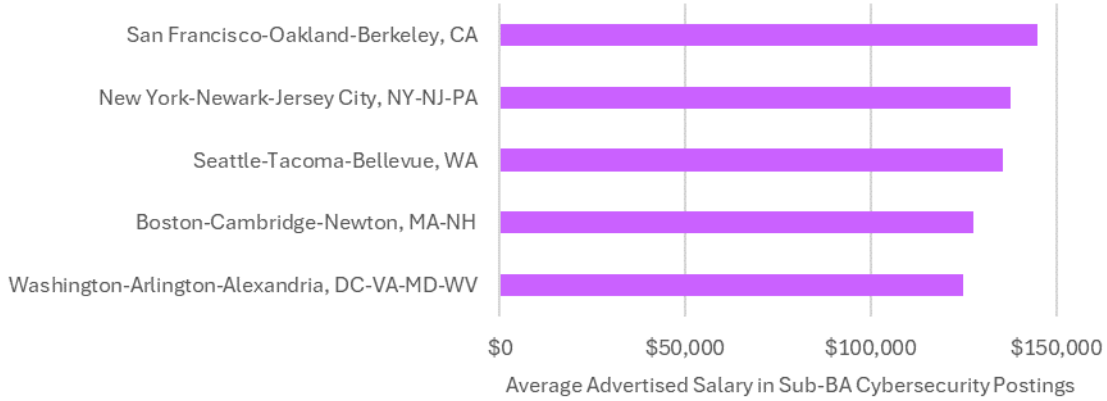
be as high as 40 percent and is often a five-digit boost over similar roles that do not employ cybersecurity skills. The occupations that see the highest salary premia are business-related: Account Manager (+$45,000 boost in advertised salary on job postings when cybersecurity skills are requested), Sales Representative (+$41,000), Risk Manager (+$36,000), Business Development Manager (+$34,000), and Project / Program Administrative Assistant (+$33,000).

Figure 22. Salary Premia for Cybersecurity Skills, by Occupation, Diffuse Cybersecurity Roles, Maryland and DC, Dec. 2023 – Jan. 2024



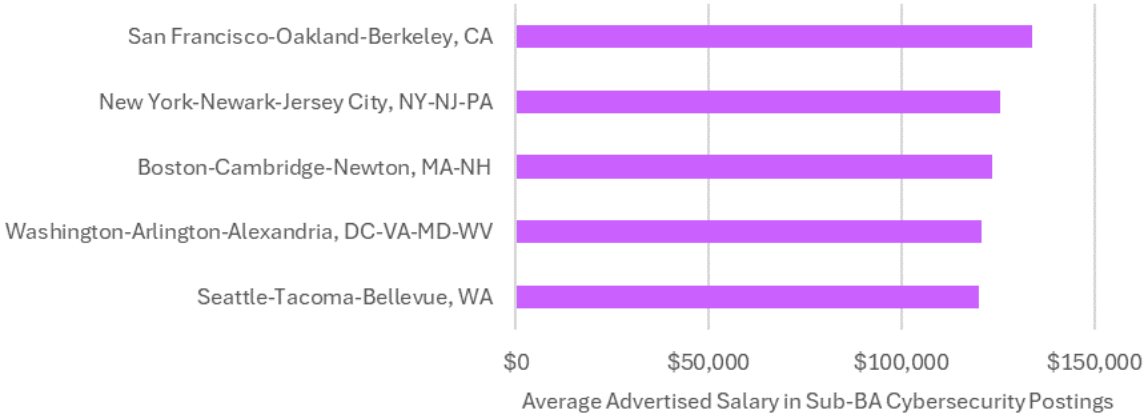
While salaries are high in the Maryland and DC area, they do not keep pace with salaries in other leading tech hubs. In the DC metro area, advertised salaries for bachelor's level cybersecurity roles are only 86 percent of the rates in the San Francisco metro.

Figure. 23. Average Advertised Salary in Cybersecurity Job Postings at the Bachelor's and Above Level, by Metro Region, 2021-2023



At the sub-bachelor's level, the rates in the DC metro are 90 percent of the San Francisco metro. Indeed, the average advertised salary at the sub-bachelor's level in the San Francisco metro is higher than the average advertised salary at the bachelor's level in the DC metro.

Figure. 24. Average Advertised Salary in Cybersecurity Job Postings at the Sub-Bachelor's Level, by Metro Region, 2021-2023

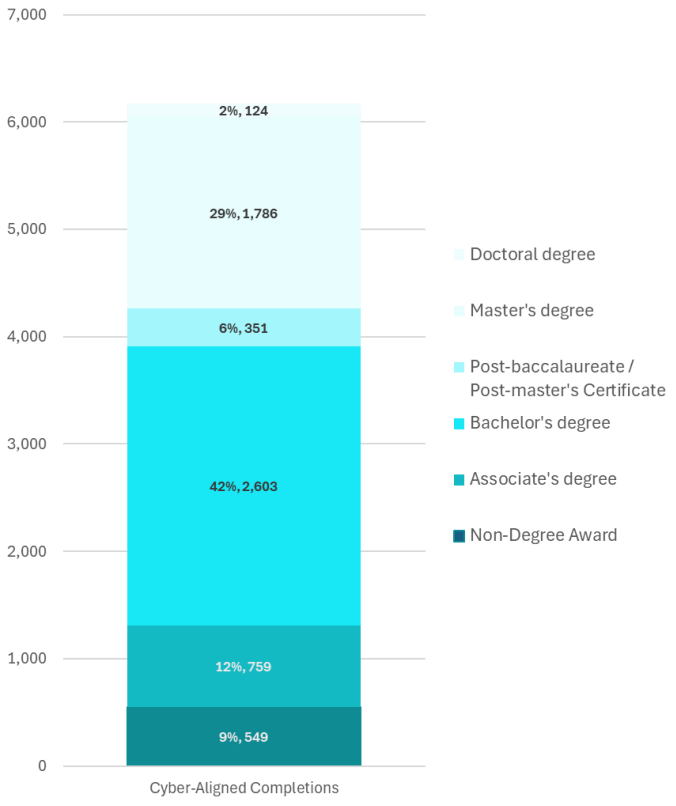


Cyber-Aligned Grads Often Choose Less Cyber-Aligned Careers

While leading the nation in the demand, employment, and concentration of cybersecurity talent, the Maryland and DC region ranks lower in its production of graduates from cybersecurity-aligned postsecondary programs. From these programs, the region ranks seventh in sub-bachelor's completions, tenth in bachelor's degree completions, and fifth in advanced degree completions.

Graduates from cyber-aligned programs in Maryland and DC tend to be from programs at the bachelor's degree level or higher. From colleges and universities, 79 percent of graduates from cyber-aligned programs come from bachelor's degree level programs or higher, and 21 percent come from either the associate degree or certificate programs. The low rate of completions at the sub-bachelor's level – and the propensity of those grads to continue their education in bachelor's level programming – contributes to hiring challenges for cybersecurity-enabled positions such as Help Desk Technicians and Technical Support Specialists.

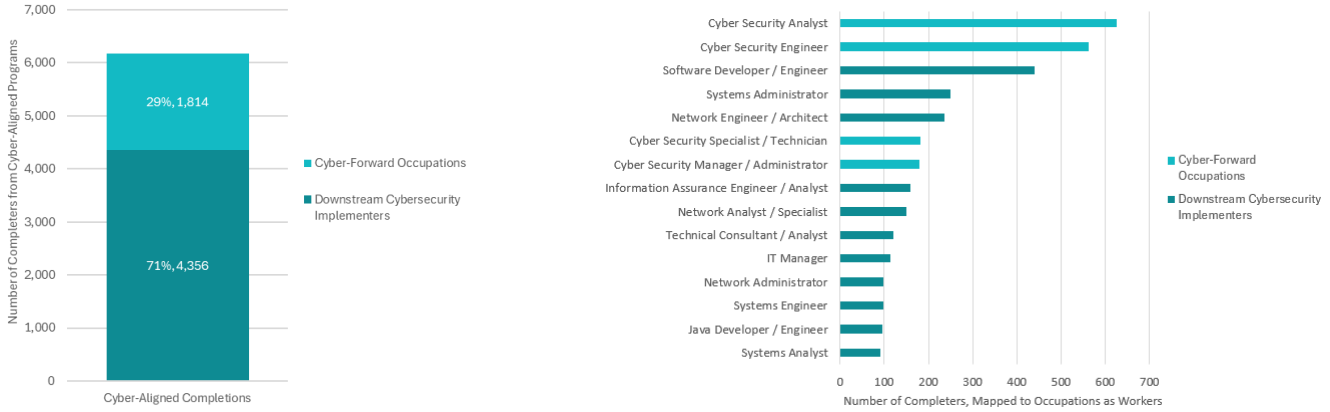
Figure 25. Annual Cyber-Aligned Completions from the Postsecondary System, by Level of Education, Maryland and DC, Annual Averages 2019-2023



Graduates from cyber-aligned programs also often choose not to go into cybersecurity upon graduation, preferring other tech roles with more modest cybersecurity requirements, if any. Of the average annual postsecondary throughput of 6,170

graduates in cyber-aligned degree programs, we estimate that only 29 percent of graduates enter Cybersecurity-Forward Roles, the category of occupations created by Lightcast to house the occupations where cybersecurity skills are definitional (and also the category with the largest gap between supply and demand). Outside of Cyber Security Analysts and Cyber Security Engineers, which are the two most frequent occupations aligning with cybersecurity degrees, eleven of the remaining thirteen most common landing spots for cybersecurity grads are outside of the cyber-forward category (and in the category of downstream cybersecurity implementors).

Figures 26 – 27. Occupation Destinations for Graduates from Cybersecurity-Aligned Programs, Bachelor's Degree Level or Higher, by Cyber-Significance Category and by Occupation, Maryland and DC, Annual Average 2019-2023



Lightcast estimates that the Maryland and DC region has the capacity to graduate up to 1,350 individuals per year in cybersecurity programs outside of the formal postsecondary system of colleges and universities. These institutions include non-profits, adult education providers, and other skills training organizations. In particular, focus group participants referenced Baltimore Cyber Ranges (BCR), which has graduated 1,000 individuals since 2017. Other than BCR, however, focus group participants felt that the nonprofit education system was underutilized.

Because of the targeted nature of these programs, a higher share of completers go on to work in Cybersecurity-Forward Roles. Lightcast estimates that approximately 60 percent of completers from these programs enter Cybersecurity-Forward Roles, compared to 29 percent from colleges and universities. The most common occupation target of these

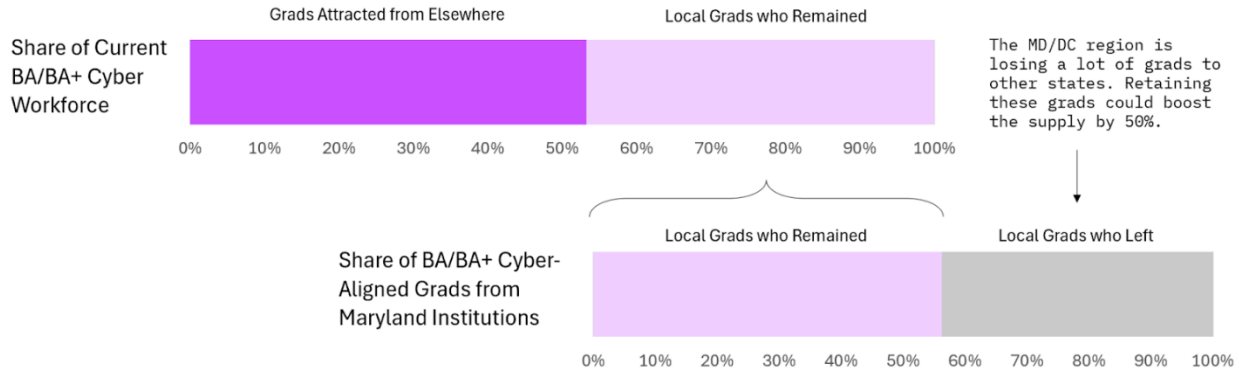
programs is Cyber Security Analyst, followed by Help Desk Technician. Returning to the example of BCR, 900 of the 1,000 graduates went on to work in the cybersecurity sector.

Strong Attraction of Cyber-Aligned Grads from Outside the Region, but Brain Drain of Local Cyber-Aligned Grads

Most of the bachelor's level cybersecurity workforce in the Maryland and DC region came from outside of the state. In fact, the region ranks fourth relative to other states in the ability to attract outside cybersecurity talent. When Northern Virginia is included, the combined region ranks first in cybersecurity talent attraction.

However, Maryland and DC ranks 24th in retention of cyber-aligned grads from local institutions. When Northern Virginia is included, that rank plummets to 45th. Grads at the bachelor's level and above are leaving the region at very high rates.

Figure 28. Migration Patterns of Cybersecurity-Aligned Bachelor's Degree Grads Into and Out of Maryland and DC



Focus group participants cited salary competitiveness as the primary reason that cyber-aligned grads leave the region. Indeed, average advertised salaries on job postings indicate that the national capital region has lower salaries that peer metros of San Francisco, New York, Boston, and Seattle, as seen in Figures 23 and 24 above.

Cybersecurity Has Better Representation of Women and People of Color Than Tech Overall, But is Below Parity with the Full Maryland and DC Workforce

Like the overall U.S. workforce, the workforce in Maryland is split roughly evenly between men and women. In the tech sector, however, there is a stark divide, with women holding 33 percent of jobs to men's 67 percent. The cybersecurity workforce has slightly better representation of women than the tech sector overall, with 35 percent of jobs held by women and 65 percent held by men. Notably, women are represented over par as Cyber Security Consultants. The cybersecurity occupations with the next-highest female share are Cyber Security Analyst, IT Auditor, and Cyber Security Technician / Analyst.

Figure 29. Gender Representation in Cybersecurity, Tech Overall, and the Maryland and DC Region Overall, Maryland and DC, 2023

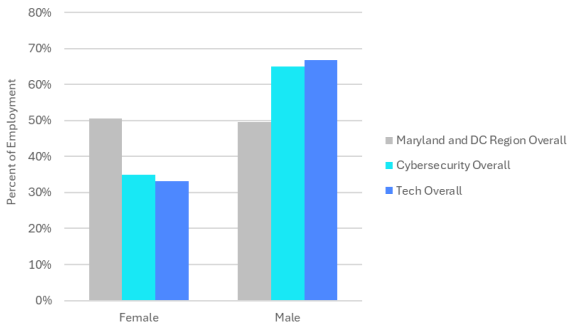
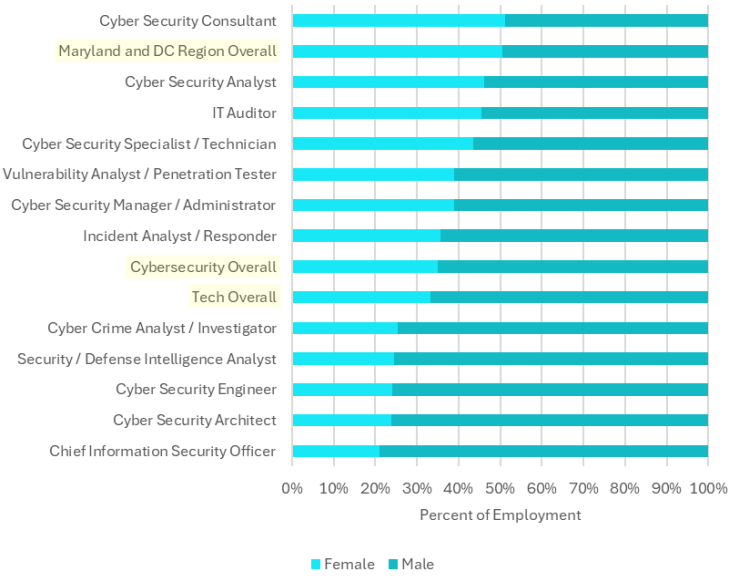


Figure 30. Gender Representation in Cybersecurity, Tech Overall, and the Maryland and DC Region Overall, by Occupation, Maryland and DC, 2023



With respect to race and ethnicity, compared to the overall workforce in Maryland and DC, the cybersecurity sector has similar shares of Asian workers (7 percent), Black workers (28 percent), White workers (52 percent in the region overall, 53 percent in cybersecurity), and workers of other or two or more races (3 percent in the region overall,

4 percent in cybersecurity). The cybersecurity sector has a slightly smaller share of Hispanic workers (9 percent in the region overall, 7 percent in cybersecurity). The tech sector overall has a much higher concentration of Asian workers, which leads to underrepresentation among Black workers and Hispanic workers, but unlike the overall tech sector, the cybersecurity sector does not have a disproportionately high concentration of Asian workers.

Many cybersecurity occupations have a higher share of workers of color than the Maryland and DC region overall. These occupations include Cyber Security Analyst, Vulnerability Analyst / Penetration Tester, Cyber Security Specialist / Technician, and Cyber Security Manager / Administrator. Notably, the most-senior occupation, Chief Information Security Officer, has a lower level of representation of people of color.

Figure 31. Race/Ethnicity Representation in Cybersecurity, Tech Overall, and the Maryland and DC Region Overall, Maryland and DC, 2023

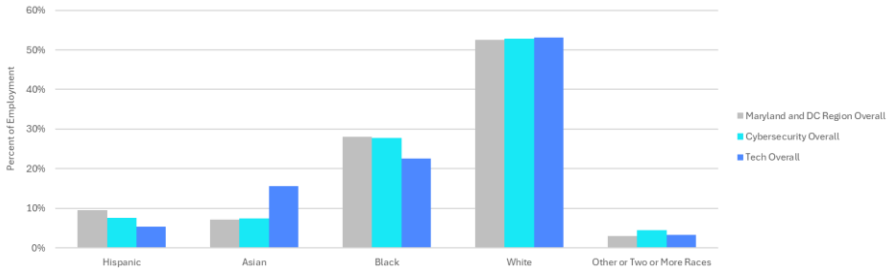
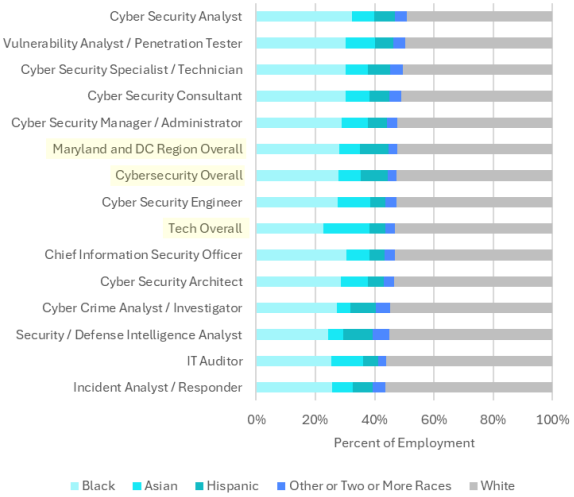
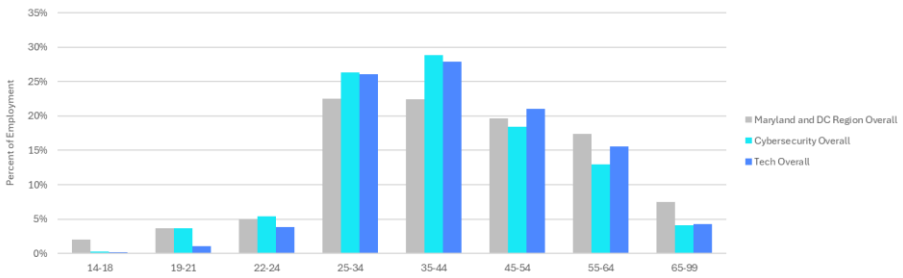


Figure 32. Race/Ethnicity Representation in Cybersecurity, Tech Overall, and the Maryland and DC Region Overall, by Occupation, Maryland and DC, 2023



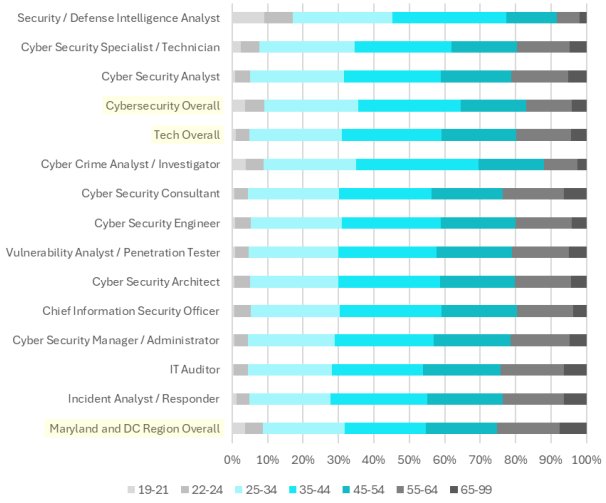
Because of the age dynamics within the cybersecurity workforce, the sector is well positioned to weather the demographic pressures of an aging workforce. The cybersecurity sector has a high share of workers in the 19-44 age category. Nearly two-thirds (64 percent) of the cybersecurity workforce are between the ages of 19-44, compared to 59 percent in the tech sector overall and 54 percent in the Maryland and DC workforce overall.

Figure 33. Age Representation in Cybersecurity, Tech Overall, and the Maryland and DC Region Overall, Maryland and DC, 2023



Once again, Cyber Security Analyst and Cyber Security Specialist / Technician appear on the list of occupations with more forward-looking demographic trends, as these occupations have a younger set of incumbent workers than other occupations in the cybersecurity sector.

Figure 34. Age Representation in Cybersecurity, Tech Overall, and the Maryland and DC Region Overall, by Occupation, Maryland and DC, 2023



Recommendations

Cyber Maryland aims to ensure collaboration between industry, education, and government by using the Talent Pipeline Management (TPM) approach. The TPM approach was developed by the U.S. Chamber of Commerce Foundation as a broadly applicable strategy to close talent gaps in any region, industry, or sector. The approach applies principles from supply chain management in manufacturing and logistics to the cultivation of talent pipelines. The Cyber Maryland board has adopted the TPM approach for closing the talent gaps in the cybersecurity sector.

The TPM approach has six strategic pillars:

1. **Organize for Employer Leadership and Collaboration**

   Employer collaboratives come together to identify common workforce needs and challenges. By collaborating, these employers can create a more unified and powerful voice in articulating their needs to education and training providers.

2. **Project Critical Job Demand**

   This involves identifying the specific skills, competencies, and credentials required for success in their industry. Demand planning allows employers to communicate more effectively with education and workforce partners about the precise nature of their workforce requirements.

3. **Align and Communicate Job Requirements**

   Clear communication of competency and credential requirements to educational institutions and training providers ensures that the curriculum and training programs are aligned with the needs of employers, increasing the likelihood that graduates will possess the skills and knowledge that employers value and ultimately land jobs in the target areas.

4. **Analyze Talent Supply**

   Mapping the pathways through which talent moves from education and training programs into employment highlights the most reliable sources of new talent and elucidates where bottlenecks or inefficiencies exist.

5. **Build Talent Supply Chains**

   Create or expand structured partnerships and collaborations between employers and education or training providers.

6. **Engage in Continuous Improvement**

   The TPM approach is inherently iterative. Stakeholders regularly review and adjust their strategies based on performance data, changing workforce needs, and feedback from partners in the ecosystem.

Lightcast has structured the recommendation section in accordance with those six pillars.

1. Organize for Employer Leadership and Collaboration

The Maryland and DC region is particularly well suited for employer collaboratives because a large share of cybersecurity employment and demand comes from a small number of government contractors and public sector agencies. Based on the above research, it could make sense to have employer collaboratives by sector: public sector agencies, government contractors, and a third collaborative for all other private industries.

- Public Sector Collaborative. The public sector collaborative could standardize hiring practices and hiring needs across agencies. There is already some precedence for this, with the job-leveling and career-pathing frameworks that OPM has produced (see pg. 26). Public agencies are also uniquely able to pool resources for workforce development, as many agencies share a central budget.

Finally, public sector agencies could collaborate on ways to streamline clearance processes or develop access areas for non-cleared individuals.

- Government Contractors Collaborative. The government contractors collaborative could provide recommendations for aligning with federal requirements or modifying procurement in a way that would enable them to better invest in their cybersecurity workforce. Ascribing a collective voice to the large government contractors in the region would enhance their policy advocacy. Government contractors could share best practices around new technologies and new training. Also, by grouping government contractors together, it could be easier to coordinate their investments into important workforce development programming such as registered apprenticeships, sponsoring individuals for security clearances, and developing on-the-job training.
- Other Private Industry Collaborative. There are many other industries in the Maryland and DC region with cybersecurity needs: healthcare employers, financial services employers, professional services employers, and more. This collaborative could be the most cross-functional. These industries share the challenge of competing for cybersecurity talent against government contractors.

2. Project Critical Job Demand

The supply-demand assessment in this report serves as a strong projection of critical job demand. The Maryland and DC region is short 6,500 cybersecurity workers, or 15,000 if Virginia is included in the labor shed. The region has the highest demand in the country, and the pace of demand has been steady for the last five years (excepting a dip during the Covid-19 pandemic).

Demand is greatest and supply shortages are most acute in technical, cyber-forward roles, such as Cyber Security Analyst, Cyber Security Engineer, Security / Defense Intelligence Analyst, and Cyber Security Specialist / Technician, as well as cybersecurity implementer roles including Network Engineer / Architect, Software Developer /

Engineer, Systems Engineer, Systems Administrator, IT Specialist / Engineer, and Network Analyst / Specialist.

Job demand is also high for workers with security clearances. Nearly half of cybersecurity vacancies require a clearance, including 15 percent of cybersecurity demand requiring the Secret Clearance level (which takes 1-2 months to acquire), 9 percent of demand at the Top Secret Clearance level (6-8 months), and 33 percent of demand at the TS/SCI Clearance level (8-15 months). Multiplying out the shortage of clearance-level workers by the average time it takes to earn a clearance, the clearance-related delay could be as high as 2,500 person-years for the Maryland and DC region (5,800 person-years if Virginia is included as well). Because this is such a steep delay, it is paramount to tap into sources of workers with existing clearances, reduce clearance requirements where possible, and organize workflows in a way that allows non-cleared individuals to contribute to cybersecurity-related work while their clearances are being processed.

3. Align and Communicate Job Requirements

The above research surfaced a number of focus areas for aligning job requirements.

Public-private knowledge share on reducing degree requirements

Government contractors and other private sector employers should take note of how the public sector has reduced degree requirements for cybersecurity jobs. The private sector consistently requests higher levels of educational attainment, even for the same jobs. If the Maryland and DC region organizes employer collaboratives for public sector employers, government contractors, and other private sector employers, the public sector collaborative could develop a set of strategies to share with their peers in the other collaboratives to reduce the reliance on degrees.

Reverse the double mandate of a degree plus a certification

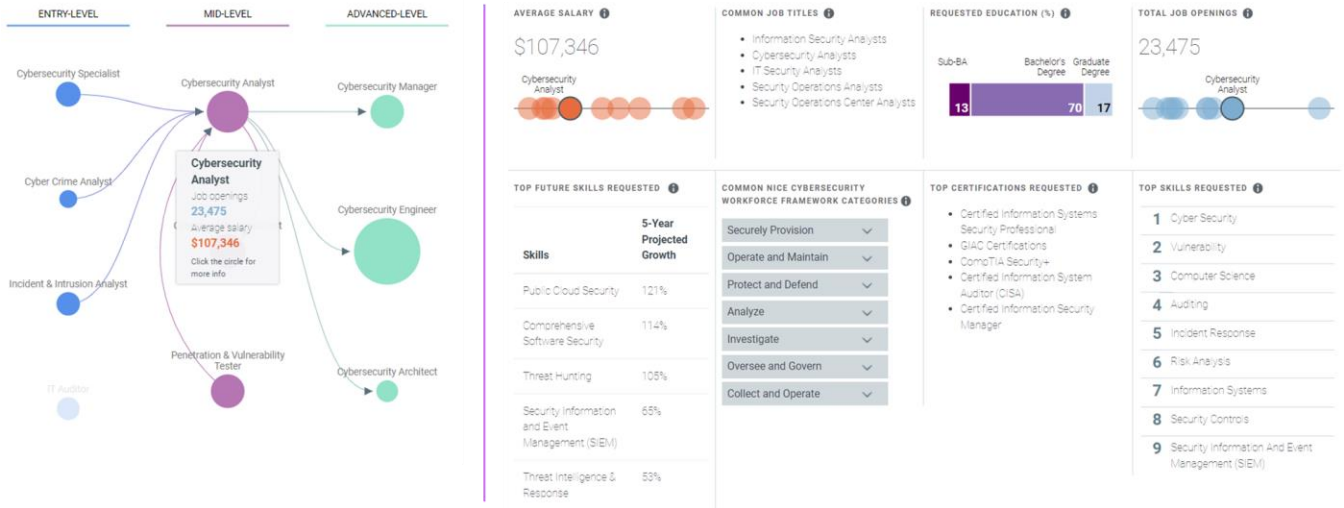
Employers can move to substitute certifications and non-degree credentials for degrees in the hiring process. Currently, employers tend to request certifications in addition to

degrees, rather than as an alternative to degrees. But the certification curriculum is designed to be comprehensive with respect to the occupations that the certification targets. One straightforward rule could be to review degree requirements anywhere a certification is requested and determine what additional requirements would be needed to remove the degree from that listing.

Share cybersecurity workforce data with jobseekers, educators, and industry

The Maryland and DC region can develop a centralized resource for cybersecurity workforce information. This resource can include role titles and descriptions, career pathways, data on the supply and demand of cybersecurity talent, and training opportunities. The portal could look like a state-specific version of CyberSeek.org, or a similar platform.

Figure 35. Cybersecurity Workforce Platform, CyberSeek.org



4. Analyze Talent Supply

At the bachelor's and above level, the talent pipeline is concentrated at a small number of institutions. At the bachelor's level, the primary sources are the University of Maryland (including the Global Campus, though those graduates are often not local) and Towson University. At the above-bachelor's level, George Washington University and the SANS Institute of Technology are also standouts.

Table 12. Average Annual Completions from Cyber-Aligned Programs at the Bachelor's Degree Level and Above, by Award Level and Institution, Maryland and DC, 2019-2023

Award Level	Institution Name	Cyber-Forward Completions	Downstream Cybersecurity Implementers Completions	Total Completions [min. 25]
Bachelor's Degree	University of Maryland-College Park	38	860	898
	Towson University	23	315	339
	University of Maryland Global Campus	191	141	332
	University of Maryland-Baltimore County	13	303	316
	George Washington University	32	78	111
	Howard University	2	89	91
	United States Naval Academy	4	69	73
	Frostburg State University	14	48	62
	Georgetown University	2	46	48
	University of the District of Columbia	3	38	41
	Strayer University-Global Region	3	37	41
	Capitol Technology University	17	18	35
	Strayer University-Maryland	3	30	33
BA+ degree or cert.	George Washington University	94	233	327
	University of Maryland-College Park	13	181	195
	SANS Technology Institute	90	66	157
	Towson University	21	118	139
	University of Maryland-Baltimore County	3	75	78
	Capitol Technology University	39	39	78
	Johns Hopkins University	43	32	76
	Georgetown University	26	41	67
	Hood College	18	23	41

At the sub-bachelor's level, the supply of completers is more evenly distributed across a wider range of institutions. In particular, at the associate's degree level, institutions with the highest throughput include Baltimore County Community College, Prince George's Community College, Anne Arundel Community College, Montgomery College, and Howard Community College. At the certificate level, institutions with the highest

throughput include Anne Arundel Community College, Frederick Community College, the SANS Technology Institute, and Baltimore City Community College.

Table 12. Average Annual Completions from Cyber-Aligned Programs at the Associate's Degree Level and Below, by Award Level and Institution, Maryland and DC, 2019-2023

Award Level	Institution Name	Cyber-Forward Completions	Downstream Cybersecurity Implementers Completions	Total Completions [min. 25]
Sub-AA award	Anne Arundel Community College	97	83	180
	Frederick Community College	16	55	71
	SANS Technology Institute	36	27	63
	Baltimore City Community College	23	38	61
	College of Southern Maryland	21	27	48
Associate's Degree	Community College of Baltimore County	40	72	112
	Prince George's Community College	27	85	112
	Anne Arundel Community College	47	52	100
	Montgomery College	46	34	79
	Howard Community College	0	70	71
	Harford Community College	18	41	59
	Baltimore City Community College	17	41	58
	College of Southern Maryland	22	30	52
	Hagerstown Community College	13	22	34
	Carroll Community College	13	18	31

Lightcast also reviewed cybersecurity education at institutions outside of colleges and universities. This list of providers includes Baltimore Cyber Range, Per Scholas, NPower, Urban Geeks, Cybrary, the National Cyber League, Practical IT, and more. This talent pipeline can produce up to 1,350 trained workers a year, though due to attrition this figure is an upper bound.

5. Build Talent Supply Chains

This section outlines a number of strategies that stakeholders in Maryland and DC can take to build the talent pipeline.

Increase the number of registered apprenticeships for cybersecurity

The Maryland General Assembly established the Apprenticeship 2030 Commission to make recommendations to the state legislature about how apprenticeships can be used to reduce skill shortages in high-demand occupations. The Commission recommends strategies to achieve two goals: reaching 60,000 registered apprenticeships across Maryland by 2030, and having 45 percent of public high school students complete the high school level of a registered apprenticeship or industry-recognized credential by the time of graduation, beginning in the 2030-31 school year.

Cyber Maryland or other cybersecurity stakeholders could offer capacity building to support employers registering for apprenticeships. The process is lengthy, but there are many resources specifically related to cybersecurity that make the process easier. For example, employers must develop a program framework that outlines the competencies required for the role. For cybersecurity roles, though, employers can borrow from the NICE Framework and the occupation frameworks developed by OMB to satisfy this requirement. Additionally, employers often do not have the capacity to host multiple apprentices. But in the Maryland and DC cybersecurity sector, a large share of demand is concentrated among a small number of government contractors. These contractors would have the capacity for larger apprentice cohorts. Finally, employers can sometimes struggle to get the word out about their apprenticeship opportunities, but in the cybersecurity sector there is a robust network of local partners that can support that effort.

In focus group sessions, participants recommended a concerted effort to rebrand apprenticeships as relevant to the work of the future and appropriate for “white collar” jobs like cybersecurity positions. Changing the perception of apprenticeships as outdated or “blue collar” can happen in tandem with the efforts to expand the

apprenticeship pipeline. Naming the apprenticeships cyber-apprenticeships can mark these opportunities as high-tech. Public awareness campaigns could include collaborations with influencers or partnerships with recognizable high-tech firms. Finally, highlighting success stories around cyber-apprenticeships completers could improve the perception of these programs.

Increase funding for cybersecurity-related training, scholarships, and grants

The cost of cybersecurity training can range from $1,000 - $5,000 per student, depending on a number of features including the student's previous experience with computing, the services delivered, the cost of any certifications earned, the length of the programming, and other features. The primary funding mechanism for cybersecurity training in Maryland is the Maryland Department of Labor's Employment Advancement Right Now (EARN) Maryland program. Most recently, the program announced the ability to train 700 Marylanders with $2 million in grant funding, or approximately $2,900 per participant.[21] In the case of organizations like that provide additional support such as career coaching, mentorship, social and emotional support, and other services, the cost per student can increase substantially.

The cost to train enough workers to satisfy the immediate need for entry-level cybersecurity workers in Maryland and DC (2,000 vacancies) would be approximately $6 million. That investment would still leave 4,500 vacancies unfilled, and it assumes that nearly all of those locally trained individuals remain in the Maryland and DC area.

The funding gap can be filled through a variety of mechanisms. The EARN Maryland program was celebrated by focus group participants. Expanding EARN Maryland and increasing its emphasis on cybersecurity would alleviate talent gaps.

Focus group participants also explained that many community college programs are funded through time-limited grants. The time-boundedness can make it difficult to sustain funding over the lifetime of the program and impedes future-forward investments

[21] A press release distributed through I95 Business can be read here: https://i95business.com/releases/5629

in tools and technology to keep pace with the changing cybersecurity landscape. Increasing the dedicated and regular funding to cybersecurity programs community colleges could also alleviate talent gaps. Community colleges with strong cybersecurity programs are identified in the previous section.

Because of the emphasis that employers place on work experience when hiring for cybersecurity roles, focus group participants also highlighted the success of cyber ranges. Cyber ranges develop interactive, simulated representations of an organization's local network, system, tools, and applications, and they are used for cybersecurity training and software testing. They provide a safe, controlled environment for hands-on cybersecurity education, allowing individuals to practice attack mitigation, system hardening, and response strategies without the risk of impacting real-world networks. Developing cyber ranges involves a large initial capital investment. Grant funding for such investments could increase the number of cyber ranges in the Maryland and DC region.

Expand staffing practices to accommodate less-experienced workers

Employers could develop and staff junior-level positions for some of the most in-demand occupations. A junior-level role could be relevant for Cyber Security Analyst, Cyber Security Specialist / Technician, Software Developer / Engineer, Systems Administrator, IT Specialist / Engineer, and Network Analyst / Specialist.

Mentorship programs can be an additional support system for junior-level positions. Mentors provide a risk-free way for junior-level workers to request additional guidance. Mentors can also guide early-career workers into the right sorts of cybersecurity career pathways.

Employers could utilize project-based hiring or temporary hiring as a way to evaluate a candidate's skills and fit for the organization without requiring extensive prior work experience. Staffing firms have a smaller share of demand in the cybersecurity sector in Maryland and DC than in other peer regions such as the Boston or New York metros, but staffing firms often offer this sort of project-based employment.

Employers can commit to hiring a certain number of graduates from training programs that incorporate practical experience.

The public sector can incorporate cybersecurity training into all public-sector roles so that a broader range of individuals have cybersecurity experience. In Massachusetts, everyone with a state-provided email address is required to complete certain cybersecurity trainings. There are additional training programs available for people to opt-into as well. This training introduces cybersecurity to employees who would otherwise have little exposure to the field.

Target workers with security clearances

Another potential talent source, particularly given the requirement for security clearances addressed above, is the corps of servicemembers that are transitioning each year to civilian life. As many as 200,000 individuals navigate this transition each year. The security clearances that they have acquired are valid as they enter civilian life, so this large source of talent would be able to fill clearance-level cybersecurity jobs immediately.

Include cybersecurity in efforts to engage young people in STEM and tech

Schools can incorporate cybersecurity exposure and education into science, tech, and STEM education. One model for this is the GenCyber program. GenCyber runs camps that aim to boost interest and competency in cybersecurity among young people in secondary school. The program is sponsored by the National Security Agency (NSA) and National Science Foundation (NSF).

Implement targeted, occupation-level interventions

Lightcast developed an occupation strategy grid for a selection of the most in-demand occupations. The grid includes the current supply-demand gap alongside the following metrics:

- Throughput: Percent of demand met by the postsecondary system and percent of demand met by the adult education ecosystem.
- Alignment: Retention rate within Maryland and DC for workers who came from local institutions and are now employed in these roles.
- Non-Skill Barriers: The percent of demand requesting a bachelor's degree or above and the percent of demand requesting a security clearance.

Lightcast highlighted cells in red to indicate areas where the supply pipeline could be constrained, based on a threshold score for each column.

Figure 36. Cyber-Forward Occupation Strategy Grid

		Throughput		Alignment	Non-Skill Barriers	
Occupation Name	Supply-Demand Gap	Postsecondary System	Adult Education Ecosystem	Cyber Retention Rate	Percent of Demand BA/BA+	Percent Requesting Clearance
Red Flag:	*>100*	*<25%*	*<25%*	*<50%*	*<75%*	*>50%*
Cyber Security Engineer	604	21%	24%	46%	74%	50%
Cyber Security Analyst	564	24%	38%	67%	70%	52%
Security / Defense Intelligence Analyst	208	0%	17%	63%	68%	59%
Cyber Security Manager / Administrator	160	14%	20%	49%	71%	30%
Vulnerability Analyst / Penetration Tester	159	9%	21%	56%	62%	48%
Cyber Security Specialist / Technician	153	19%	15%	61%	65%	51%
Incident Analyst / Responder	96	10%	20%	56%	63%	44%
Security Manager	53	0%	26%	48%	76%	47%
Cyber Security Architect	52	16%	20%	38%	73%	36%
Security Supervisor	45	0%	15%	80%	74%	57%

All cyber-forward occupations could benefit from an expansion of targeted and aligned postsecondary programming

Existing skills-training organizations could expand their offerings to target the roles highlighted in red.

The Maryland / DC region has a retention issue with these occupations. Build out internships, apprenticeships, or earn-and-learn programs for these occupations to make learners sticky when they graduate.

Engage employers and ind. assocs. on non-degree pathways into these roles.

6. Engage in Continuous Improvement

Lightcast has identified a set of seven cybersecurity workforce health metrics, which can be used for continuous improvement. The metrics and use cases are as follows:

1. Supply/Demand Ratio for cyber-forward and cyber implementer occupations. Over time, the expectation is that the supply/demand ratio should move closer to equilibrium, if interventions to expand the cybersecurity supply pipeline are successful.
2. Ratio of BA/BA+ to Sub-BA Job Postings for cyber-forward occupations. Employers can reduce reliance on degree requirements by substituting them for certifications, implementing skil-based hiring practices, requesting work portfolios, or by engaging more deeply with the education and training system such that they can be sure that individuals coming out of a certain training program are well qualified. Over time, this ratio should decrease.
3. Share of Cyber Postings with Cyber Certification, disaggregated by public sector vs. private sector. Over time, this number should increase as shorter-term, lower-cost certifications are embraced by employers.
4. Rate of Change for Cyber-Aligned Completions vs Cyber Demand, which can be used to monitor whether the supply pipeline is increasing at least at the same pace as any changes on the demand side.
5. Share of Cyber Demand Met by Postsecondary Completers, disaggregated to the sub-BA, BA, and BA+ levels. As the postsecondary pipeline expands, these shares should increase.
6. Race/Ethnicity Representation Ratio, or the percent of non-white/non-Asian cyber-forward workers to that population's share of the overall workforce. This ratio is currently close to parity, and monitoring it over time will ensure that supply pipelines are not biased.
7. Gender Representation Ratio – percent women in cyber-forward workforce to that population's share of the overall workforce. This ratio is currently far from parity, and monitoring it over time will indicate how well women are integrated into the supply pipelines.

www.lightcast.io