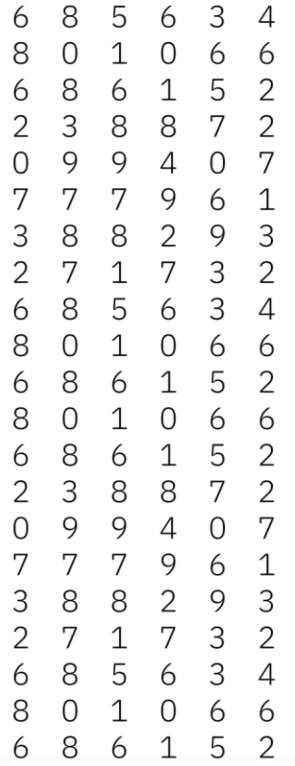
Maryland & DC Cybersecurity Workforce Analysis & Strategy

Action Framework

TEDCO // Lightcast



Agenda

- Review the TPM Framework
- Apply the TPM Framework to the cybersecurity sector in Maryland/DC

Talent Pipeline Management (TPM) Framework

TPM is an *employer-led* framework from the U.S. Chamber

Why use an employer-led framework?

Employers benefit directly from talent pipeline expansion and ultimately determine the success of worker- and learner-level interventions

- Encourages ecosystem buy-in
- Builds on industry best practices
- Generates granular, actionable data on demand
- Provides a structured and agile process for collective action and decision making
- Engages the full spectrum of talent sourcing providers
- Creates shared value, competitiveness, and accountability
- Focused on employer ROI

What is the TPM Framework?

These recommendations will hue to the US Chamber Talent Pipeline Management (TPM) framework for upskilling and reskilling. This framework has 6 pillars:

1. Organize for employer leadership
2. Project critical job demand
3. Create a shared language for hiring requirements
4. Analyze talent supply
5. Build talent “supply chains” (or pipelines)
6. Continuous improvement and resiliency planning

The TPM Framework Also Tees Up Policy

- **Data-driven discoveries *lead to* policy interventions**
  - Skill gaps → Targeted training subsidies
  - Small entry-level pipeline → Apprenticeships
  - In-demand certifications → Workforce development provider portfolio
  - Need for applied skills → Cyber ranges
  - Difficulty hiring for outdated systems → Funding for infrastructure revitalization
  - Clearance issues → Increase processing, streamline processing, change process

- **Sizing pipeline constraints can help *prioritize* policy interventions**
  - Postsecondary gap at the sub-BA level > gap at the BA/BA+
  - Capital region has the largest cyber gap → competitive for federal funding

- TPM helps bridge the gap between employers, education, and policymaking.
  - Within this ecosystem, employers tend to be the largest and most diffuse, which helps make the case for an employer-led framework.

Applying the TPM Framework to the Cybersecurity Sector in Maryland/DC

1. Organize for Employer Leadership

Many options, of which two were considered...

By sector

The report suggested three employer *collaboratives,* organized by sector.

- Public Sector Collaborative
- Government Contractors Collaborative
- Other Private Industry Collaborative

By working-group issue area

Cyber Maryland has developed summer 2024 *workgroups*:

- Apprenticeships, Internships, and Work Learning
- Skills-based Hiring
- Evolving Cybersecurity Education and Training
- Cyber Workforce Data Collection and Metrics

2. Project 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).

`Second` in the Size of the Talent Gap

State Name	Talent Gap
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

`Sixth to Last` in the Ratio of Supply-Demand

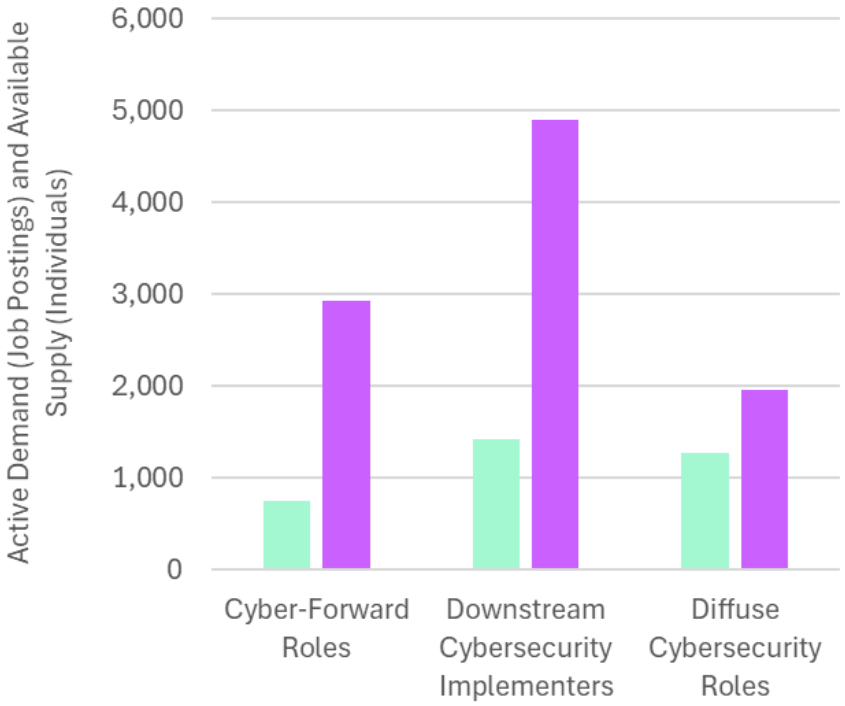
State Name	Share of Demand Met by Supply
Vermont	23%
Alaska	24%
Rhode Island	30%
North Dakota	32%
Nebraska	33%
Maryland and DC	33%
South Dakota	33%
Wyoming	34%
Hawaii	35%
New Mexico	35%

2. Project Critical Job Demand

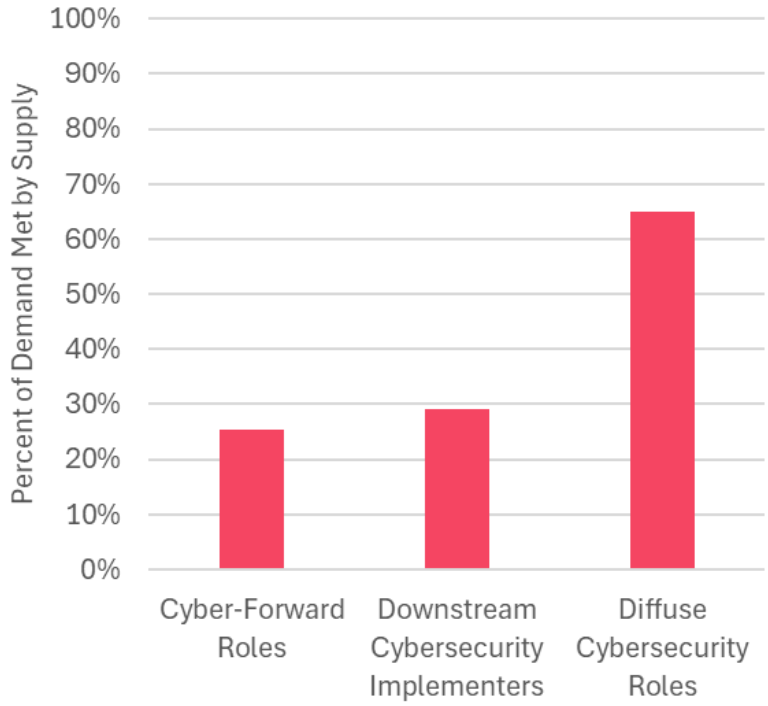
- Cybersecurity skills exacerbate talent gaps in IT jobs

Cybersecurity Employment

Supply and Demand



Percent of Demand Met by Supply



2. Project Critical Job Demand

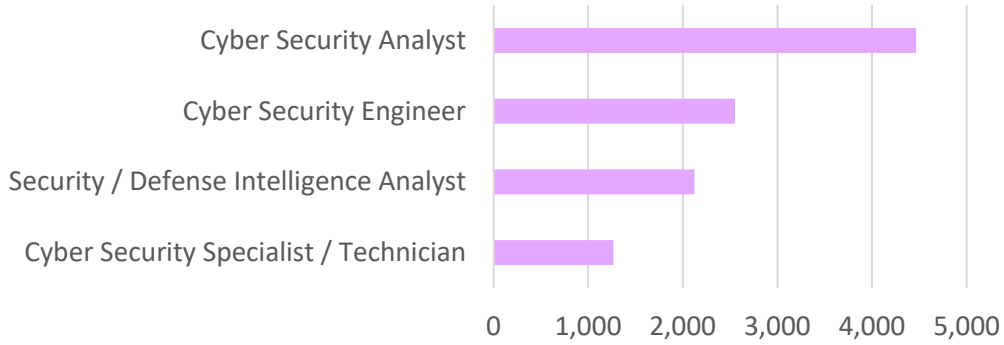
- Demand is greatest and supply shortages most acute in technical, **cyber-forward** roles

  Cyber Security Analyst
  Cyber Security Engineer
  Security / Defense Intelligence Analyst
  Cyber Security Specialist / Technician

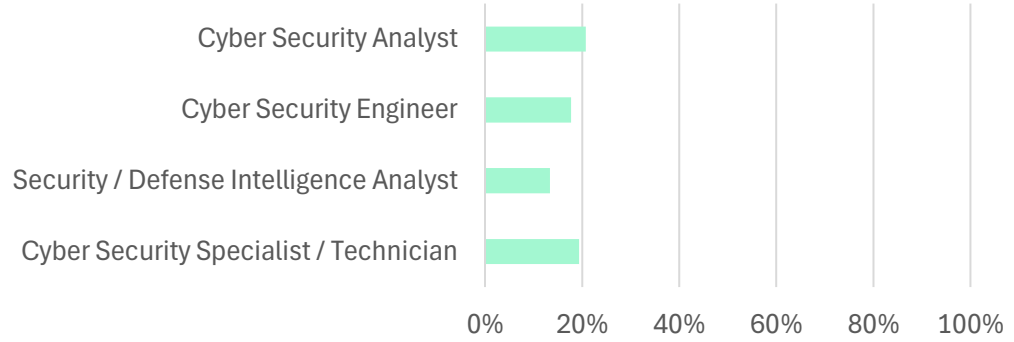
- And **cybersecurity implementer** roles

  Network Engineer / Architect
  Software Developer / Engineer
  Systems Engineer
  Systems Administrator
  IT Specialist / Engineer
  Network Analyst / Specialist

Cyber Employment by Occupation Category

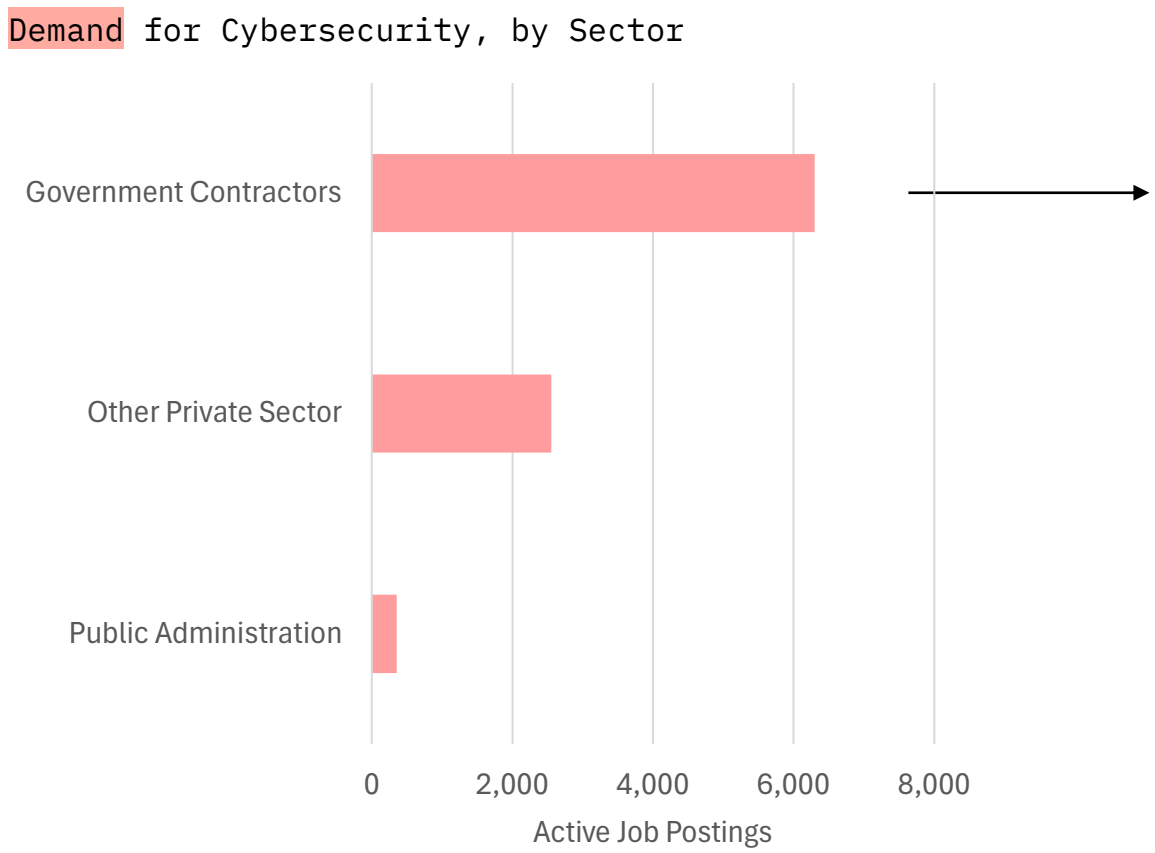


Percent of Demand that can be Met by Available Supply



2. Project Critical Job Demand

- Government contractors drive much of cybersecurity demand

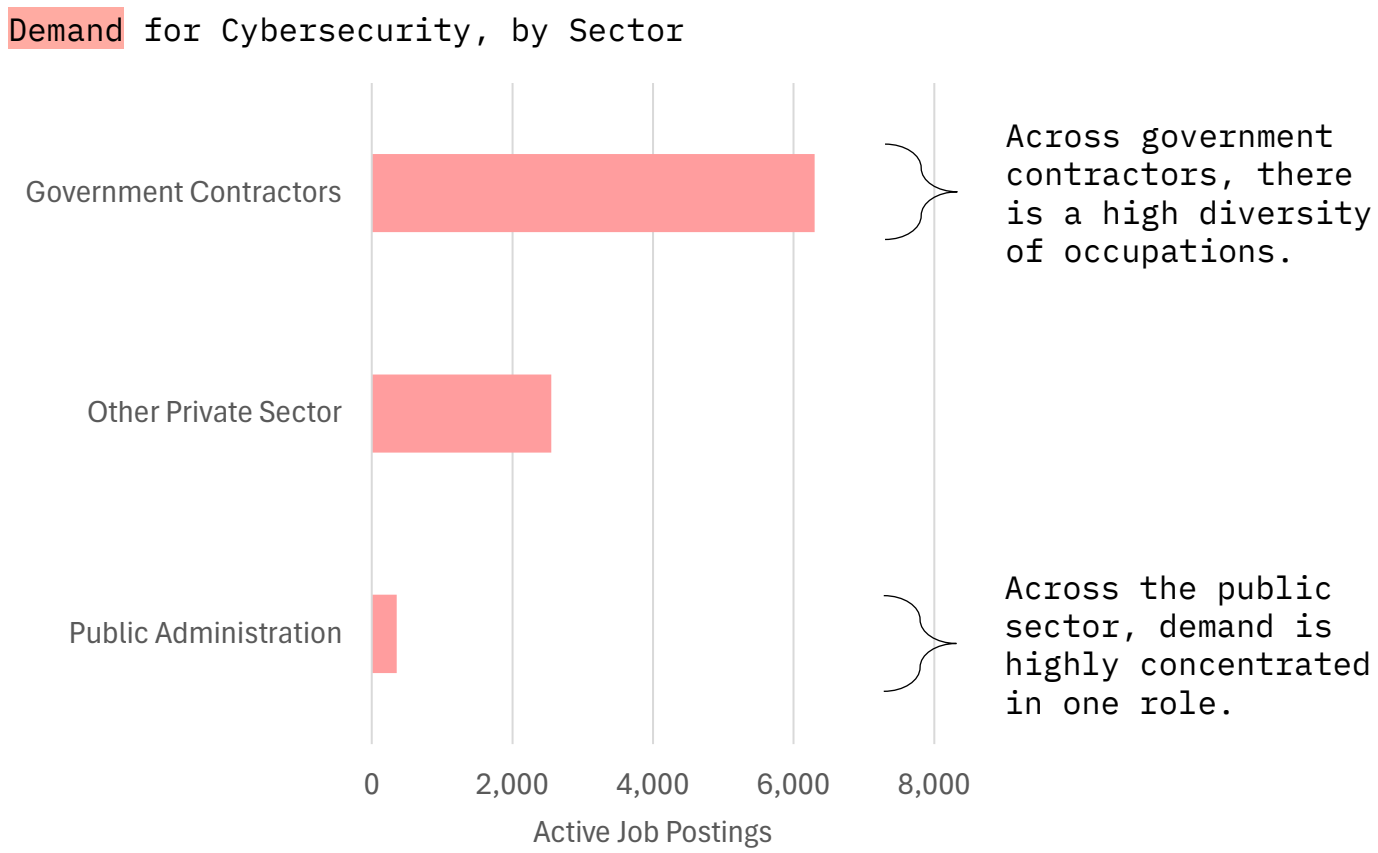


Postings (2019-2023) for cybersecurity, by Contractor Name

Employer Name	Demand (5yrs)
Leidos	10,704
General Dynamics	6,844
Booz Allen Hamilton	4,770
CACI International	3,179
Northrop Grumman	3,016
Deloitte	2,936
Guidehouse	2,765
SAIC	2,683
ManTech	2,581
Lockheed Martin	2,559
Kforce	1,454
Raytheon Technologies	1,374
Parsons	1,285
Accenture	1,283
Jacobs Engineering Group	1,223
IBM	1,110
Randstad	1,105
BAE Systems	945
Johns Hopkins	935
Mindpoint Group	853

2. Project Critical Job Demand

- And government contractors hire for a different profile of occupations



Occupation Name	Share of Cyber Demand in Gov. Contractors Sector
Cyber Security Engineer	8%
Cyber Security Analyst	7%
Network Engineer / Architect	5%
Software Developer / Engineer	4%
Systems Engineer	3%
Cyber Security Manager / Administrator	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 Specialist / Technician	4%
Cyber Security Manager / Administrator	4%
Cyber Security Engineer	3%
Security / Defense Intelligence Analyst	3%
Contracts Analyst	2%
Other Occupations	50%

2. Project Critical Job Demand

- 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).

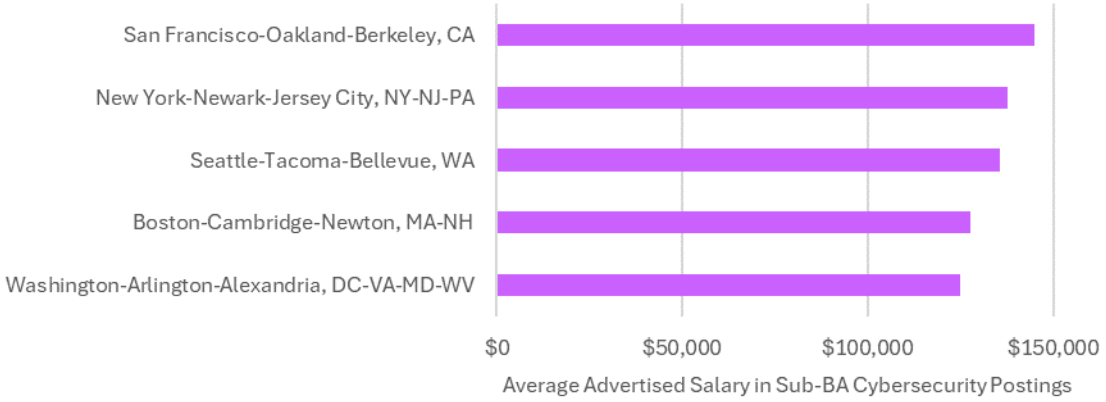
- Multiplying out the shortage of clearance-level workers by the average time it takes to earn a clearance, the clearance-related delay could be as high as 2,500 person-years for the Maryland and DC region (5,800 person-years if Virginia is included as well).

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%

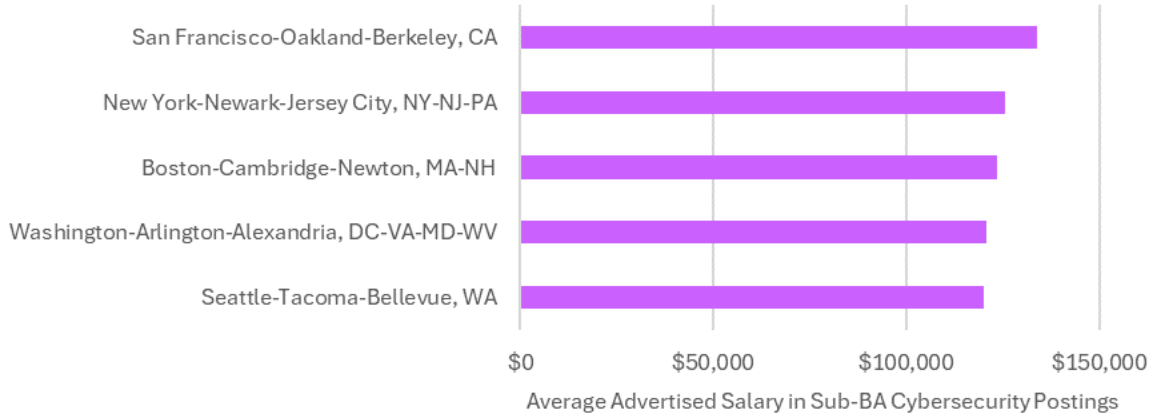
2. Project Critical Job Demand

- Cybersecurity skills command salary premia, but salaries are lower in Maryland and DC than in peer markets.

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



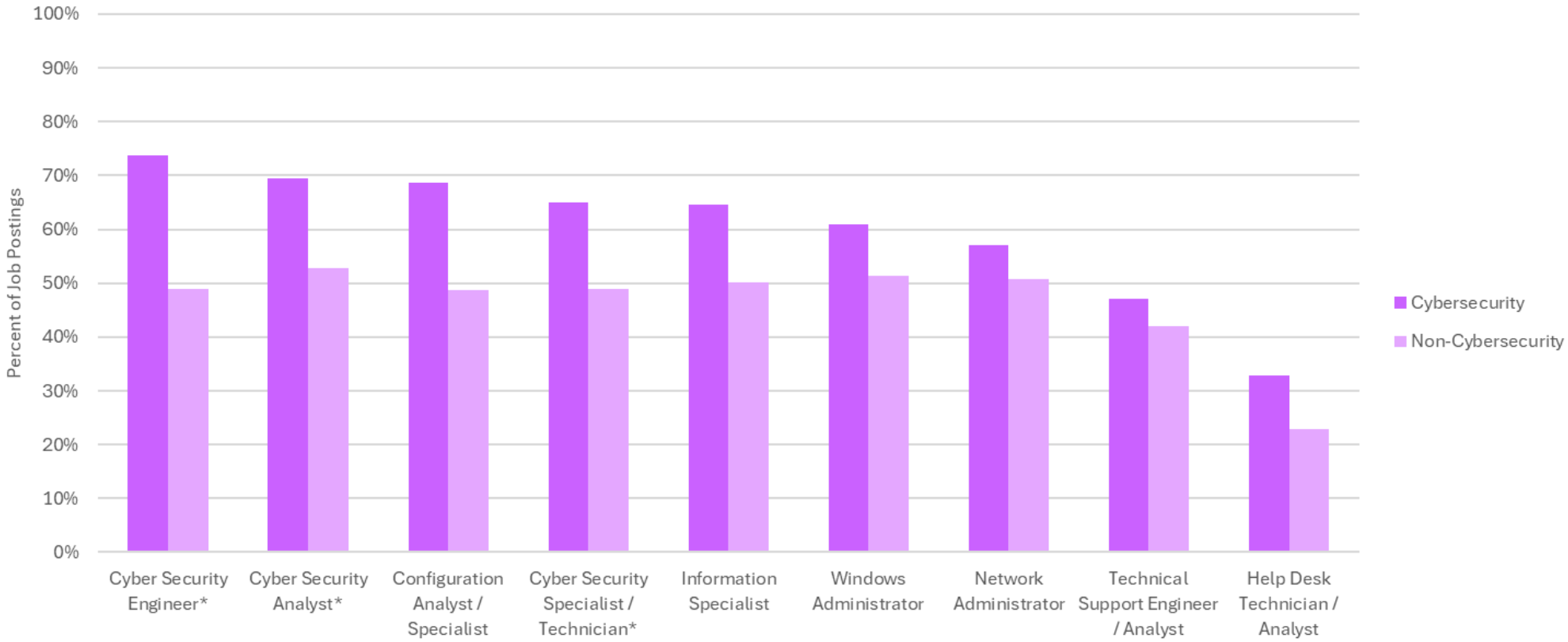
Average Advertised Salary in Cybersecurity Job Postings at the Sub-Bachelor's Level, by Metro Region, 2021-2023



3. Create a Shared Language for Hiring Requirements

- Degree inflation in cybersecurity roles contributes to talent gaps

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

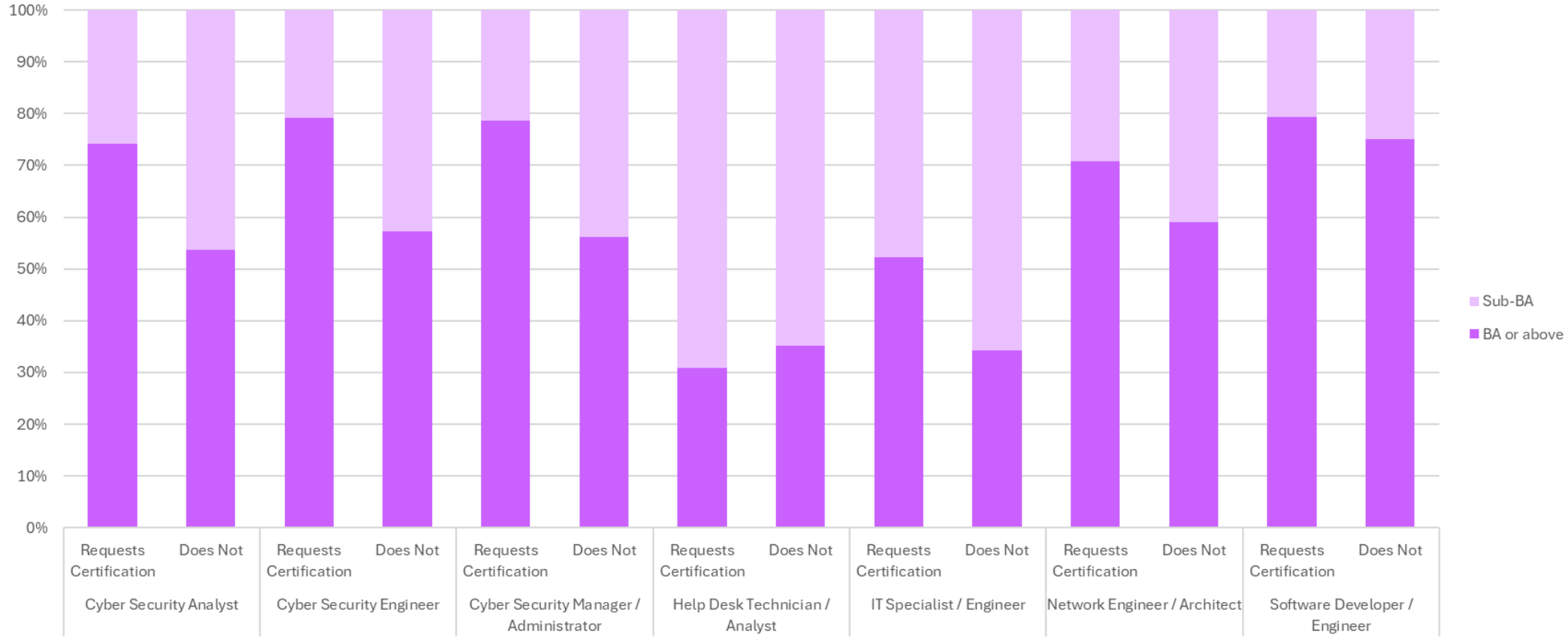


* The starred occupations only ever reference cybersecurity skills, as their job title suggests. For these occupations, an alternative non-cyber occupation was used for the comparison: Cyber Security Engineer used IT Specialist / Engineer, Cyber Security Analyst used ERP Analyst, and Cyber Security Specialist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

3. Create a Shared Language for Hiring Requirements

- There is a tension between degrees and certifications in cybersecurity – currently, certifications are associated with higher degree requirements.

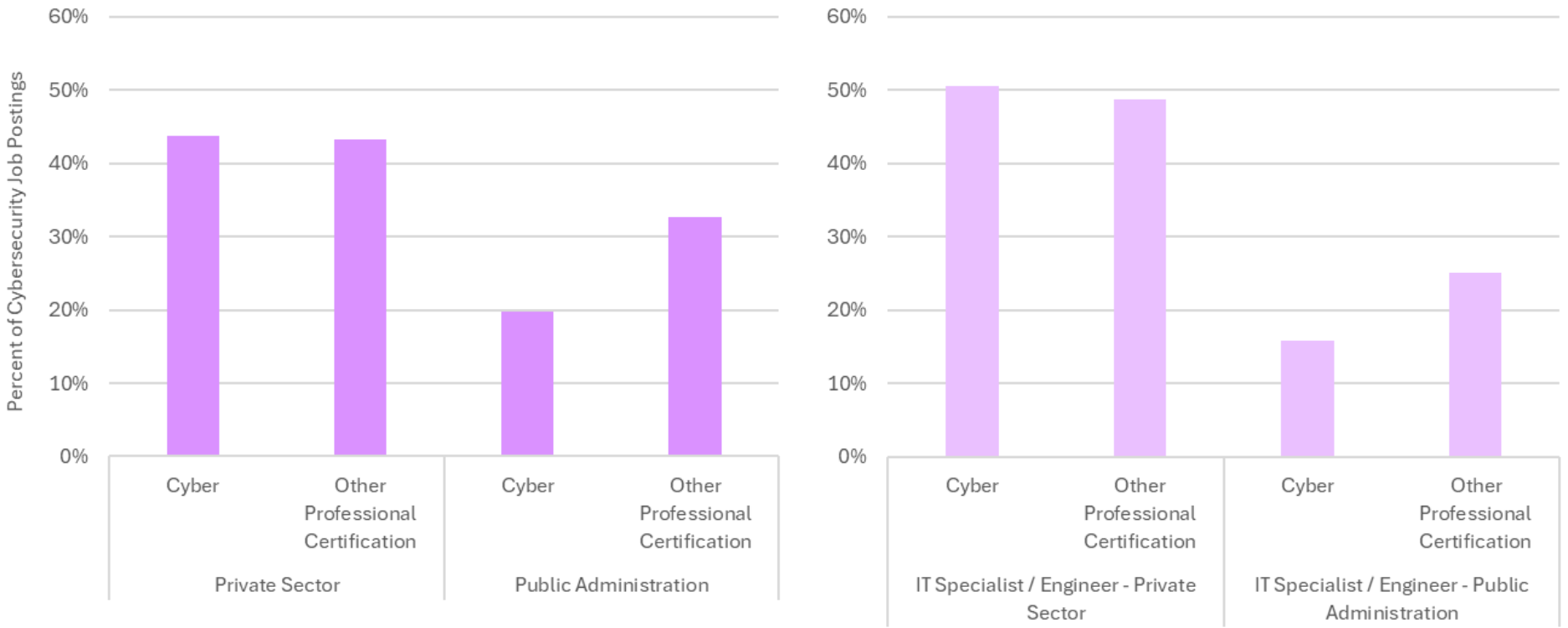
Education Requested in Job Postings, Disaggregated by Whether the Job Posting Requests a Certification, Maryland and DC, 2021-2023



3. Create a Shared Language for Hiring Requirements

- Public sector employers have *lower* degree requirements but also lean on certifications *less often*

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



3. Create a Shared Language for Hiring Requirements

- Experience is the truest measure of readiness but the most difficult to acquire

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

4. Analyze Talent Supply

- At the bachelor's and above level, the talent pipeline is concentrated at a small number of institutions.

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 Completion [min. 25
Bachelor's Degree	University of Maryland-College Park	38	860	89
	Towson University	23	315	33
	University of Maryland Global Campus	191	141	33
	University of Maryland-Baltimore County	13	303	31
	George Washington University	32	78	11
	Howard University	2	89	9
	United States Naval Academy	4	69	7
	Frostburg State University	14	48	6
	Georgetown University	2	46	4
	University of the District of Columbia	3	38	4
	Strayer University-Global Region	3	37	4
	Capitol Technology University	17	18	3
	Strayer University-Maryland	3	30	3
BA+ degree or cert.	George Washington University	94	233	32
	University of Maryland-College Park	13	181	19
	SANS Technology Institute	90	66	15
	Towson University	21	118	13
	University of Maryland-Baltimore County	3	75	7
	Capitol Technology University	39	39	7
	Johns Hopkins University	43	32	7
	Georgetown University	26	41	6
	Hood College	18	23	4

4. Analyze Talent Supply

- At the sub-bachelor's level, the supply of completers is more evenly distributed across a wider range of institutions.
- Lightcast also reviewed cybersecurity education at institutions outside of colleges and universities and estimates that this talent pipeline can produce up to 1,350 trained workers a year.

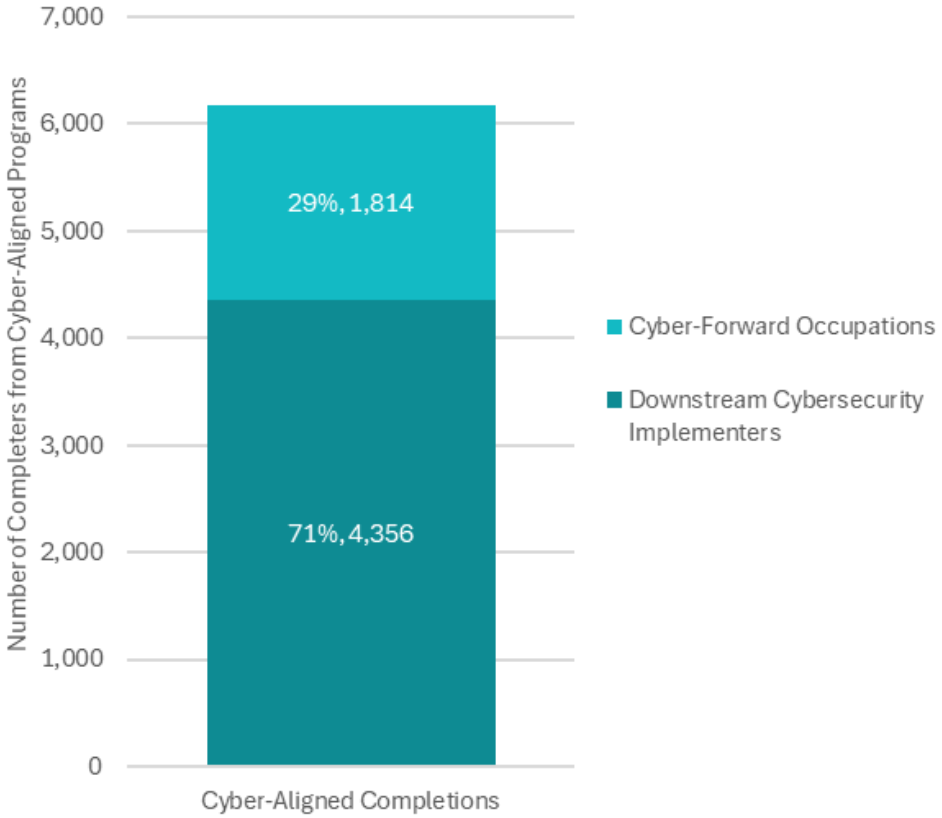
Average Annual Completions from Cyber-Aligned Programs at the Associate's Degree Level and Below, by Award Level and Institution, Maryland and DC, 2019-2023

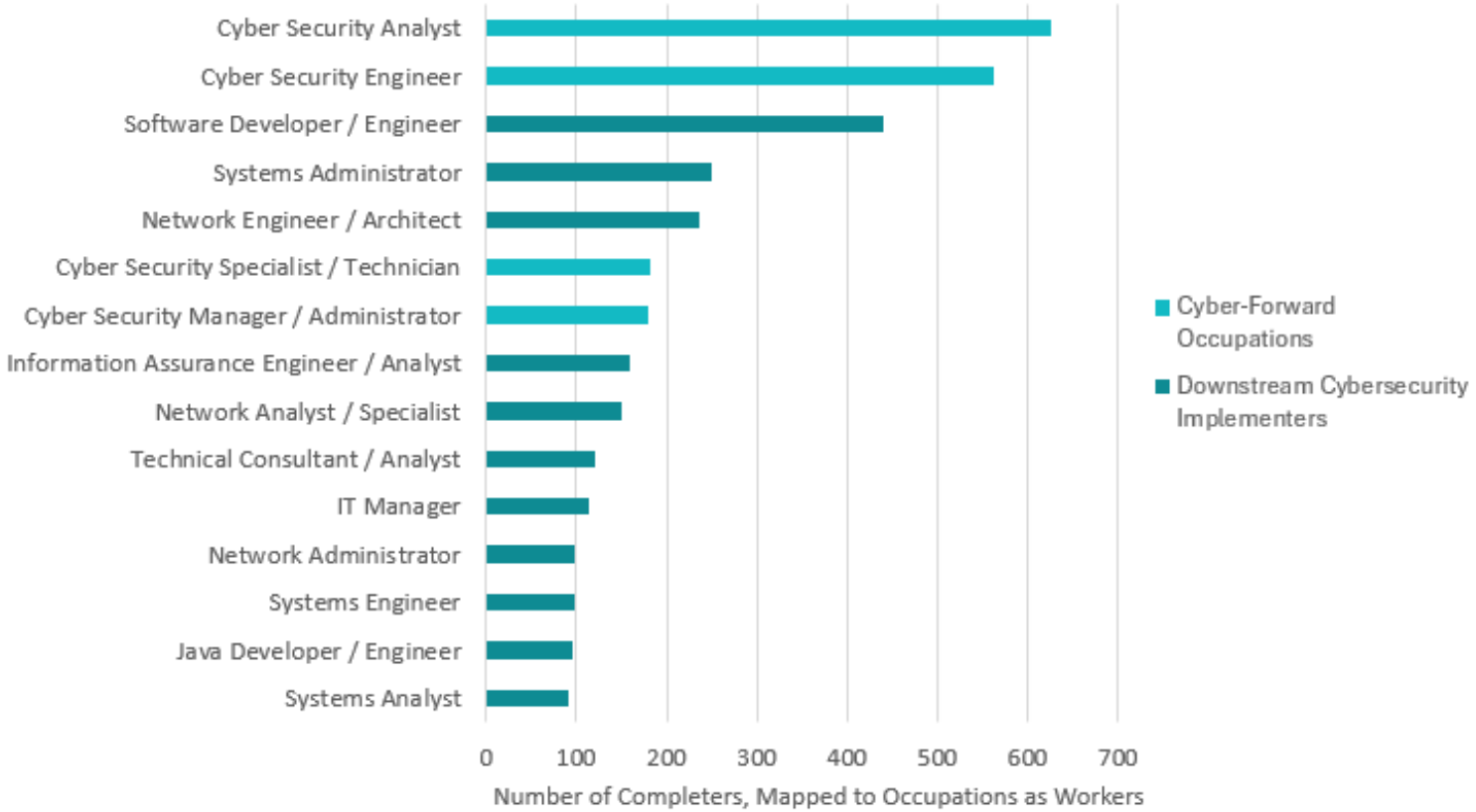
Award Level	Institution Name	Cyber-Forward Completions	Downstream Cybersecurity Implementers Completions	Total Completion [min. 25
Sub-AA award	Anne Arundel Community College	97	83	18
	Frederick Community College	16	55	7
	SANS Technology Institute	36	27	6
	Baltimore City Community College	23	38	6
	College of Southern Maryland	21	27	4
Associate's Degree	Community College of Baltimore County	40	72	11
	Prince George's Community College	27	85	11
	Anne Arundel Community College	47	52	10
	Montgomery College	46	34	7
	Howard Community College	0	70	7
	Harford Community College	18	41	5
	Baltimore City Community College	17	41	5
	College of Southern Maryland	22	30	5
	Hagerstown Community College	13	22	3
	Carroll Community College	13	18	3

4. Analyze Talent Supply

- Cyber-aligned grads often choose less cyber-aligned careers

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

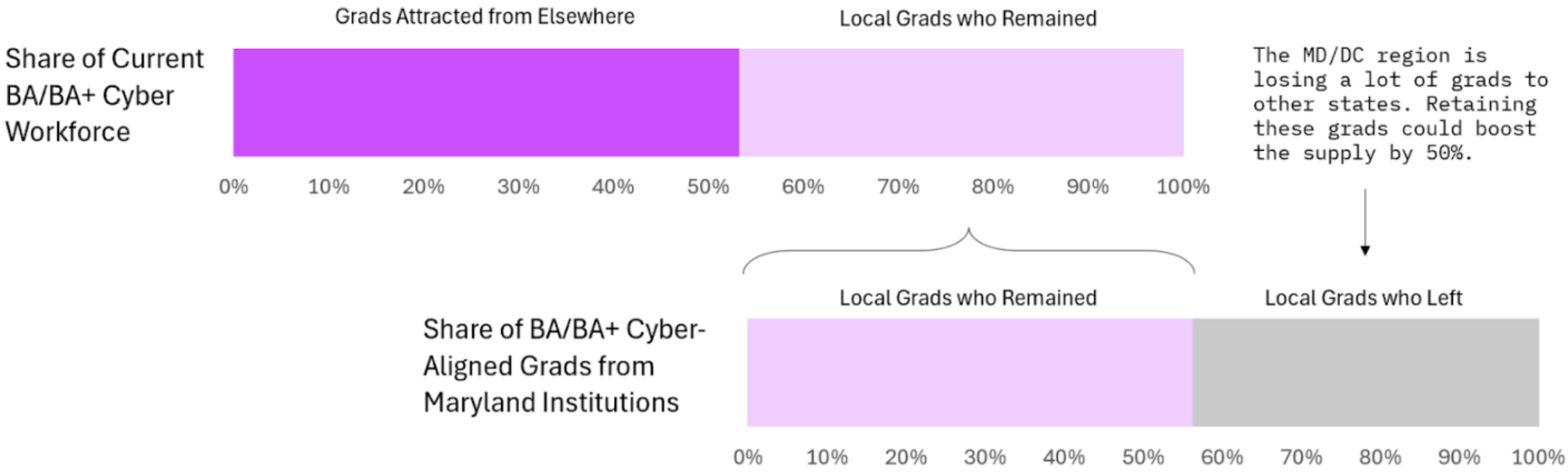




4. Analyze Talent Supply

- Strong attraction of cyber-aligned grads from outside the region, but brain drain locally

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



4. Analyze Talent Supply

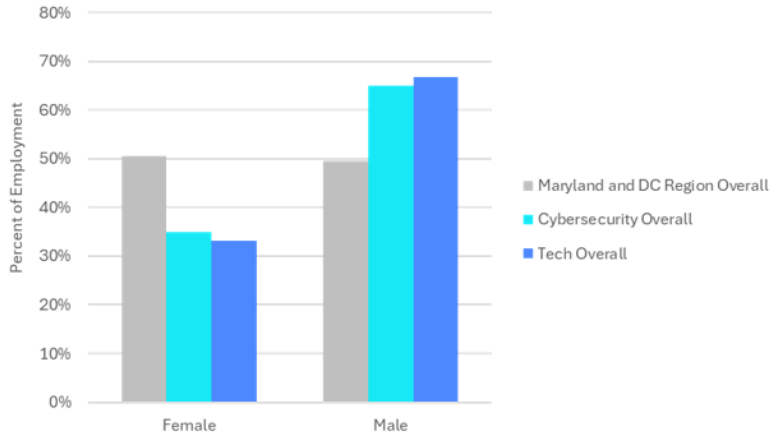
- The issue of brain drain is highlighted by comparisons against other states

4th	Maryland / DC rank of *people attracted* to the local cyber sector
5th	Maryland / DC rank of *non-local share* of the local cyber sector
10th	Maryland / DC rank of *producing* cyber grads
24th	Maryland / DC rank of *retention rate* for cyber grads

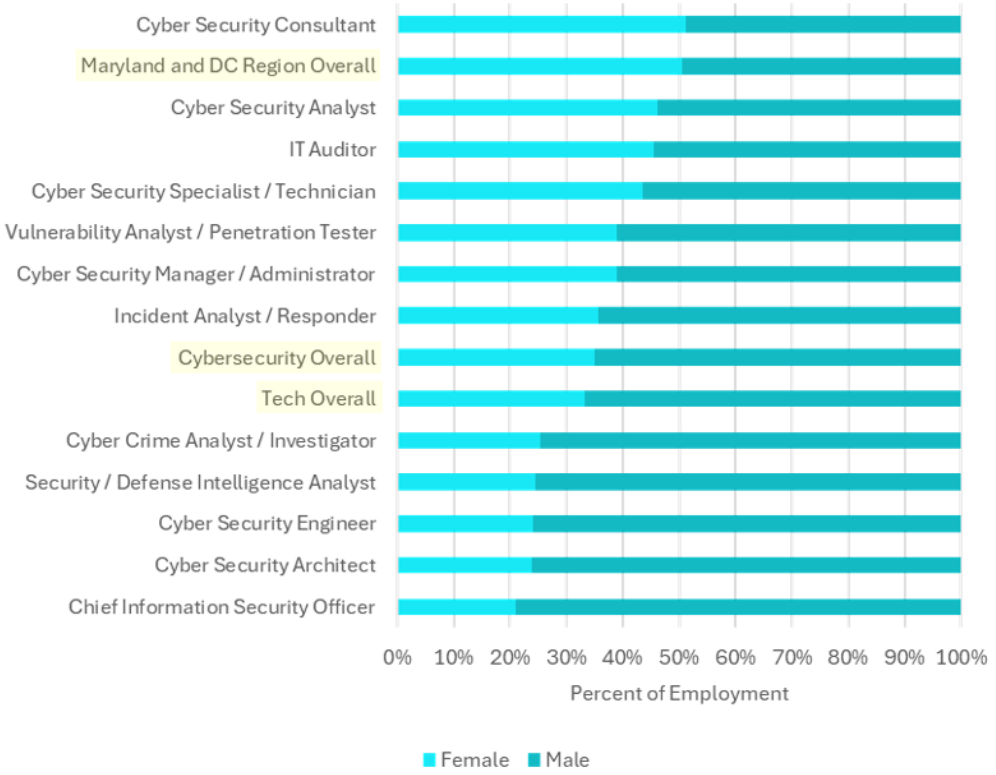
4. Analyze Talent Supply

- Cybersecurity has better representation of women than tech overall, but most occupations fall below parity with the overall region

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



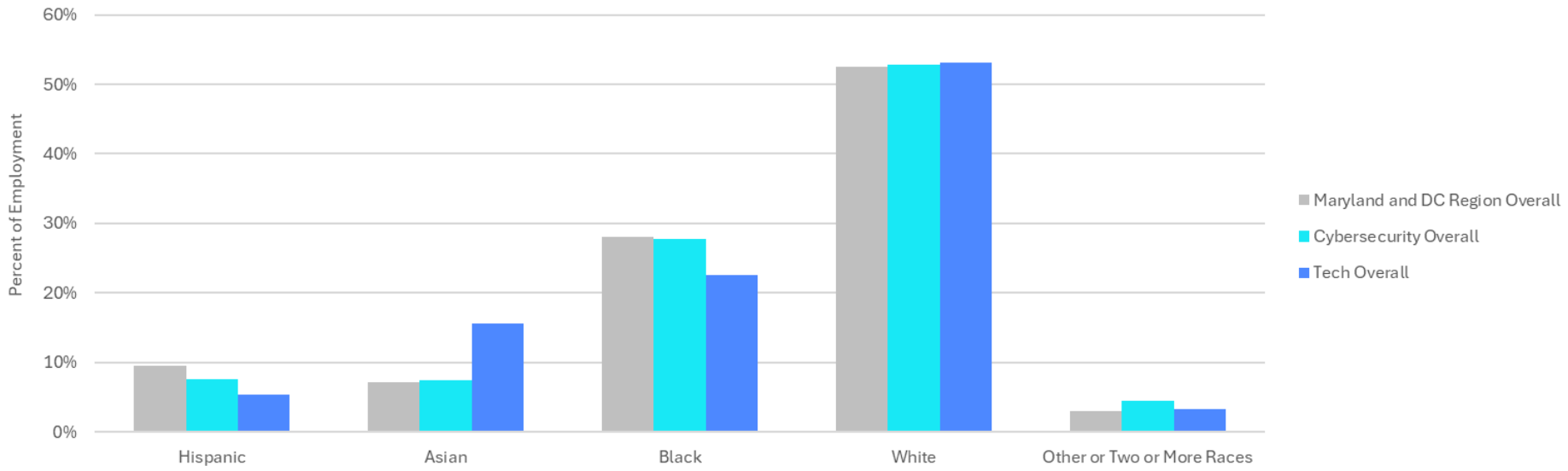
Gender Representation in Cybersecurity, Tech Overall, and the Maryland and DC Region Overall, by Occupation, Maryland and DC, 2023



4. Analyze Talent Supply

- Similar story by race/ethnicity

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



5. Build Pipelines

- Target cleared workers

  One potential talent source – 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.

- 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 and secondary school educators.

  The program is sponsored by the National Security Agency (NSA) and National Science Foundation (NSF), which could be approached with other funding ideas.

5. Build Pipelines

- Apprenticeships

  The state of Maryland established the Apprenticeship 2030 Commission to make recommendations to the state legislature on how apprenticeships can be used to reduce skill shortages in high-demand occupations. (Maryland has a goal of 80,000 registered apprenticeships by 2030.) The Commission can prioritize cybersecurity jobs in their recommendations for apprenticeship expansion.

  Cyber Maryland or other cybersecurity stakeholders could offer capacity building to support employers registering for apprenticeships.

  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.

5. Build Pipelines

- Skills training organizations

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. In general, 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. (Returning to the example of BCR, 900 of the 1,000 graduates went on to work in the cybersecurity sector.)

The most common occupation target of these programs is Cyber Security Analyst, followed by Help Desk Technician.

5. Build Pipelines

- Sizing the funding gap

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. (Most recently, the program announced the ability to train 700 Marylanders with $2 million in grant funding, or approximately $2,900 per participant.)

The primary funding mechanism for cybersecurity training in Maryland is the Maryland Department of Labor's Employment Advancement Right Now (EARN) Maryland program.

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.

However, 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.

5. Build Pipelines

- Examining funding mechanisms

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.

However, the *time-boundedness* of those grants can make it difficult to sustain funding over the lifetime of the program and impedes future-forward investments 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.

Legislatures play a significant role in determining community college budgets.

5. Build Pipelines

- Employers implement modified staffing strategies

Employers could develop and staff junior-level positions for some of the most in-demand occupations.

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.

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.

6. Continuous improvement

- Track key workforce health improvement metrics.

1. Supply/Demand Ratio for cyber-forward and cyber implementer occupations
2. Ratio of BA/BA+ to Sub-BA Job Postings for cyber-forward occupations
3. Share of Cyber Postings with Cyber Certification, disaggregated by public sector vs. private sector
4. Rate of Cyber-Aligned Completions vs Cyber Demand, year-on-year
5. Share of Cyber Demand Met by Postsecondary Completers, disaggregated to the sub-BA, BA, and BA+ levels
6. Race/Ethnicity Representation Ratio – percent of non-white/non-Asian cyber-forward workers to that population’s share of the overall workforce
7. Gender Representation Ratio – percent women in cyber-forward workforce to that population’s share of the overall workforce

6. Continuous improvement

- Democratize cyber workforce industry data.