Please Note...

This webinar and the engagement tools will be recorded.

An archive will be available on the [event website](#).
FEDERAL CYBERSECURITY WORKFORCE WEBINAR

Providing Timely and Clear Data to Support Federal Cybersecurity Workforce Needs
FEDERAL CYBERSECURITY WORKFORCE WEBINAR

Cyber Workforce Dashboard
Sarah Brickner
Program Analyst (Data Scientist)
U.S. Office of Personnel Management
Cyber Workforce Dashboard

- Under development – due to sensitivity of data, OPM is deliberating which data can be released to the public; no release date set
- Dummy data used for this demonstration
- EHRI-SDM data
  - EHRI-SDM data comes from Federal Agencies’ Human Resource Systems
  - Onboard data (all employees at single point in time at end of FY): 3-5 months delay
  - Dynamic data (hiring and separation actions throughout FY): 6-7 months delay
- Data is presented as percentages; Visuals with 10 or less people are withheld
- Excludes data at the Department/Agency/Sub-Agency levels
FEDERAL CYBERSECURITY WORKFORCE WEBINAR

Track the Gap to Hack the Gap

Will Markow
Vice President of Applied Research- Talent
Lightcast
Track the Gap to Hack the Gap

Will Markow – Vice President of Applied Research
The Cybersecurity Talent Pipeline is Broken
You Can’t Prepare Workers for Jobs You Know Nothing About
Overcoming Data Shortfalls to Quantify the Full Cybersecurity Ecosystem

The Problem

1. Historically, labor market information only tracked limited cybersecurity roles.
2. Cybersecurity jobs evolve rapidly, but most workforce data come with a lag.
3. No common language for describing cybersecurity jobs, skills, etc.

The Solution

1. Leverage real-time job posting and social profile data.
2. Define cybersecurity workforce in terms of job titles, skills, and credentials required.
3. Map cybersecurity jobs to NICE Framework to create common language.
Tracking the Workforce of Today and Tomorrow

Lightcast Collects Workforce Data from Thousands of Sources Around the Globe

- **Talent Pool Estimates**
  - Government collected data providing structured job counts to benchmark with.

- **Skills**
  - Dig beneath vague and unreliable job titles to find the specific skills you need.

- **Locations**
  - Compare over 1,500 markets globally for talent supply with a singular taxonomy.

- **Companies**
  - See top companies who are hiring or currently employing the talent you need.

- **Job Postings**
  - See real-time trends on postings in almost 750 markets around the world.

- **Profiles**
  - See beyond government data to analyze over 350 million aggregated resumes to see deep insights.

Regularly featured in:

- The Atlantic
- Forbes
- Harvard Business Review
- The New York Times
- WSJ
- USA Today
Illuminating Cybersecurity Workforce Challenges and Opportunities

Lightcast Illuminates the Public and Private Cybersecurity Job Market
Deciphering the Cybersecurity Job Market with CyberSeek.org
What Do the Latest Data Tell Us About the Cybersecurity Workforce?
Despite Economic Uncertainty, 
Cybersecurity Job Demand Remains Strong

Over 755,743 cyber job openings in the U.S. last year

Over 1.1 million existing cybersecurity workers
But Supply Can’t Keep Up with Demand

Cybersecurity Worker Supply and Demand Ratio

- Cybersecurity jobs take 21% longer to fill than other IT jobs
- Cybersecurity jobs pay 10% higher salaries than other IT jobs
What is Unique About Federal Cybersecurity Workforce Challenges?
Cybersecurity jobs are posted by 165 different federal entities.
Public Cyber Demand is More Concentrated in Work Roles Related to Operate & Maintain, Collect & Operate, and Investigate

Public vs. Private Demand Across NICE Cybersecurity Framework

Note: One job may perform duties related multiple work roles, so the numbers will add to greater than 100%
Public Sector Cyber Jobs Struggle to Keep Up with Private Sector Pay…

Average Advertised Salary for Core Cybersecurity Jobs

<table>
<thead>
<tr>
<th>Salary Range</th>
<th>Public Sector</th>
<th>Private Sector</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0-$20,000</td>
<td>$92,600</td>
<td>$117,200</td>
</tr>
<tr>
<td>$20,000-$40,000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$40,000-$60,000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$60,000-$80,000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$80,000-$100,000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$100,000-$120,000</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

...But Offer More Entry-Level Opportunities

Entry-Level Cybersecurity Opportunities

<table>
<thead>
<tr>
<th>% Entry-Level Cyber Openings</th>
<th>Public Sector</th>
<th>Private Sector</th>
</tr>
</thead>
<tbody>
<tr>
<td>10%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>28%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>% Sub-BA Cyber Openings</th>
<th>Public Sector</th>
<th>Private Sector</th>
</tr>
</thead>
<tbody>
<tr>
<td>9%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>22%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Private Employers Are 87% More Likely to Emphasize Emerging High-Value Skills

Sample Cyber Skills More Commonly Requested by Private Employers Than Public Employers

- Python (Programming Language): +191%
- Automation: +184%
- Cloud Computing Security: +138%
- Identity And Access Management: +106%
- Risk Management: +38%
Questions? Are There Other Challenges Federal Employers Face?
How Can the Federal Government Address its Cybersecurity Hiring Challenges?
Direct Workforce Development Where it is Most Needed
Focus on Building the Talent Pipeline for In-Demand Work Roles

Demand by Work Role: Public Sector

Systems Security Analyst 20,833
System Administrator 14,962
Network Operations Specialist 14,747
Technical Support Specialist 7,181
Data Analyst 9,156
Knowledge Manager 4,134
Database 3,859

Notes: The NICE Workforce Categories are not mutually exclusive—one job could perform multiple roles within the framework. The data shown here are not intended to be aggregated.

Systems Security Analyst is the most-demanded work role among public employers.
Train for High-Value Skills
Arm Students with the Skills Employers Most Value...Not Just Degrees

Many emerging cybersecurity skills boost salaries by $10k-$15k+

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Development Security</td>
<td>164%</td>
<td>29,635</td>
<td>$12,266</td>
</tr>
<tr>
<td>Cloud Security</td>
<td>115%</td>
<td>19,477</td>
<td>$15,025</td>
</tr>
<tr>
<td>Risk Management</td>
<td>60%</td>
<td>57,967</td>
<td>$13,379</td>
</tr>
<tr>
<td>Threat Intelligence</td>
<td>41%</td>
<td>60,039</td>
<td>$9,609</td>
</tr>
<tr>
<td>Incident Response</td>
<td>37%</td>
<td>23,497</td>
<td>$5,683</td>
</tr>
<tr>
<td>Compliance and Controls</td>
<td>36%</td>
<td>54,770</td>
<td>$12,423</td>
</tr>
<tr>
<td>Data Privacy and Security</td>
<td>36%</td>
<td>88,527</td>
<td>$5,256</td>
</tr>
<tr>
<td>Access Management</td>
<td>32%</td>
<td>118,096</td>
<td>$6,451</td>
</tr>
<tr>
<td>Security Strategy and Governance</td>
<td>20%</td>
<td>82,952</td>
<td>$7,735</td>
</tr>
<tr>
<td>Health Information Security</td>
<td>20%</td>
<td>413,687</td>
<td>$738</td>
</tr>
</tbody>
</table>
Right-Size Job Requirements
Focus on Need-To-Haves Versus Nice-To-Haves

Sample Cybersecurity Job Requirements

<table>
<thead>
<tr>
<th>IT Security Analyst</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Qualifications</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Experience in information security, cloud security, or cybersecurity</td>
</tr>
<tr>
<td>Bachelor’s degree in IT, cybersecurity or related area of study</td>
</tr>
<tr>
<td>Experience with multiple environments and operating systems, devices and databases including Windows Server, Active Directory, VMWare, Azure, AWS</td>
</tr>
<tr>
<td>Strong understanding of Cloud API development, SDLC processes, and security automation desired</td>
</tr>
<tr>
<td>Strong analytical and problem solving skills</td>
</tr>
<tr>
<td>Strong Incident Response background preferred</td>
</tr>
<tr>
<td>Fundamental understanding of security related technologies such as SIEM and SOAR</td>
</tr>
<tr>
<td>Must have obtain and maintain one or more Cloud or Security certifications such as AWS, Azure, CISSP, CISA, CISSM, CIPT, SSCP, CCSP</td>
</tr>
<tr>
<td>Strong understanding of information security standards, concepts, controls, testing techniques and technical risk assessment</td>
</tr>
</tbody>
</table>

Removing a BA requirement
Saves $16,000 and grows entry-level candidate pool by 61%

Building, not buying, emerging cybersecurity skills
Saves $10,000+ for each emerging skill

Eliminating specific certification requirements
Drops average salary costs by $9,000
Unlock the Power of Pathways
Build Diverse Talent Pipelines with Cybersecurity Career Pathways

Building career pathways between skill-adjacent roles helps you:

- Expand your talent pipeline
- Increase retention and employee engagement
- Reduce onboarding time
- Access more diverse pools of workers
Find Others With Skin in the Game
Partner with Local Employers, Policymakers, and Training Providers to Build the Next Generation of Cybersecurity Workers
How Do We Make CyberSeek Even More Actionable for Federal Cybersecurity Employers?

**Planned Enhancements to CyberSeek**

1. Separate federal data from state and local governments in the tool

2. Include time series data to track historical cybersecurity demand, add breakouts by education and experience levels, and increase the number of certifications and training providers tracked in the tool

3. Provide sample job descriptions and other tools that help employers shift to skills-based hiring
Questions?
Contact Information:

Will Markow
Vice President of Applied Research - Talent
will.markow@lightcast.io

Learn More:

Lightcast.io
CyberSeek.org
Complete Evaluation Form