Government Cyber Workforce Challenges

Steven Hernandez

Chief Information Security Officer
U. S. Department of Education

OCIO
Office of the Chief Information Officer
U.S. Department of Education

Agenda

- ED's challenge space
- Current observations
- What's working in the Federal environment
- Strategies going forward
- Questions

Ed’s Challenge Space

- Protecting a 1.6 trillion dollar portfolio
- Overseeing approximately a third of the nation’s PII
- Medical information
- Investigations information
- Institution Oversight

The evolution of cyber diversity workforce planning

Decade Ago: Civilian Departments and Agencies were in there formulation phase of cyber workforce development. The Federal Information Security Management Act (FISMA) was the lead driving legislation.

Many agencies transferred employees with minimal or no information assurance skills to positions such as Information System Security Officers or Information System Owners. Many attempted to do well in these positions, but lacked the experience and training.

While agencies reported they were staffed with cybersecurity personnel they struggled to maintain systems without breaches and their FISMA scores showed very poor performance. There was a silver lining. Multi-disciplinary employees started to arrive.

The evolution of cyber diversity workforce planning

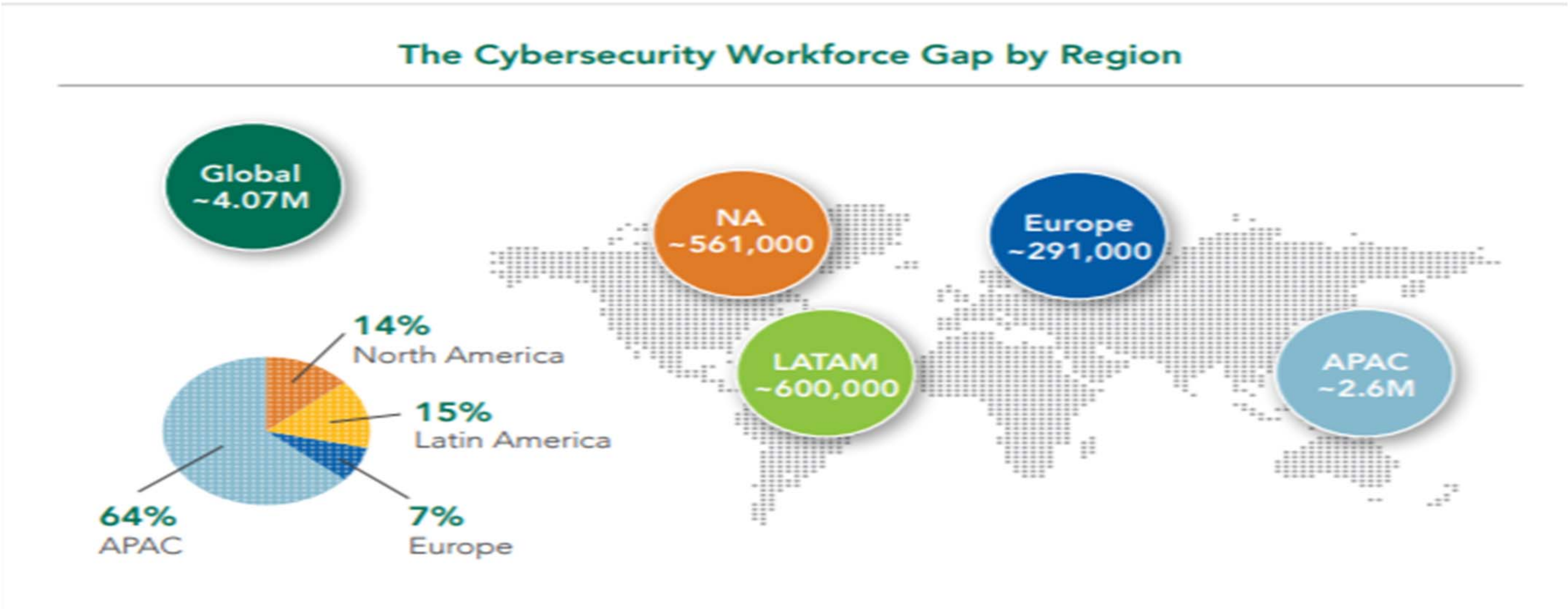
2000: Begin to see the rise of programs such as the Scholarship for Service. Centers of Academic Excellence are accredited by NSA to develop specialized and hybrid information assurance professionals.

2004/5: DoD releases Directive 8570, formally assigning credentials to specific function areas and levels of complexity/challenge. 2015: 8140 cyberspace workforce management.

2016: National Initiative for Cybersecurity Education (NICE)

Present: Reskilling and pipeline.

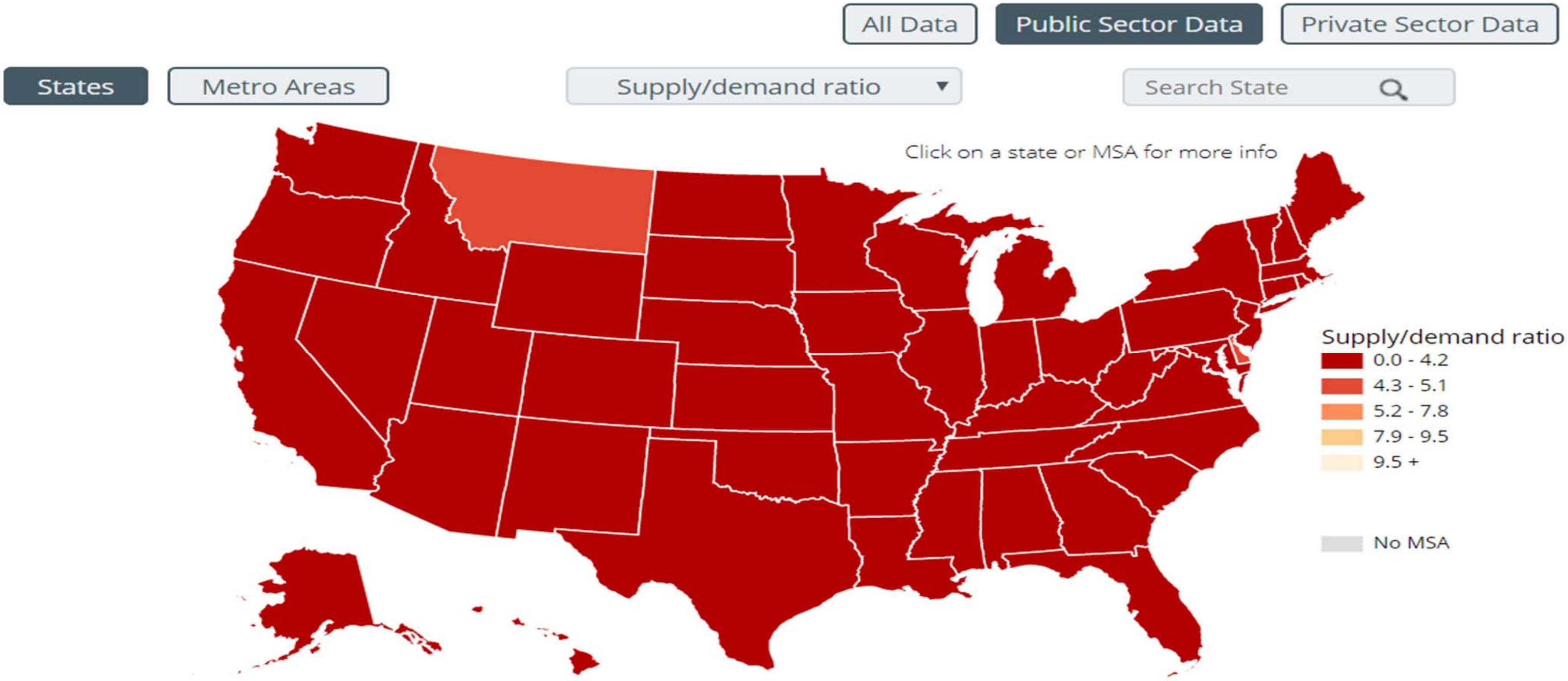
Our Information Assurance Workforce Challenge



The Cybersecurity Workforce Gap by Region

https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx

Our Information Assurance Workforce Challenge



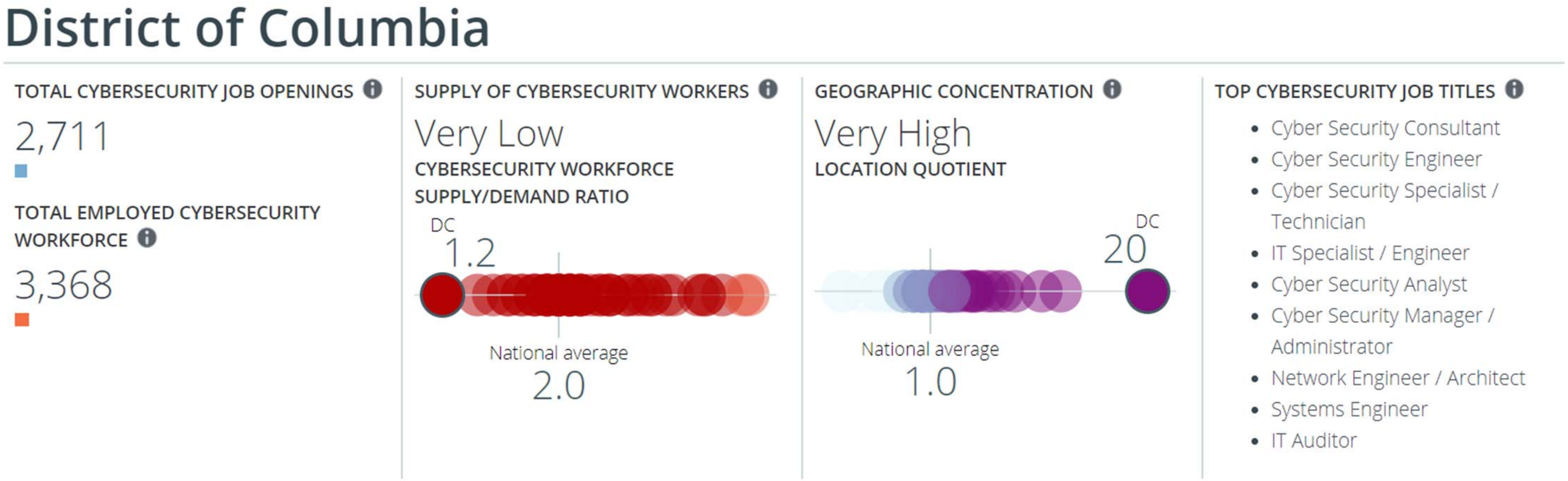
Click on a state or MSA for more info

Supply/demand ratio

🟥	0.0 - 4.2
🟥	4.3 - 5.1
🟧	5.2 - 7.8
🟨	7.9 - 9.5
⬜	9.5 +
⬜	No MSA

https://www.cyberseek.org/heatmap.html

Our Information Assurance Workforce Challenge



District of Columbia

TOTAL CYBERSECURITY JOB OPENINGS

2,711

🟦

TOTAL EMPLOYED CYBERSECURITY WORKFORCE

3,368

🟧

SUPPLY OF CYBERSECURITY WORKERS

Very Low

CYBERSECURITY WORKFORCE SUPPLY/DEMAND RATIO

GEOGRAPHIC CONCENTRATION

Very High

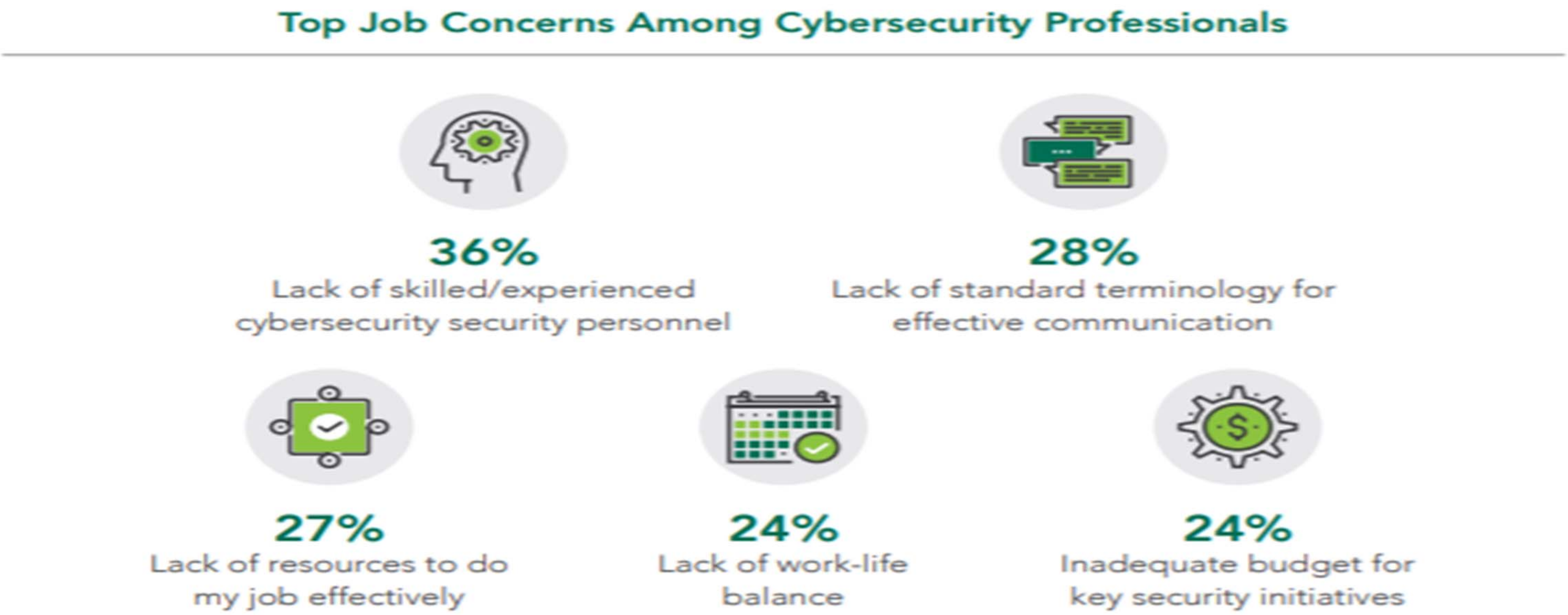
LOCATION QUOTIENT

TOP CYBERSECURITY JOB TITLES

- Cyber Security Consultant
- Cyber Security Engineer
- Cyber Security Specialist / Technician
- IT Specialist / Engineer
- Cyber Security Analyst
- Cyber Security Manager / Administrator
- Network Engineer / Architect
- Systems Engineer
- IT Auditor

https://www.cyberseek.org/heatmap.html

Our Information Assurance Workforce Challenge



Top Job Concerns Among Cybersecurity Professionals

36%
Lack of skilled/experienced cybersecurity security personnel

28%
Lack of standard terminology for effective communication

27%
Lack of resources to do my job effectively

24%
Lack of work-life balance

24%
Inadequate budget for key security initiatives

https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx

Conflicting Observations and Understanding

“Employers today are in critical need for more cybersecurity professionals, but they do not want more compliance officers or cybersecurity policy planners. What organizations are truly desperate for are graduates who can design secure systems, create new tools for defense, and hunt down hidden vulnerabilities in software and networks.”

“One solution to the deficit of practical skills in cybersecurity graduates is to expand apprenticeship, internship, and work-study offerings for students.[23] These opportunities give students a chance to apply what they have learned in a real-world environment, developing tangible skills in the process and giving a grounding to the theory-based components of their education. While these opportunities serve as useful supplements to existing education programs, there are also ways for instructors to do more to incorporate hands-on learning opportunities directly within the curricula themselves. The use of cyber ranges[24] and cybersecurity competitions,[25] for example, has been growing in popularity among education and training providers over the past several years. These offerings give students the chance to experience challenges modeled on real-world situations, letting them build practical skills while also improving their ability to work as teams in a fast-paced, adversarial environment.”

https://www.csis.org/analysis/cybersecurity-workforce-gap

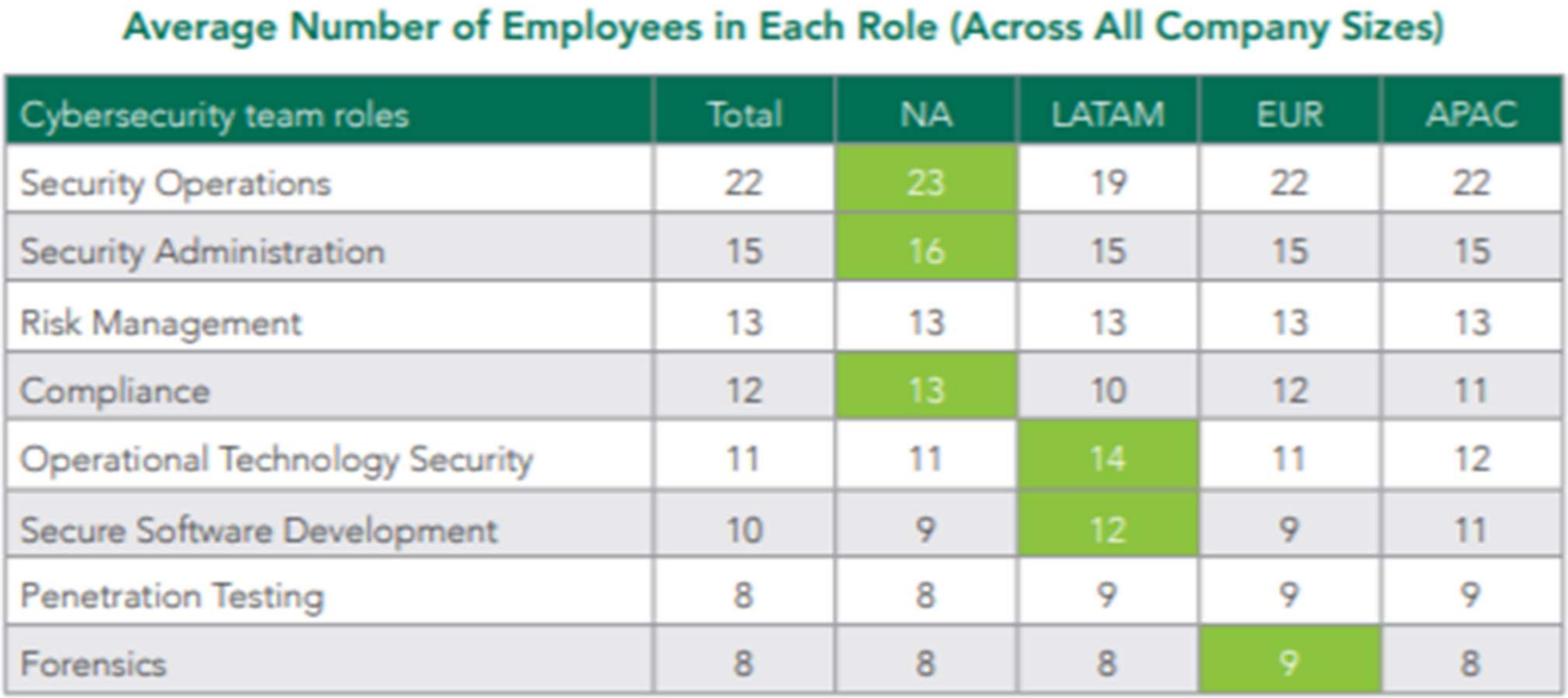
Observations

A wide spectrum exists regarding what experts think the Federal Government needs for Information Assurance and Cybersecurity professionals.

The U.S. Government is unique in its requirements for inherently governmental functions.

Additionally recruiting, retaining and maintaining cybersecurity professionals with technical talent can be challenging.

Observations

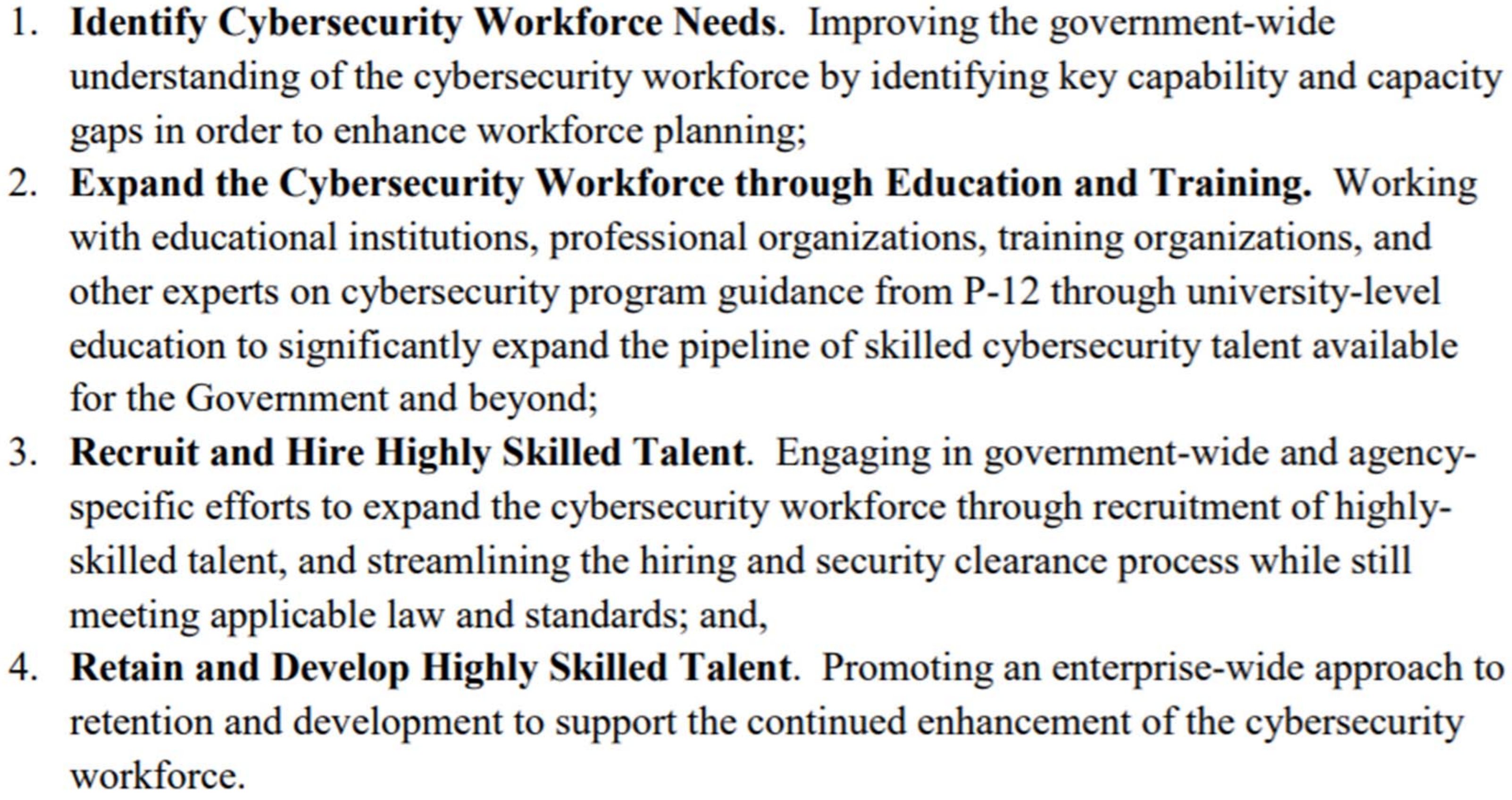


Average Number of Employees in Each Role (Across All Company Sizes)

Cybersecurity team roles	Total	NA	LATAM	EUR	APAC
Security Operations	22	23	19	22	22
Security Administration	15	16	15	15	15
Risk Management	13	13	13	13	13
Compliance	12	13	10	12	11
Operational Technology Security	11	11	14	11	12
Secure Software Development	10	9	12	9	11
Penetration Testing	8	8	9	9	9
Forensics	8	8	8	9	8

https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx

OMB 16-15 Observations



1. **Identify Cybersecurity Workforce Needs**. Improving the government-wide understanding of the cybersecurity workforce by identifying key capability and capacity gaps in order to enhance workforce planning;
2. **Expand the Cybersecurity Workforce through Education and Training.** Working with educational institutions, professional organizations, training organizations, and other experts on cybersecurity program guidance from P-12 through university-level education to significantly expand the pipeline of skilled cybersecurity talent available for the Government and beyond;
3. **Recruit and Hire Highly Skilled Talent**. Engaging in government-wide and agency-specific efforts to expand the cybersecurity workforce through recruitment of highly-skilled talent, and streamlining the hiring and security clearance process while still meeting applicable law and standards; and,
4. **Retain and Develop Highly Skilled Talent**. Promoting an enterprise-wide approach to retention and development to support the continued enhancement of the cybersecurity workforce.

Observations

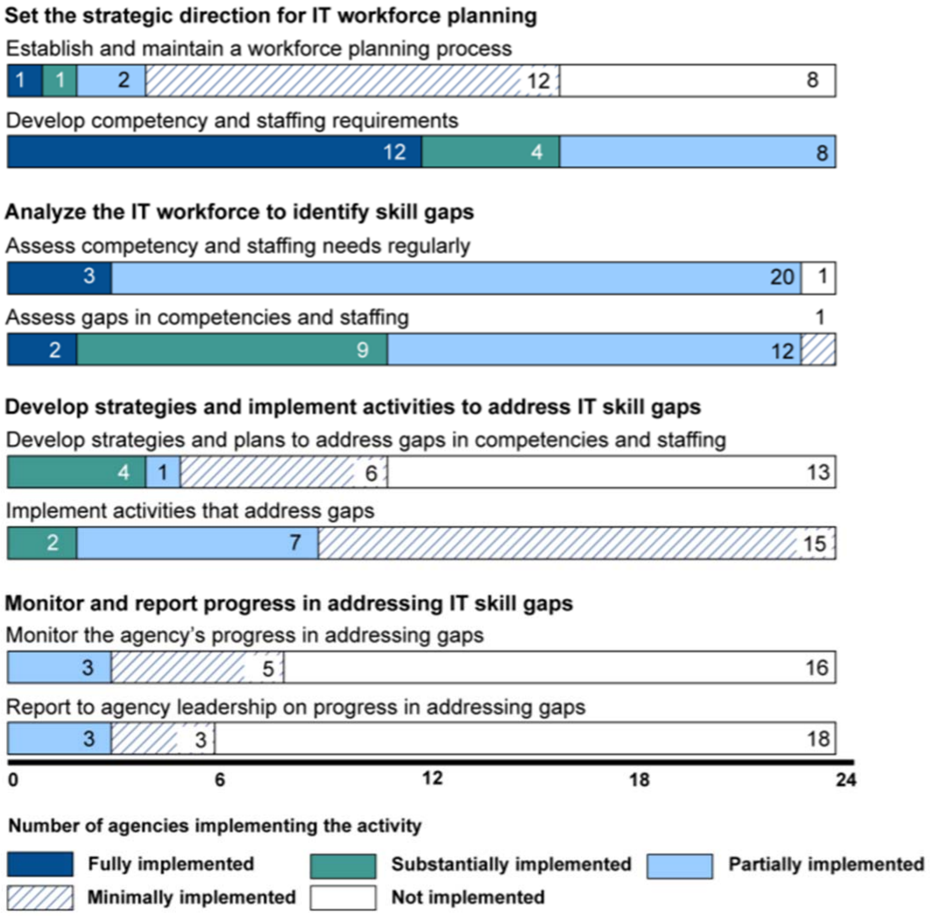
No single approach is going to work for getting the support we need. We are going to have to be creative in how we gain the resources we need.

In the Federal space we have lengthily requisition, posting, screening, interviewing, clearance and selection processes that compound the hiring process.

What works in the Federal sector will vary greatly based on agency.

GAO Oct 2019 Observations

Agencies' Overall Implementation of the Key Information Technology (IT) Workforce Planning Activities



Source: GAO analysis of agency information technology workforce planning policies and documentation. | GAO-20-129

Observations

- Hybrid skillsets are an absolute must. For example, if a cybersecurity professional can't perform the duties of a contracting officer's representative, they are a single powerful asset, but limited to what they can perform.

What's working

- Hiring the right skillset out of the gate and growing them
  - Scholarship for Service Program
    - MBA with CISSP
    - Forensics Experts
    - Legal and Risk Management
  - Ladders and blue sky are a must!
    - Progressive clearances and responsibilities.
  - Challenging assignments with meaning and opportunities to engage with senior leadership
  - Contracts, Budget, Appropriations, Antideficiency

What’s working

- Working with what we have
  - Reskilling
    - Overall very promising in terms of the results of the program
    - Opportunities exist to help transition reskilled employees to positions relevant to their training
    - Reskilling should grow beyond hard technical skills to include the managerial and operational skills such as COR training and FAC PPM.
    - OMB has completed the initial reskilling work and Departments and Agencies are determining how best to leverage reskilling going forward.

http://www3.weforum.org/docs/WEF_Towards_a_Reskilling_Revolution.pdf

https://www.cio.gov/programs-and-events/reskilling/

https://fcw.com/articles/2019/08/23/cyber-reskilling-grads-kent.aspx

What’s working

- CISO and CIO SES Candidate development
  - Called the CIO/CISO Multi-Agency Senior Executive Service Candidate Development Program (SES CDP), it’s accepting applications from current federal employees looking to lead the department’s IT offices.
  - Applicants must have previously managed subordinates and be General Schedule-14 or above
  - The program itself consists of formal trainings, assessments and seminars with participants expected to complete a 90-day executive-level developmental assignment. Funding for the 80 hours of training is being provided by the Federal CIO Council.

https://www.fedscoop.com/usda-cio-ciso-development-program/

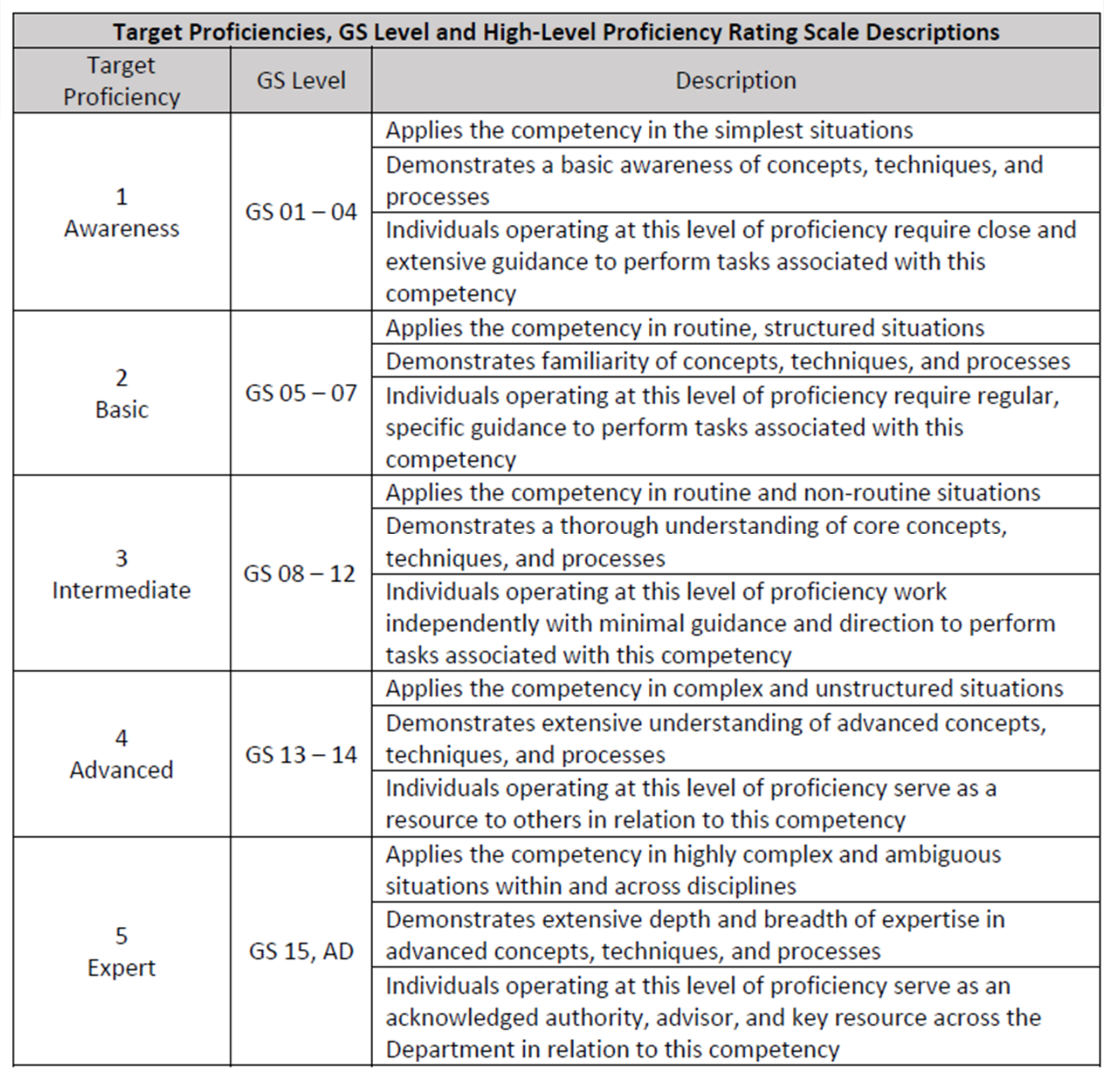
What’s working

- Working with what we have
  - Rotations and Details
    - Absolutely critical for the success of reskilling
    - An excellent way to transfer talent from other parts of the organization to determine fit and growth potential
    - Gets experience for the candidate. 12 months is typically the required experience to compete for a cybersecurity position.
  - Information Assurance training
    - Robust program that now must include:
      - Statistics / Data Science
      - Privacy
      - IOT

Competency Assessments

- Organizational Assessments
  - IT assessments
    - Capabilities mapped to NICE
    - Supervisors and leadership confirmed significance of capabilities
    - Employees self-assessed this mastery of capabilities
    - Supervisors then verify and validate the employees self-rating
    - The deltas tell an incredible story

Competency Assessments



Target Proficiencies, GS Level and High-Level Proficiency Rating Scale Descriptions		
Target Proficiency	GS Level	Description
1 Awareness	GS 01 – 04	Applies the competency in the simplest situations
		Demonstrates a basic awareness of concepts, techniques, and processes
		Individuals operating at this level of proficiency require close and extensive guidance to perform tasks associated with this competency
2 Basic	GS 05 – 07	Applies the competency in routine, structured situations
		Demonstrates familiarity of concepts, techniques, and processes
		Individuals operating at this level of proficiency require regular, specific guidance to perform tasks associated with this competency
3 Intermediate	GS 08 – 12	Applies the competency in routine and non-routine situations
		Demonstrates a thorough understanding of core concepts, techniques, and processes
		Individuals operating at this level of proficiency work independently with minimal guidance and direction to perform tasks associated with this competency
4 Advanced	GS 13 – 14	Applies the competency in complex and unstructured situations
		Demonstrates extensive understanding of advanced concepts, techniques, and processes
		Individuals operating at this level of proficiency serve as a resource to others in relation to this competency
5 Expert	GS 15, AD	Applies the competency in highly complex and ambiguous situations within and across disciplines
		Demonstrates extensive depth and breadth of expertise in advanced concepts, techniques, and processes
		Individuals operating at this level of proficiency serve as an acknowledged authority, advisor, and key resource across the Department in relation to this competency

Strategies Moving Ahead

- Leverage results of competency assessment
- Continued support of Scholarship for Service
- Further refinement of the reskilling approach
- Professionalization and centralization of skills (ISSO for example)
- Leveraging the NICE framework for skills assessment and training.
- Leverage industry certifications and training whenever possible
- Cyber-pay and Credential-pay

Questions?