NICE

NATIONAL INITIATIVE FOR **CYBERSECURITY** EDUCATION

Marian Merritt, Lead for Industry Engagement

Marian.merritt@nist.gov

National Initiative for Cybersecurity Education (NICE)

- The NICE Strategic Goals
- Why we need a Cybersecurity Workforce Framework
  - Development process
  - Target audience
- The Framework: categories; specialty areas; work roles
  - Resources for adoption
  - CyberSeek.org

NICE Strategic Goals

Accelerate Learning and Skills Development

- *Inspire a sense of urgency in both the public and private sectors to address the shortage of skilled cybersecurity workers*

Nurture A Diverse Learning Community

- *Strengthen education and training across the ecosystem to emphasize learning, measure outcomes, and diversify the cybersecurity workforce*

Guide Career Development & Workforce Planning

- *Support employers to address market demands and enhance recruitment, hiring, development, and retention of cybersecurity talent*

https://www.nist.gov/itl/applied-cybersecurity/nice/about/strategic-plan

NICE Strategic Goal #3: Guide Career Development and Workforce Planning

Support employers to address market demands and enhance recruitment, hiring, development, and retention of cybersecurity talent

Objectives:

....

3.2 Publish and raise awareness of the NICE Cybersecurity Workforce Framework and encourage adoption

Why we need a workforce framework

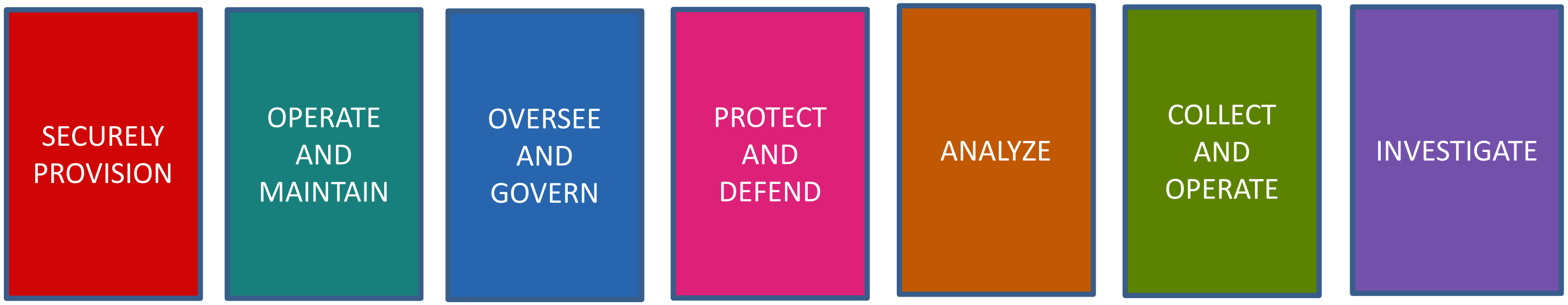
- Standardized taxonomy and lexicon for describing cybersecurity work
- Professionalization of the industry
- Employers: define workforce, identify gaps, create position descriptions
- Workers (current and future): explore work roles, identify areas of interest, areas for development
- Training/certification: help workforce gain and demonstrate KSAs
- Educators: develop curriculum, degrees, research
- All together create ecosystem and pathway that guides activities and reduces confusion

What is the history behind the NICE Framework?

- Beg. ~2010 an effort to understand cybersecurity work and those who perform it
- Focus originally on the government workforce with input from industry and academia; now appropriate to all sectors
- Standardizing occupations and associated information to help create career pathways public<>private sector and academia>workforce
- First draft in 2011
- SP 800-181, Released in 2017, now in second version
- May 2019 EO on Cybersecurity Workforce encourages wide adoption:
  - Adopted across federal government, increasingly state and local level
  - Recently adopted in New Brunswick, Canada
  - Industry also adopting: JP Morgan, AT&T, Fidelity Investments, etc.

NICE Framework – NIST Special Publication 800-181

Workforce Categories (7)



SECURELY PROVISION

OPERATE AND MAINTAIN

OVERSEE AND GOVERN

PROTECT AND DEFEND

ANALYZE

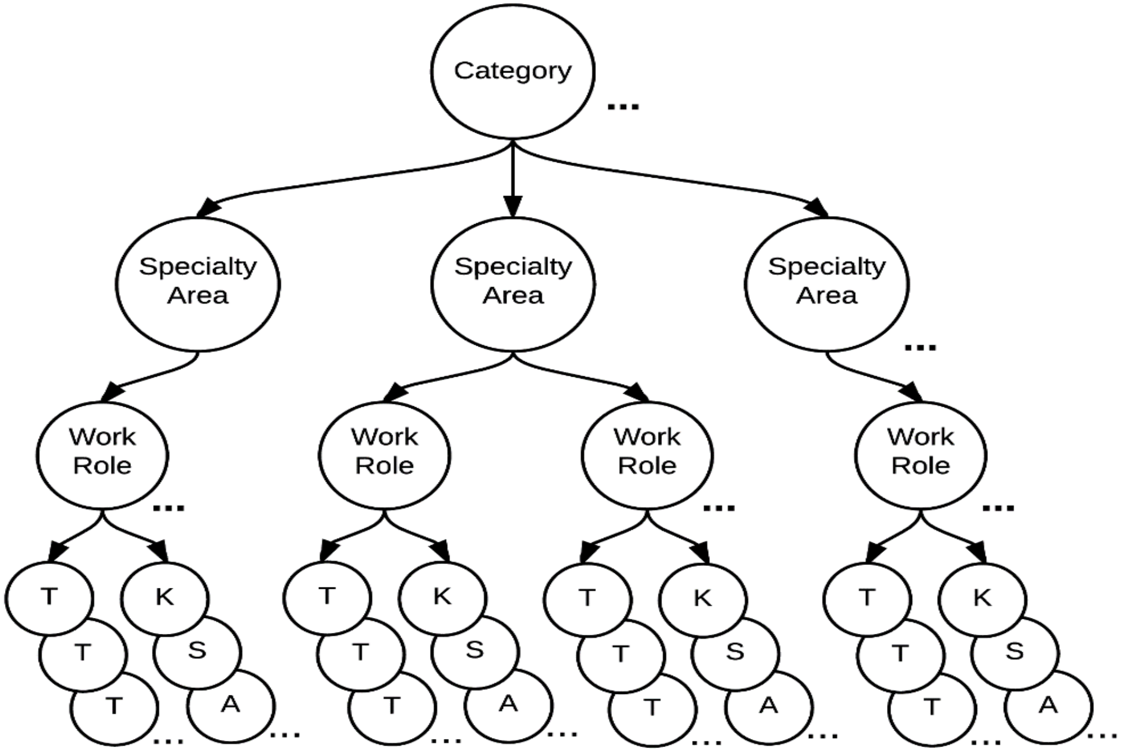
COLLECT AND OPERATE

INVESTIGATE

- **Specialty Areas** (33) – Distinct areas of cybersecurity work
- **Work Roles** (52) – The most detailed groupings of IT, cybersecurity, or cyber-related work, which include specific *Knowledge, Skills, and Abilities (KSA's)* required to perform a set of *Tasks*.

NICE Framework: Tasks and KSA's

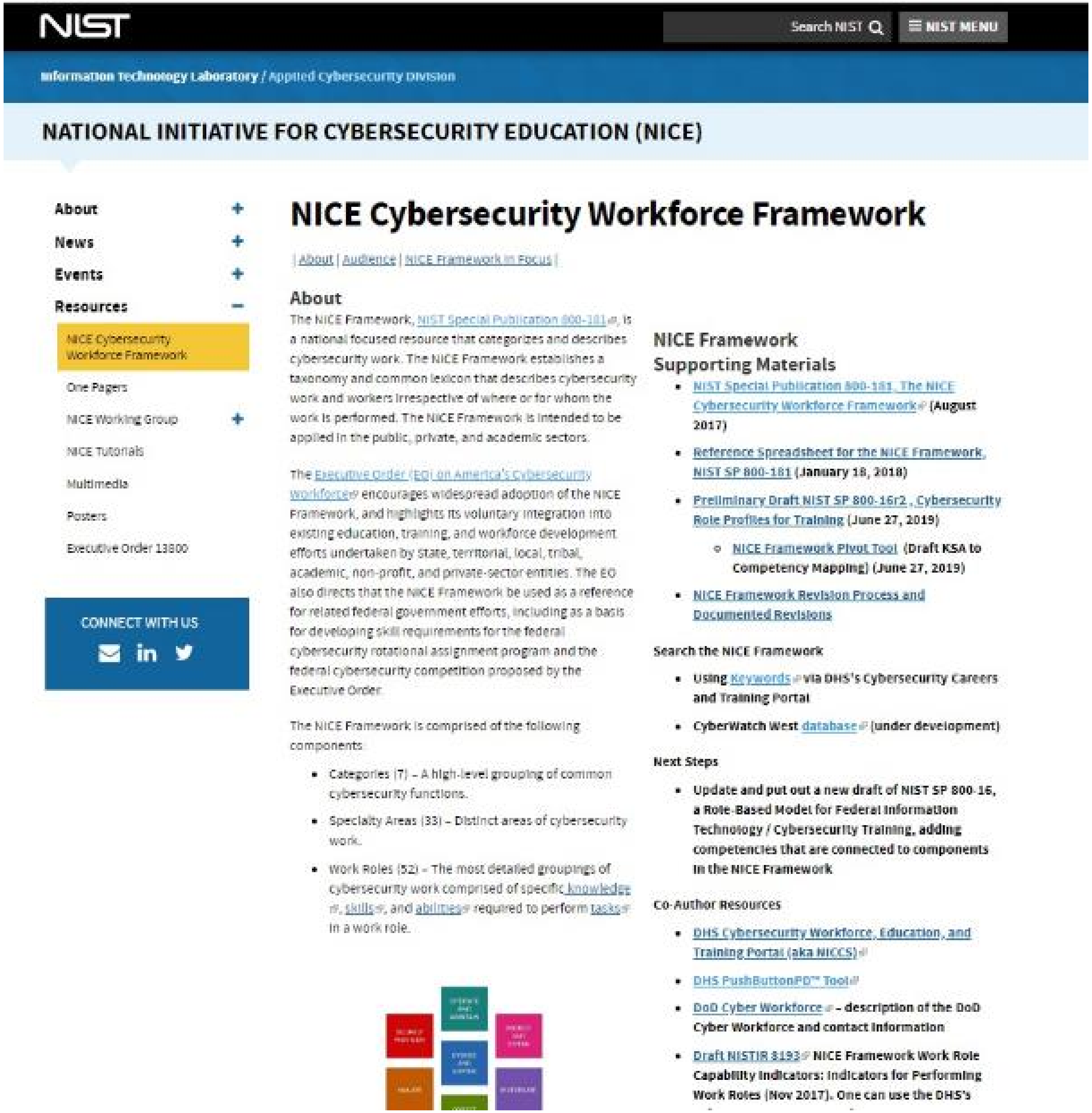
- Tasks – Specific work activities that could be assigned to a practitioner working in one of the NICE Framework Work Roles; and,
- Knowledge, Skills, and Abilities (KSAs) – Knowledge, Skills, and Abilities (KSAs) are the attributes required to perform work roles and are generally demonstrated through relevant experience, education, or training



Securely Provision (7 Specialty Areas, 11 Work Roles)

Category	Specialty Area	Work Role
Securely Provision	Risk Management	Authorizing Official/Designating Representative
		Security Control Assessor
	Software Development	Software Developer
		Secure Software Assessor
	Systems Architecture	Enterprise Architect
		Security Architect
	Technology R&D	Research & Development Specialist
	Systems Requirements Planning	Systems Requirements Planner
	Test and Evaluation	Testing and Evaluation Specialist
	Systems Development	Information Systems Security Developer
		Systems Developer

https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework



NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE)

NICE Cybersecurity Workforce Framework

| About | Audience | NICE Framework in Focus |

About

The NICE Framework, NIST Special Publication 800-181, is a national focused resource that categorizes and describes cybersecurity work. The NICE Framework establishes a taxonomy and common lexicon that describes cybersecurity work and workers irrespective of where or for whom the work is performed. The NICE Framework is intended to be applied in the public, private, and academic sectors.

The Executive Order (EO) on America's cybersecurity workforce encourages widespread adoption of the NICE Framework, and highlights its voluntary integration into existing education, training, and workforce development efforts undertaken by state, territorial, local, tribal, academic, non-profit, and private-sector entities. The EO also directs that the NICE Framework be used as a reference for related federal government efforts, including as a basis for developing skill requirements for the federal cybersecurity rotational assignment program and the federal cybersecurity competition proposed by the Executive Order.

The NICE Framework is comprised of the following components:

- Categories (7) – A high-level grouping of common cybersecurity functions.
- Specialty Areas (33) – Distinct areas of cybersecurity work.
- Work Roles (52) – The most detailed groupings of cybersecurity work comprised of specific knowledge, skills, and abilities required to perform tasks in a work role.

NICE Framework Supporting Materials

- NIST Special Publication 800-181, The NICE Cybersecurity Workforce Framework (August 2017)
- Reference Spreadsheet for the NICE Framework, NIST SP 800-181 (January 18, 2018)
- Preliminary Draft NIST SP 800-16r2, Cybersecurity Role Profiles for Training (June 27, 2019)
  - NICE Framework Pivot Tool (Draft KSA to Competency Mapping) (June 27, 2019)
- NICE Framework Revision Process and Documented Revisions

Search the NICE Framework

- Using Keywords via DHS's Cybersecurity Careers and Training Portal
- CyberWatch West database (under development)

Next Steps

- Update and put out a new draft of NIST SP 800-16, a Role-Based Model for Federal Information Technology / Cybersecurity Training, adding competencies that are connected to components in the NICE Framework

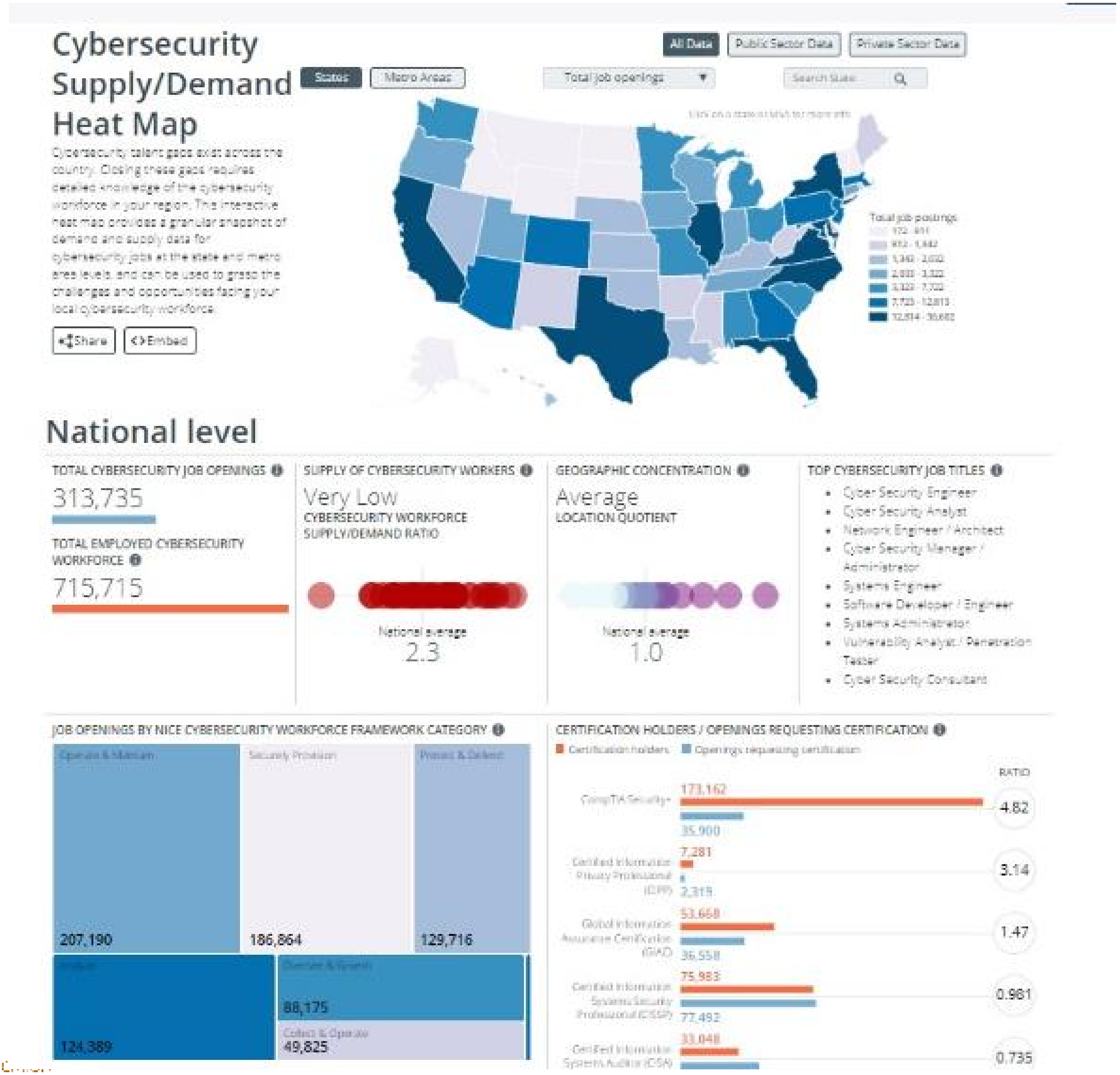
Co-Author Resources

- DHS Cybersecurity Workforce, Education, and Training Portal (aka NICCS)
- DHS PushButtonPD™ Tool
- DoD Cyber Workforce – description of the DoD Cyber Workforce and contact information
- Draft NISTIR 8193 NICE Framework Work Role Capability Indicators: Indicators for Performing Work Roles (Nov 2017). One can use the DHS's

Resources to use the Framework

- Visit NICCS portal https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework/search
- Or CyberWatchWest: http://cyberindustry.org/Workrole
- Example: if you search the keyword “Educator”, it leads to
  - Tasks ID: T0380. Description: Plan instructional strategies such as lectures, demonstrations, interactive exercises, multimedia presentations….
- Leads to a **Work Role**: Cyber Instructional Curriculum Developer
- OV-TEA-001 which is found under the **Category** “**Oversee and Govern**” under the **Specialty Area** of **Training, Education and Awareness**.
- The NICCS portal also shows entry, intermediate and advanced credentials, education, training, etc for these roles.

Cyber Seek



Cybersecurity Supply/Demand Heat Map

Cybersecurity talent gaps exist across the country. Closing these gaps requires detailed knowledge of the cybersecurity workforce in your region. This interactive heat map provides a granular snapshot of demand and supply data for cybersecurity jobs at the state and metro area levels, and can be used to grasp the challenges and opportunities facing your local cybersecurity workforce.

National level

TOTAL CYBERSECURITY JOB OPENINGS
313,735

TOTAL EMPLOYED CYBERSECURITY WORKFORCE
715,715

SUPPLY OF CYBERSECURITY WORKERS
Very Low
CYBERSECURITY WORKFORCE SUPPLY/DEMAND RATIO

GEOGRAPHIC CONCENTRATION
Average
LOCATION QUOTIENT

TOP CYBERSECURITY JOB TITLES

- Cyber Security Engineer
- Cyber Security Analyst
- Network Engineer / Architect
- Cyber Security Manager / Administrator
- Systems Engineer
- Software Developer / Engineer
- Systems Administrator
- Vulnerability Analyst / Penetration Tester
- Cyber Security Consultant

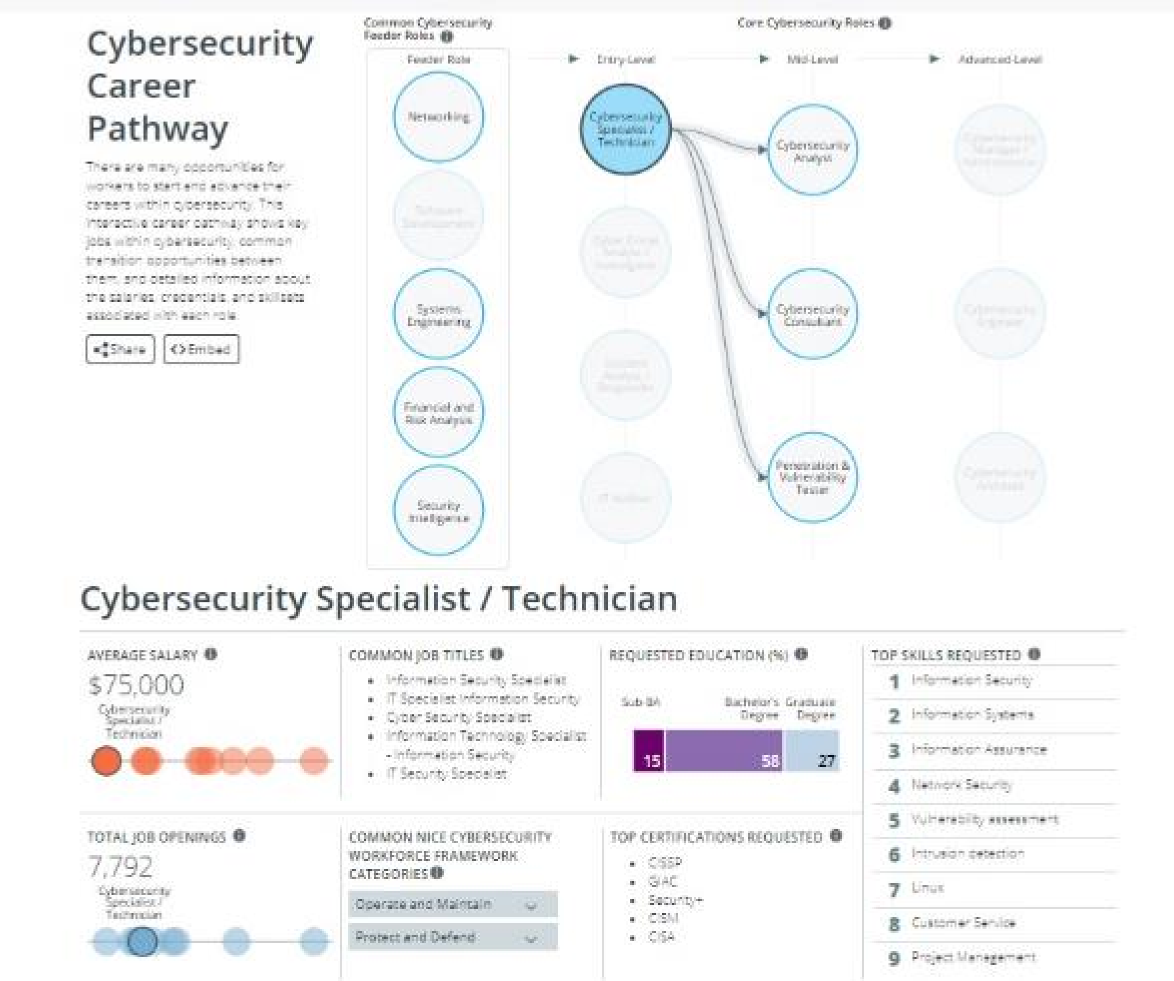
JOB OPENINGS BY NICE CYBERSECURITY WORKFORCE FRAMEWORK CATEGORY

CERTIFICATION HOLDERS / OPENINGS REQUESTING CERTIFICATION

🟥 Certification holders
🟦 Openings requesting certification
RATIO
CompTIA Security+
173,162
35,900
4.82
Certified Information Privacy Professional (CIPP)
7,281
2,319
3.14
Global Information Assurance Certification (GIAC)
53,668
36,558
1.47
Certified Information Systems Security Professional (CISSP)
75,983
77,492
0.981
Certified Information Systems Auditor (CISA)
33,048
0.735

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Career pathway tool



Cybersecurity Career Pathway

There are many opportunities for workers to start and advance their careers within cybersecurity. This interactive career pathway shows key jobs within cybersecurity, common transition opportunities between them, and detailed information about the salaries, credentials, and skillsets associated with each role.

Cybersecurity Specialist / Technician

AVERAGE SALARY

$75,000

COMMON JOB TITLES

- Information Security Specialist
- IT Specialist Information Security
- Cyber Security Specialist
- Information Technology Specialist - Information Security
- IT Security Specialist

REQUESTED EDUCATION (%)

Sub-BA	Bachelor's Degree	Graduate Degree
15	58	27

TOP SKILLS REQUESTED

1	Information Security
2	Information Systems
3	Information Assurance
4	Network Security
5	Vulnerability assessment
6	Intrusion detection
7	Linux
8	Customer Service
9	Project Management

TOTAL JOB OPENINGS

7,792

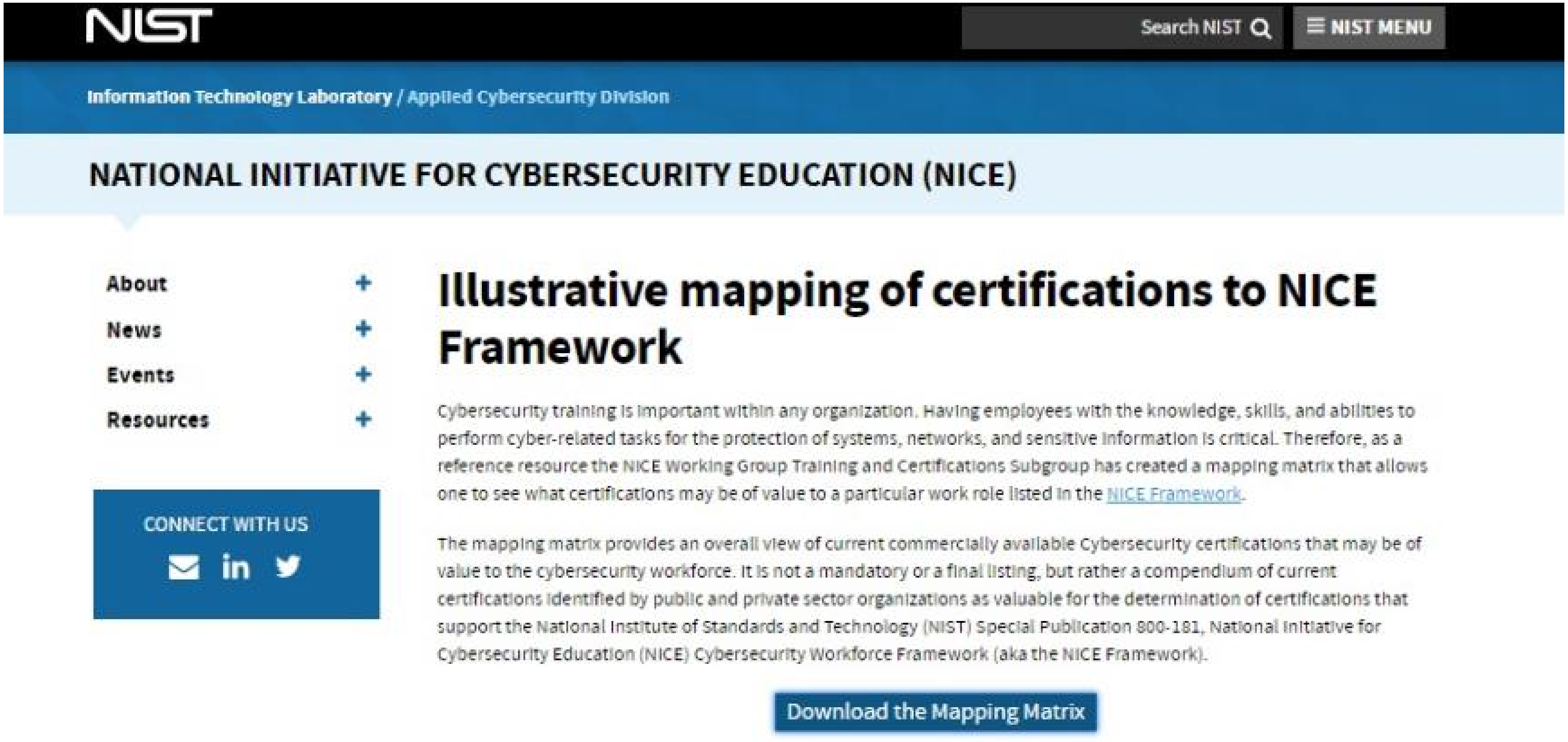
COMMON NICE CYBERSECURITY WORKFORCE FRAMEWORK CATEGORIES

- Operate and Maintain
- Protect and Defend

TOP CERTIFICATIONS REQUESTED

- CISSP
- GIAC
- Security+
- CISM
- CISA

NICE Working Group effort



NIST
Search NIST
☰ NIST MENU
Information Technology Laboratory / Applied Cybersecurity Division

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE)

Illustrative mapping of certifications to NICE Framework

Cybersecurity training is important within any organization. Having employees with the knowledge, skills, and abilities to perform cyber-related tasks for the protection of systems, networks, and sensitive information is critical. Therefore, as a reference resource the NICE Working Group Training and Certifications Subgroup has created a mapping matrix that allows one to see what certifications may be of value to a particular work role listed in the NICE Framework.

The mapping matrix provides an overall view of current commercially available Cybersecurity certifications that may be of value to the cybersecurity workforce. It is not a mandatory or a final listing, but rather a compendium of current certifications identified by public and private sector organizations as valuable for the determination of certifications that support the National Institute of Standards and Technology (NIST) Special Publication 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (aka the NICE Framework).

NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Thank you!