NICE

NATIONAL INITIATIVE FOR **CYBERSECURITY** EDUCATION

Vision

A digital economy enabled by a knowledgeable and skilled cybersecurity workforce.

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Mission of NICE

To energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development.

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

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

CyberSeek™

About | Interactive map | Career pathway | Who this tool is for | Project partners

Cybersecurity Supply/Demand Heat Map

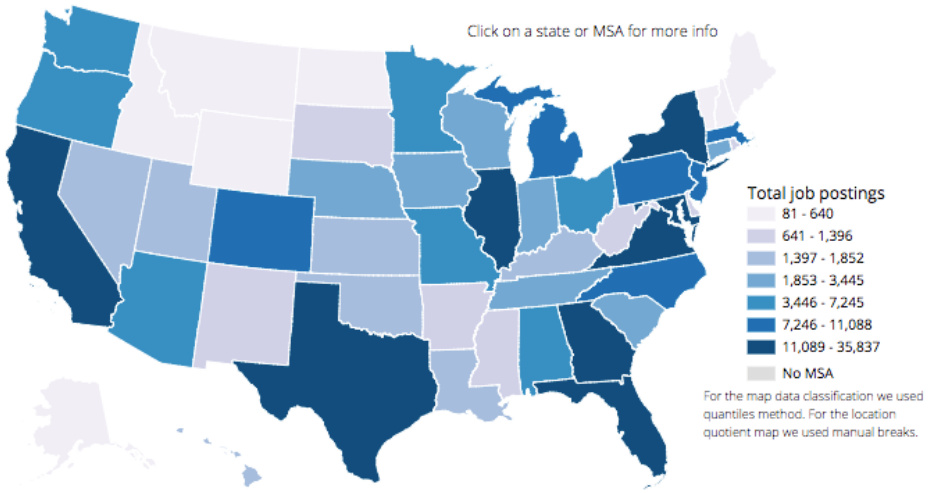
Cybersecurity talent gaps exist across the country. Closing these gaps requires detailed knowledge of the cybersecurity workforce in your region. This interactive heat map provides a granular snapshot of demand and supply data for cybersecurity jobs at the state and metro area levels, and can be used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

Share

States | Metro Areas

Total job openings

Search State



National level

TOTAL CYBERSECURITY JOB OPENINGS
299,335

TOTAL EMPLOYED CYBERSECURITY WORKFORCE
746,858

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

National average
2.5

GEOGRAPHIC CONCENTRATION
Average
LOCATION QUOTIENT

National average
1.0

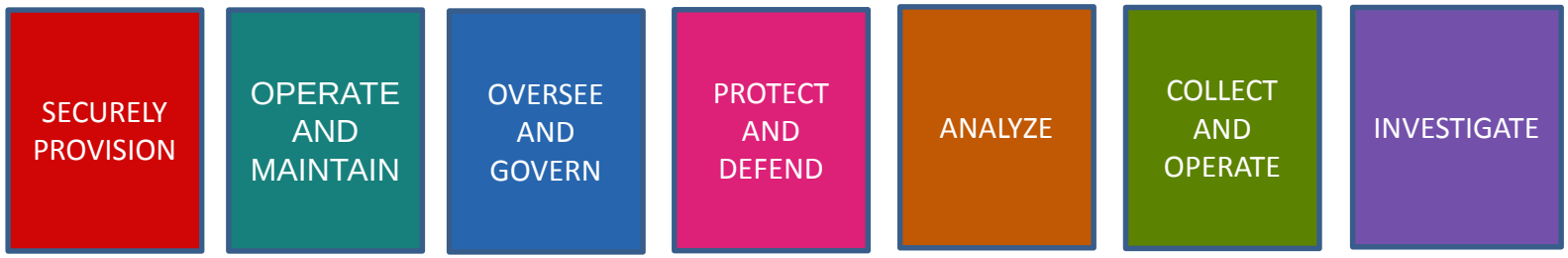
TOP CYBERSECURITY JOB TITLES

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

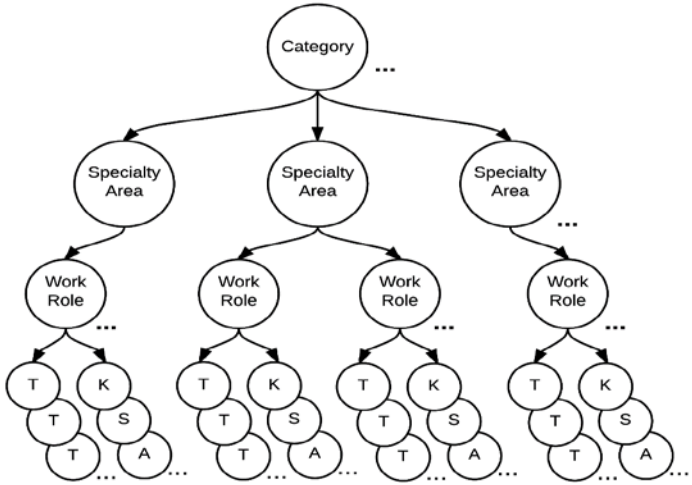
NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NICE Cybersecurity Workforce Framework – Draft NIST SP 800-181

Reference Resource for cybersecurity workforce development

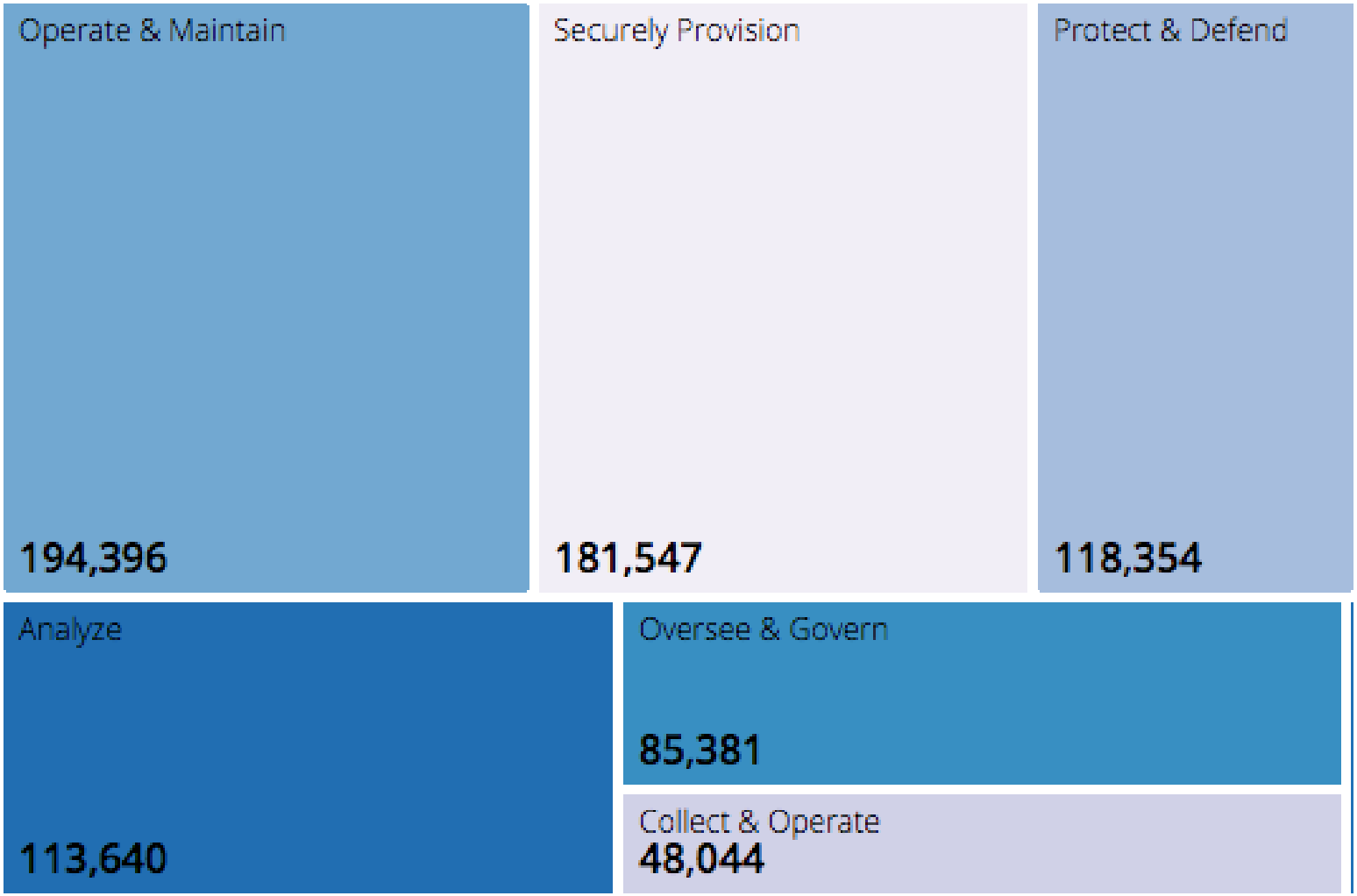


- Specialty Areas (33) – Distinct areas of cybersecurity work;
  - Work Roles (52) – The most detailed groupings of IT, cybersecurity or cyber-related work, which include specific knowledge, skills, and abilities required to perform a set of tasks.
    - Tasks – Specific work activities that could be assigned to a professional working in one of the NCWF's Work Roles; and,
    - Knowledge, Skills, and Abilities (KSAs) –
    - Attributes required to perform Tasks, generally **demonstrated through relevant experience or performance-based education and training**.
- Audience:
  - Employers
  - Current and Future Cybersecurity Workers
  - Training and Certification Providers
  - Education Providers
  - Technology Providers



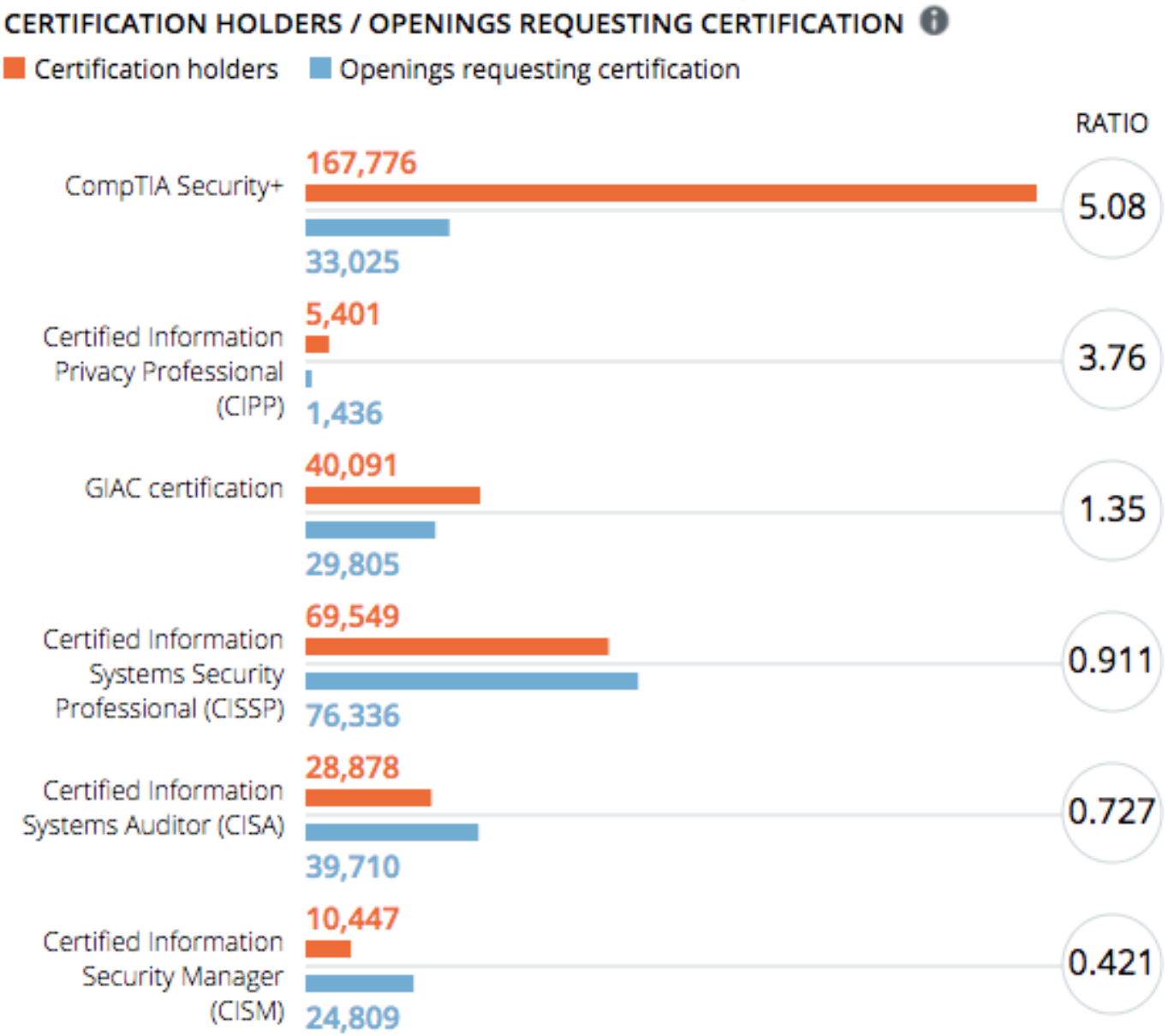
NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

POSTINGS BY NICE CYBERSECURITY WORKFORCE FRAMEWORK CATEGORY



NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

CERTIFICATION HOLDERS / OPENINGS REQUESTING CERTIFICATION



NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

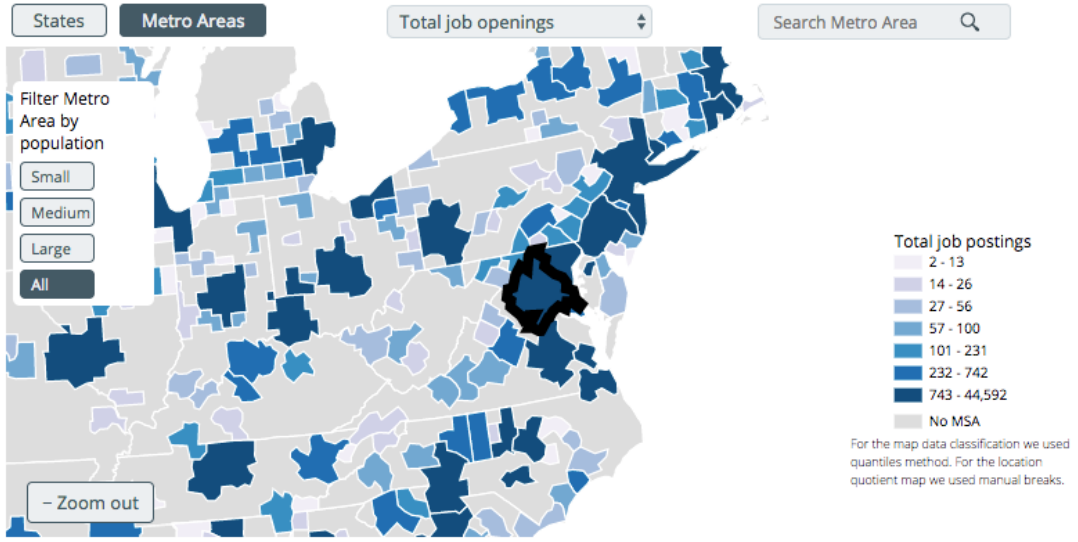
CyberSeek™

About | Interactive map | Career pathway | Who this tool is for | Project partners

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.

Share



Washington-Arlington-Alexandria, DC-VA-MD-WV

TOTAL CYBERSECURITY JOB OPENINGS
44,592

TOTAL EMPLOYED CYBERSECURITY WORKFORCE
77,630

SUPPLY OF CYBERSECURITY WORKERS
Very Low
CYBERSECURITY WORKFORCE SUPPLY/DEMAND RATIO
Washington-Arlington-Alexandria, DC
1.74
National average
2.5

GEOGRAPHIC CONCENTRATION
Very High
LOCATION QUOTIENT
rlington-Alexandria, DC-VA-MD-WV
6.81
National average
1.0

TOP CYBERSECURITY JOB TITLES

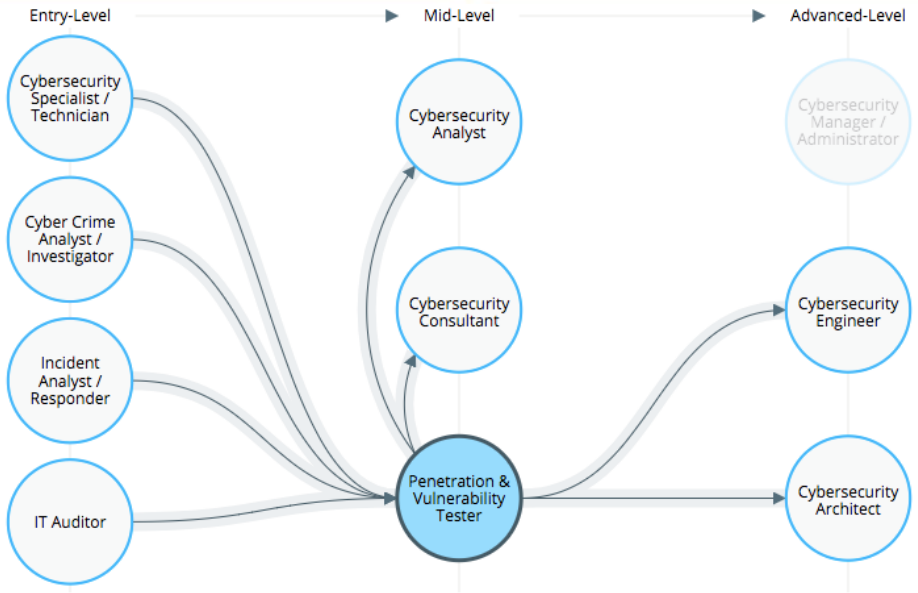
- Cyber Security Engineer
- Cyber Security Analyst
- Network Engineer / Architect
- Software Developer / Engineer
- Systems Engineer
- Cyber Security Manager / Administrator
- Information Assurance Engineer / Analyst
- Systems Administrator
- Cyber Security Specialist /

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

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.

Share



Penetration & Vulnerability Tester

AVERAGE SALARY

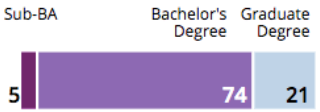
$101,000

and Vulnerability Tester

COMMON JOB TITLES

- Penetration Tester
- Security Analyst
- Application Security Analyst
- Senior Penetration Tester
- Lead Security Analyst

REQUESTED EDUCATION (%)



TOP SKILLS REQUESTED

1. Information Security
2. JAVA
3. LINUX
4. Information Systems
5. Project Management
6. Software Development
7. SQL
8. Python
9. Scanners

TOTAL JOB OPENINGS

10,547

and Vulnerability Tester

COMMON NICE CYBERSECURITY WORKFORCE FRAMEWORK CATEGORIES

Analyze

Protect and Defend

TOP CERTIFICATIONS REQUESTED

- CISSP
- GIAC
- CISA
- CISM
- Certified Ethical Hacker

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NICE KNOWLEDGE, SKILLS, AND ABILITIES

- Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.
- Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.
- Knowledge of application vulnerabilities.
- Skill in conducting application vulnerability assessments.
- Knowledge of cryptography and cryptographic key management concepts.
- Skill in assessing the application of cryptographic standards.
- Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools.
- Knowledge of cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
- Knowledge of network access, identity, and access management (e.g., public key infrastructure [PKI]).
- Knowledge of network protocols (e.g., Transmission Critical Protocol/Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]), and directory services (e.g., Domain Name System [DNS]).
- Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).
- Knowledge of penetration testing principles, tools, and techniques.
- Knowledge of programming language structures and logic.
- Ability to apply programming language structures (e.g., source code review) and logic.

NICE FRAMEWORK TASKS

- Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational directives.
- Conduct and/or support authorized penetration testing on enterprise network assets.
- Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) to support cyber defense audit missions.
- Maintain knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing.
- Prepare audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions.
- Conduct required reviews as appropriate within environment (e.g., Technical Surveillance, Countermeasure Reviews [TSCM], TEMPEST countermeasure reviews).
- Perform technical (evaluation of technology) and non-technical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (e.g., local computing environment, network and infrastructure, enclave boundary, supporting infrastructure, and applications).
- Make recommendations regarding the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems and processes).

NICE Engagement Process

- NICE Working Group

  Subgroups: K-12, Collegiate, Competitions, Training and Certifications, and Workforce Management
- NICE Interagency Coordinating Council
- NICE Webinars (Monthly)
- NICE eNewsletter (Quarterly)
- NICE Email Updates (Periodic)
- NICE Events

  Annual Conference & Expo: November 7-8, 2017, Dayton, OH

  NICE K-12 Cybersecurity Education Conference: Dec 3-4, Nashville, TN
- NICE Website: nist.gov/nice

REGISTER TODAY!

NICE Conference & Expo

November 7-8, 2017

Dayton Convention Center, Dayton, Ohio

https://www.fbcinc.com/e/nice/attendeereg.aspx

Keynotes

Rob Joyce
Special Assistant to the President, Cybersecurity Coordinator
National Security Council, The White House

CISO Panel
Moderated by...
Aric K. Perminter
President
International Consortium of Minority Cybersecurity Professionals

Angela M. Messer
Executive Vice President
Booz Allen Hamilton Cyber Innovation and Talent Officer