Outline

• About
  – Mission
  – Values
  – Goals
  – Purpose

• Engagement
  – Collaboration
  – Tools
Partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development.
Mission of NICE

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

Seek Evidence
Pursue Action
Challenge Assumptions
Embrace Change
Stimulate Innovation
Foster Communication
Facilitate Collaboration
Share Resources
Model Inclusion
Measure Results
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
Accelerate Learning and Skills Development

http://gbievents.com/blog/minding-the-security-gap
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
Managing Risk

Risk Management

- **Information technologies** – products, services, and systems
- **Processes** - policies and procedures
- **People**
  - Users of information technologies
  - Trained workforce capable of addressing security threats

Image from https://www.itgovernance.co.uk/blog/wp-content/uploads/2015/07/PPT-Diagram-Blog.png
How to Engage

Participate and Learn

Contribute and Invest

Experiment and Innovate
NICE Engagement

Inform

- NICE Working Groups (K-12, Collegiate, Competitions, Training and Certifications, and Workforce Management)
- NICE Interagency Coordinating Council (ICC)
- NICE eNewsletter (Quarterly)
- Events:
  - Monthly Webinars – Cybersecurity Careers for Autistic People.
  - NICE Annual Conference – Nov. 7-8 in Dayton, OH
  - National K-12 Cybersecurity Education Conf. – Dec. 4-5 in Nashville, TN

Influence

- NICE Framework
- Cybersecurity Jobs Heat Map
- RAMPS Federal Funding Opportunity

Innovate

- NICE Challenge Project
• **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
Common knowledge areas (6)

- Knowledge of computer networking concepts and protocols, and network security methodologies.
- Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
- Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.
- Knowledge of specific operational impacts of cybersecurity lapses.
- Knowledge of cybersecurity principles.
- Knowledge of cyber threats and vulnerabilities.
CyberSeek

**Interactive Map**

A heat map of cybersecurity supply and demand

**Career Pathway**

An interactive career pathway showing common roles within cybersecurity and transition opportunities between them

http://cyberseek.org/
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

<table>
<thead>
<tr>
<th>TOTAL CYBERSECURITY JOB OPENINGS</th>
<th>SUPPLY OF CYBERSECURITY WORKERS</th>
<th>GEOGRAPHIC CONCENTRATION</th>
<th>TOP CYBERSECURITY JOB TITLES</th>
</tr>
</thead>
<tbody>
<tr>
<td>299,335</td>
<td>Very Low</td>
<td>Average</td>
<td>- Cyber Security Engineer</td>
</tr>
<tr>
<td>TOTAL EMPLOYED CYBERSECURITY</td>
<td>CYBERSECURITY WORKFORCE</td>
<td>LOCATION QUOTIENT</td>
<td>- Cyber Security Analyst</td>
</tr>
<tr>
<td>WORKFORCE</td>
<td>SUPPLY/DEMAND RATIO</td>
<td></td>
<td>- Network Engineer / Architect</td>
</tr>
<tr>
<td>746,858</td>
<td></td>
<td></td>
<td>- Cyber Security Manager / Administrator</td>
</tr>
<tr>
<td></td>
<td>National average</td>
<td>National average</td>
<td>- Software Developer / Engineer</td>
</tr>
<tr>
<td></td>
<td>2.5</td>
<td>1.0</td>
<td>- Systems Engineer</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Systems Administrator</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- IT Auditor</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Vulnerability Analyst / Penetration Tester</td>
</tr>
<tr>
<td>Category</td>
<td>Postings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operate &amp; Maintain</td>
<td>194,396</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Securely Provision</td>
<td>181,547</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protect &amp; Defend</td>
<td>118,354</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analyze</td>
<td>113,640</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oversee &amp; Govern</td>
<td>85,381</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collect &amp; Operate</td>
<td>48,044</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
CERTIFICATION HOLDERS / OPENINGS REQUESTING CERTIFICATION

- CompTIA Security+: 167,776 (Certification holders), 33,025 (Openings requesting certification), Ratio: 5.08
- Certified Information Privacy Professional (CIPP): 5,401 (Certification holders), 1,436 (Openings requesting certification), Ratio: 3.76
- GIAC certification: 40,091 (Certification holders), 29,805 (Openings requesting certification), Ratio: 1.35
- Certified Information Systems Security Professional (CISSP): 69,549 (Certification holders), 76,336 (Openings requesting certification), Ratio: 0.911
- Certified Information Systems Auditor (CISA): 28,878 (Certification holders), 39,710 (Openings requesting certification), Ratio: 0.727
- Certified Information Security Manager (CISM): 10,447 (Certification holders), 24,809 (Openings requesting certification), Ratio: 0.421
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.

Penetration & Vulnerability Tester

Average Salary: $101,000

Common Job Titles:
- Penetration Tester
- Security Analyst
- Application Security Analyst
- Senior Penetration Tester
- Lead Security Analyst

Requested Education (%):
- Sub-BA: 5
- Bachelor's Degree: 74
- Graduate Degree: 21

Total Job Openings: 10,547

Common NICE Cybersecurity Workforce Framework Categories:
- Analyze
- Protect and Defend

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

CyberSeek
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION
RAMPS for Cybersecurity Education and Workforce

Regional Alliances and Multistakeholder Partnerships Stimulating (RAMPS) Cybersecurity Education and Workforce Development

- **Southwest Region**: Arizona Statewide Cyber Workforce Consortium
- **Western Region**: Cyber Prep Program
- **Central Region**: Cincinnati-Dayton Cyber Corridor (Cin-Day Cyber)
- **Mid-Atlantic Region**: Hampton Roads Cybersecurity Education, Workforce, and Economic Development Alliance (HRCyber)
- **Northeast Region**: The Partnership to Advance Cybersecurity Education and Training (PACET)
Virtual environment to test students and professionals alike on their ability to perform NICE Cybersecurity Workforce Framework tasks and exhibit their knowledge, skills, and abilities.

https://nice-challenge.com/
Going Forward

Let’s Be........

• **Innovative**: new ways
• **Engaged**: collaborate
• **Aware**: learn
• **Adaptive**: change
• **Aligned**: on same page
• **Successful**: progress
• **Investors**: workforce
Thank you!
Clarence Williams, Lead for Government Engagement

clarence.williams@nist.gov

nist.gov/nice