

NICE

NATIONAL INITIATIVE FOR **CYBERSECURITY** EDUCATION



The National Cybersecurity Workforce Framework

2015 Delaware Cyber Security Workshop – September 29, 2015

Bill Newhouse

NICE Program Office at the National Institute of Standards and Technology



- NICE is a ***national initiative*** to address cybersecurity education, training, and workforce development
- NICE is a public-private ***partnership*** between government, academia, and the private sector
- NICE will build upon existing ***successful programs***
- NICE will facilitate ***change and innovation***
- NICE will bring ***leadership*** and vision
- NICE values communication, collaboration, inclusion, evidence, **action and results**

NICE Strategic Goals

- Accelerate Learning and Skills Development
- Nurture a Diverse Learning Community
- Guide Career Development and Workforce Planning

Accelerate Learning and Skills Development

- Invoke a sense of urgency in both the public and private sectors to address the shortage of a skilled workforce
- Stimulate approaches and techniques that can more rapidly increase the supply of qualified cybersecurity workers
- Reduce the time and cost for obtaining **knowledge, skills, and abilities** for in demand work roles
- Pursue displaced workers or underemployed individuals who are available and motivated
- Identify and fill gaps in cybersecurity skills training to support identified workforce needs

Nurture a Diverse Learning Community

- Encourage creative and effective efforts to increase the number of underrepresented populations
- Inspire cybersecurity **career awareness**, exploration, and preparedness with students in elementary and secondary schools
- Strengthen formal education programs, co-curricular experiences, training and certifications, and employer-based training
- Build on institutional initiatives to improve student success by establishing academic pathways for cybersecurity careers
- Explore international approaches that could inform practice in the United States or that NICE could influence

Guide Career Development and Workforce Planning

- Promote the National Cybersecurity Workforce Framework and encourage sector implementations
- Identify and analyze data sources that project present and future workforce demand and supply of qualified cybersecurity workers
- Explore tools and techniques that effectively measure and validate knowledge, skills, and abilities
- Identify and promote effective practices and solutions that enhance recruitment, hiring, promotion, and retention
- Promote tools that assist human resource professionals and hiring managers with talent management

NICE Engagement

- Interagency Coordinating Committee
 - NSF, NSA, DHS, OPM, ED, DoC, DoL, DoD, and more . . .
- NICE Working Group
 - Collegiate Subgroup
 - K-12 Subgroup
 - Competitions Subgroup
 - Training and Certifications Subgroup
 - **Workforce Framework Subgroup**
 - Career Development Subgroup
- NICE365 Industry Advisory Group

NICE FRAMEWORK

The NICE Cybersecurity Workforce Framework outlines 31 functional work specialties within seven categories

- Developed in collaboration with subject matter experts from government, non-profits, academia, and the private sector.
- Foundation for increasing the size and capability of the US cybersecurity workforce.
- National resource for employers, educators, trainers, and policy makers, providing a common cybersecurity lexicon.



Securely Provision	concerned with conceptualizing, designing, and building secure IT systems, with responsibility for some aspect of the systems' development
Operate and Maintain	responsible for providing the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security
Protect and Defend	responsible for the identification, analysis, and mitigation of threats to internal IT systems or networks
Investigate	responsible for the investigation of cyber events and/or crimes of IT systems, networks, and digital evidence
Operate and Collect	responsible for specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence
Analyze	responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence
Oversight and Development	providing leadership, management, direction, and/or development and advocacy so that all individuals and the organization may effectively conduct cybersecurity work

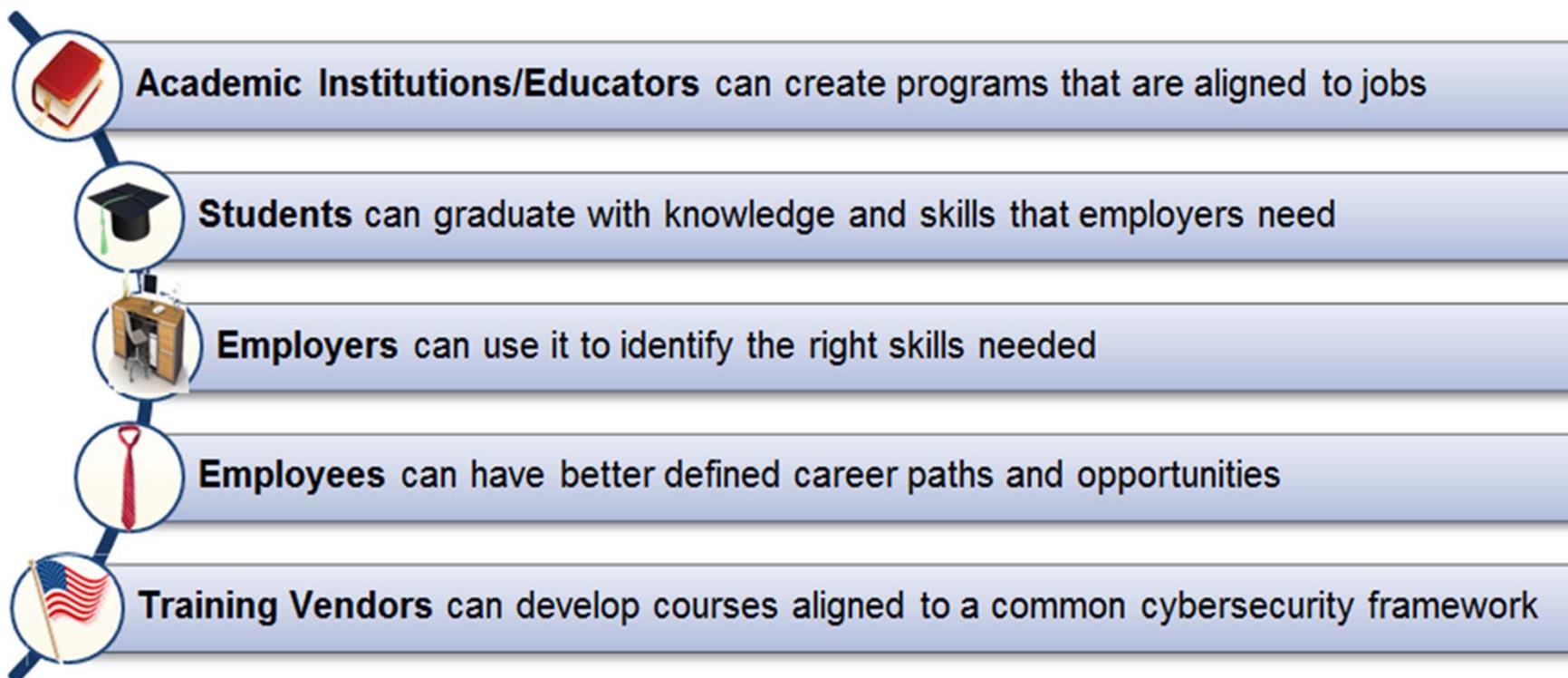
- Describes and categorizes cybersecurity work
 - Related Job Titles - persons working in this Specialty area may have job titles similar to: (e.g. Job Titles for Incident Response)
 - Incident Response: Computer Crime Investigator, Incident Handler, Incident Responder, Incident Response Analyst, Incident Response Coordinator, and Intrusion Analyst
 - Tasks – persons involved in this Specialty perform the following tasks: (e.g. 2 of 14 tasks for Incident Response)
 - Collect intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise
 - Coordinate with and provide expert technical support to enterprise-wide Computer Network Defense technicians to resolve Computer Network Defense incidents
 - KSAs - experts in the Specialty Area have the following Knowledge, Skills, and Ability: (e.g. 2 of 26 KSAs for Incident Response)
 - Knowledge of basic system administration, network, and operating system hardening techniques
 - Knowledge of Computer Network Defense policies, procedures, and regulations



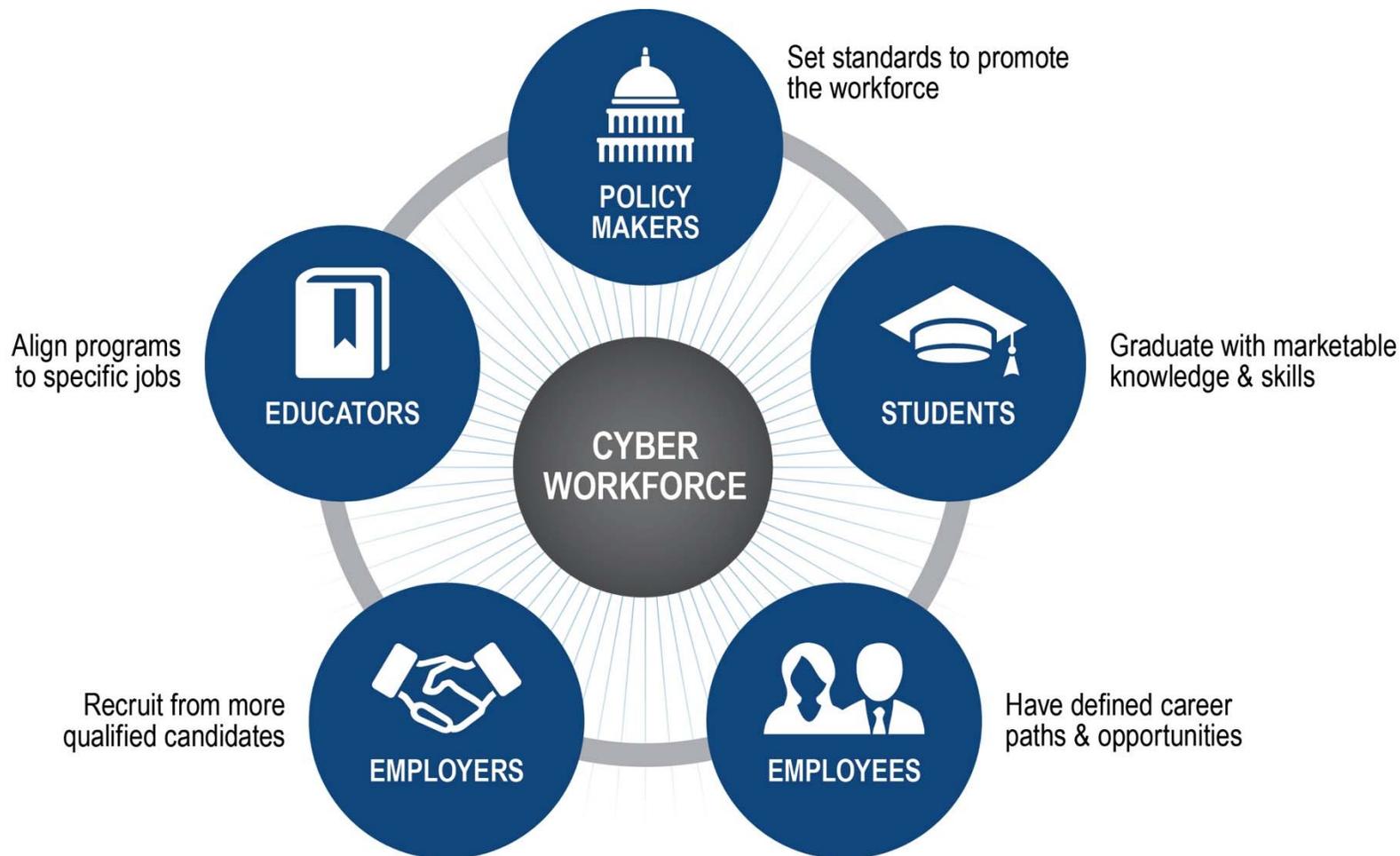
- Provides a foundation that organizations can use to develop position descriptions, competency models, and training.
 - Competencies are areas of expertise required for successful performance of a role or job function.
 - Competency list displays the types of workforce characteristics an individual must exhibit to successfully perform his/her specific role.
 - The Framework defines competencies through the association of KSAs.

National Cybersecurity Workforce Framework

When degrees, jobs, training and certifications are aligned to the Workforce Framework:



Vision for the Nation's Cyber Workforce



Key Programs and Activities

- Advanced Technological Education (ATE) Centers (NSF)
- Centers of Academic Excellence (DHS/NSA)
 - 2Y Cyber Defense
 - 4Y Cyber Defense
 - Cyber Research
 - Cyber Operations
- CyberCorps[®] : Scholarship for Service
- NICE 2015: November 3-4 in San Diego
- National Cybersecurity Workforce Framework

Contact Info

- NICE Website: <http://nist.gov/nice>
- Bill Newhouse
 - 301-975-2869
 - william.newhouse@nist.gov