NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Federal Facilities Council Workshop

Bill Newhouse, Government Lead - NICE Program Office at NIST

NICE Strategic Plan Draft – Vision & Mission

(November 3, 2015)

- Vision: A digital economy that is powered by secure technologies, enabled by a skilled cybersecurity workforce, and used by risk-aware citizens and organizations.

- Mission: To foster, energize, and promote a robust network and an integrated ecosystem of cybersecurity education, training, and workforce development.

NICE Strategic Plan Draft - Values (November 3, 2015)

- **Seek Evidence** –inform actions or decisions with data whenever possible or pursue objective and reliable sources of information
- **Pursue Action** – strive for concrete steps towards deliverable outcomes to achieve mission and goals
- **Challenge Assumptions** –examine rationale for past and present approaches and apply critical analysis to solutions
- **Embrace Change** – seek creative and innovative solutions that might disrupt or defy the status quo
- **Stimulate Innovation** – inspire and test new approaches to education, training, and skills development
- **Foster Communication** – engage in information sharing and encourage openness to build trust and enhance effectiveness
- **Facilitate Collaboration** – connect or combine similar efforts to avoid duplication and maximize use of limited resources
- **Share Resources** – communicate, leverage, and support community-developed approaches and solutions
- **Model Inclusion** – encourage participation from diverse stakeholders and represent diverse backgrounds and viewpoints
- **Measure Results** –quantitatively and qualitatively assess the effectiveness of deliverables and program outcomes based on explicit goals

NICE Strategic Goal #1: Accelerate Learning and Skills Development

Invoke a sense of urgency in both the public and private sectors to address the shortage of a skilled cybersecurity workforce

Objectives:

- **1.1 Stimulate approaches and techniques that can more rapidly increase the supply of qualified cybersecurity workers**
- **1.2 Reduce the time and cost for obtaining knowledge, skills, and abilities for in-demand work roles**
- **1.3 Influence employers to shape job descriptions to reflect knowledge, skills, and abilities appropriate for tasks to be performed**
- **1.4 Pursue displaced workers or underemployed individuals who are available and motivated**
- **1.5 Identify and fill gaps in cybersecurity skills training to support identified workforce needs**

NICE Strategic Goal Goal #2: Nurture a Diverse Learning Community

Strengthen education and training across a multifarious ecosystem that prioritizes learning, emphasizes outcomes, and celebrates diversity.

Objectives:

- **2.1 Strengthen formal education programs, co-curricular experiences, training and certifications, and employer-based training**
- **2.2 Explore tools and techniques that effectively measure and validate individual aptitude, knowledge, skills, and abilities**
- **2.3 Inspire cybersecurity career awareness, exploration, and preparedness with students in elementary and secondary schools**
- **2.4 Encourage creative and effective efforts to increase the number of women, minorities, veterans, and underrepresented populations**
- **2.5 Build on institutional initiatives to improve student success by establishing academic pathways for cybersecurity careers**

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

Support job seekers and employers to address market demands and maximize talent management.

Objectives:

- **3.1 Identify and analyze data sources that project present and future workforce demand and supply of qualified cybersecurity workers**
- **3.2 Promote the National Cybersecurity Workforce Framework and encourage sector implementations**
- **3.3 Facilitate state and local consortium that identify cyber pathways that address local and national workforce needs**
- **3.4 Promote tools that assist human resource professionals and hiring managers with recruitment, hiring, promotion, and retention**
- **3.5 Explore international approaches that could inform practice in the United States and share NICE successes with other countries**

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

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 2016: November 2-3 in Kansas City, Missouri
- National Cybersecurity Workforce Framework

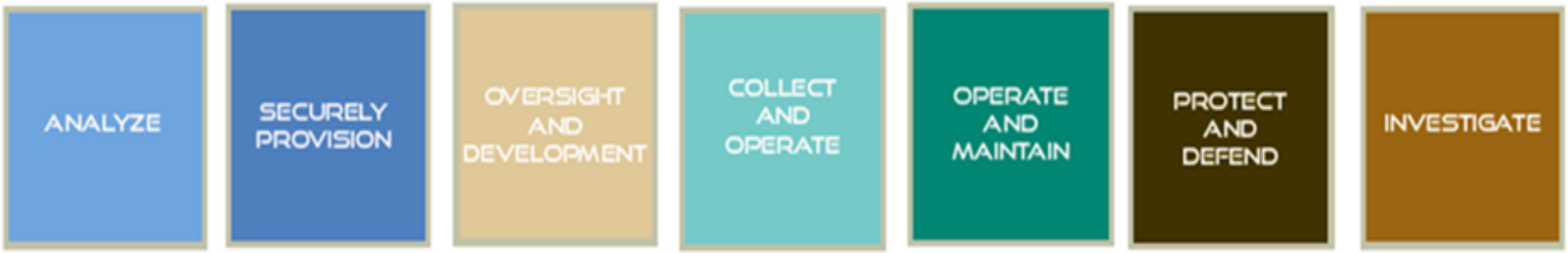
Outreach and Engagement: Government

- Government
  - Federal Departments and Agencies
  - State Governments
- Academia
  - Post-Secondary, 2 Year, 4 Year, Graduate, Research
  - Elementary and Secondary
- Industry
  - Employers of cybersecurity workforce
  - Specialized: IT sector, training and certification providers, etc.

The Foundation for our Nation's Cyber Workforce

The National Cybersecurity Workforce Framework

- 7 Categories, 30+ Specialty Areas
- Baselines knowledge, skills, and abilities & tasks
- Support for strategic workforce development



NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

National Cybersecurity Workforce 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.

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Vision for the Nation's Cyber Workforce

- **Educators** Align programs to jobs
- **Students** Graduate with knowledge & skills
- **Employers** Recruit from more qualified candidates
- **Employees** Identify career paths & opportunities
- **Policy makers** Set standards to promote the workforce

Common Understanding

Work Role.
A specialized set of tasks/functions requiring specific knowledge, skills & abilities.

Job/Position.
One or more work roles one regularly performs for pay.

Job Title.
A description of ones job/position in the organization.

Current & Planned
Cyber Workforce Issuances

DoD Cyberspace Workforce Strategy

NOTE:
DoD 8570.01-m is still in effect until such time as it is replaced

DoD Directive 8140.01
Cyberspace Workforce Management

Planned **- DoD Instruction 8140**
Cyber Workforce
Identification, Tracking & Report Requirements

DoD Cyber Workforce Framework
(Lexicon of Cyber Work Roles)

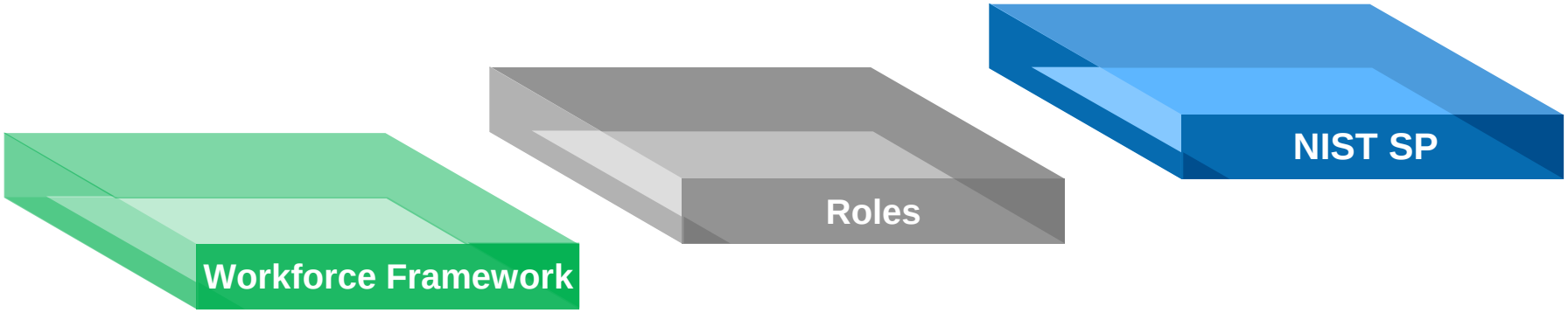
Planned **- DoD Manual(s) - Cyber Workforce Qualification Requirements**

Conceptual Qualification Methodology

- **Education**
- **Training**
- **Residency**
  - **O-J-T**
  - **Supervisor Evaluation**
  - **Performance-based Assessments***
- **Credentials***
  - **Certifications***
- **Continuous Development**
  - **Knowledge, Exercises, Skills Labs**

*Where applicable

Workforce Framework Evolution to NIST Special Publication



Establish structure for all cybersecurity work

- Organize work into Categories and Specialty Areas
- Describe tasks and KSAs required to execute work

Define roles to enable workforce development

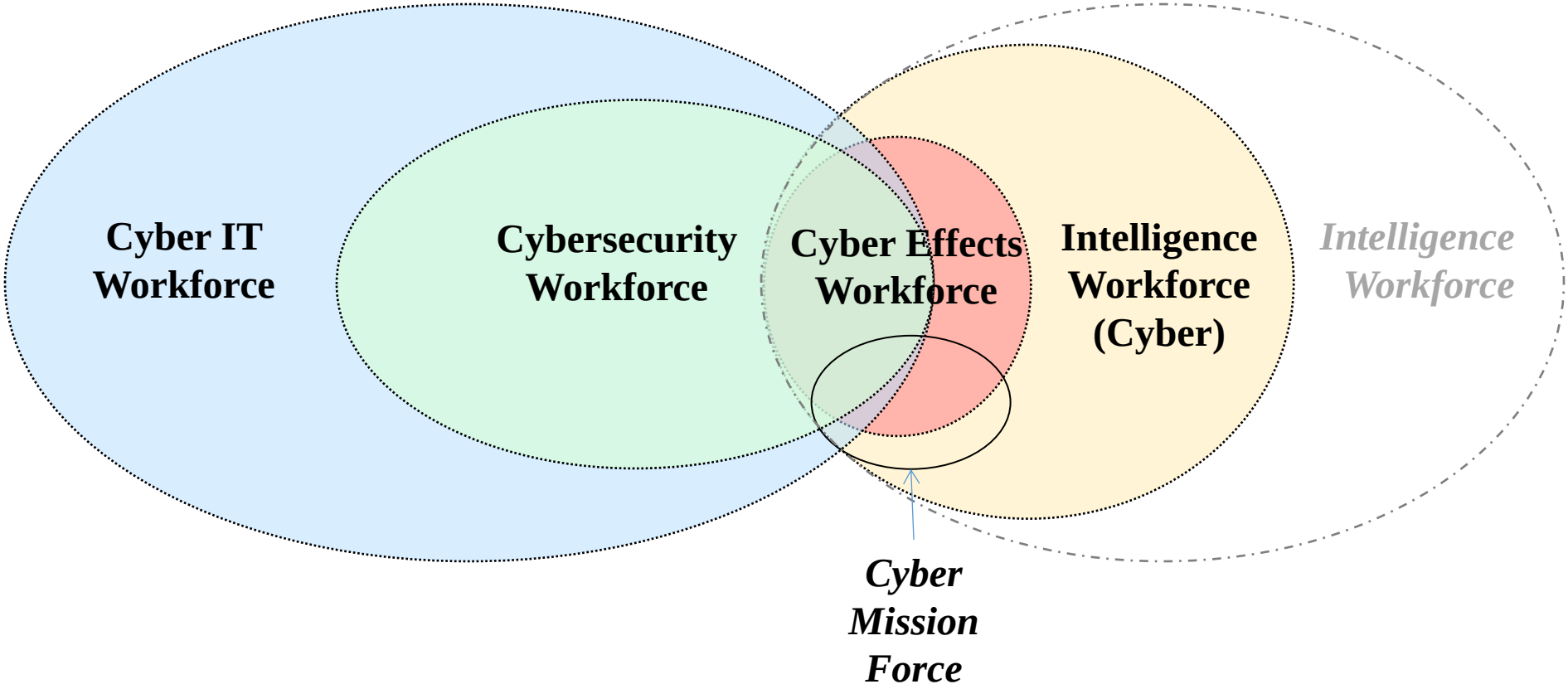
- Define most common cybersecurity roles
- Align roles to Workforce Framework

Consolidate Workforce Framework and Roles

- Drafting a Cybersecurity Workforce Framework that incorporates Roles, to be published as a NIST Special Publication

Cyber Workforce Notional Representation

Size not to scale



Definitions

Cyberspace Workforce

Personnel who build, secure, operate, defend, and protect DoD and U.S. cyberspace resources; conduct related intelligence activities; enable future operations; and project power in or through cyberspace. It is comprised of personnel assigned to the areas of cyberspace effects, cybersecurity, cyberspace IT, and portions of the Intelligence workforce

– (DoDD 8140.01 signed 11 Aug 2015)

Definitions
Cyber Workforce Skill Categories

Cyberspace IT Workforce: Personnel, who design, build, configure, operate, and maintain IT, networks, and capabilities. This includes actions to prioritize portfolio investments; architect, engineer, acquire, implement, evaluate, and dispose of IT as well as information resource management; and the management, storage, transmission, and display of data and information. (DoDD 8140.01 signed 11 Aug 2015)

Cybersecurity Workforce: Personnel who secure, defend, and preserve data, networks, net-centric capabilities, and other designated systems by ensuring appropriate security controls and measures are in place, and taking internal defense actions. This includes access to system controls, monitoring, administration, and integration of cybersecurity into all aspects of engineering and acquisition of cyberspace capabilities. - (DoDD 8140.01 signed 11 Aug 2015)

Cyberspace Effects Workforce: Personnel who plan, support, and execute cyberspace capabilities where the primary purpose is to externally defend or conduct force projection in or through cyberspace. - (DoDD 8140.01 signed 11 Aug 2015)

Intelligence Workforce (Cyberspace): Personnel who collect, process, analyze, and disseminate information from all sources of intelligence on foreign actors' cyber programs, intentions, capabilities, research and development, and operational activities. - (DoDD 8140.01 signed 11 Aug 2015)

Contact Info

- NICE Website: http://nist.gov/nice
- Bill Newhouse
  - william.newhouse@nist.gov