NARUC
Winter Committee Meetings

Committee
on
Critical Infrastructure
Cyber Workforce—Addressing the Gap

Panelists:
Aileen Alexander, Korn Ferry
Bill Newhouse, NIST
Mark Troutman, George Mason University
The National Initiative for Cybersecurity Education (NICE)

2017 Winter Committee Meetings of the National Association of Regulatory Utility Commissioners

Committee on Critical Infrastructure

February 12, 2017

Bill Newhouse, Deputy Director of NICE

Applied Cybersecurity Division, Information Technology Laboratory, National Institute of Standards and Technology (NIST)
National Initiative for Cybersecurity Education (NICE)

• Workforce Demand: http://nist.gov/nice/NICE_Workforce_Demand.pdf

• The NICE strategic plan http://csrc.nist.gov/nice/about/strategicplan.html

• The NICE Cybersecurity Workforce Framework http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-181

Resources

• NICE provide a grant to support the creation of Cyberseek http://cyberseek.org/

• The NICE Working Group and subgroups (K-12, Collegiate, Competitions, Training and Certifications, and Workforce Management) http://csrc.nist.gov/nice/nicewg/index.html
  – Forum to identify and share best practices that help us as a nation make progress towards the NICE Strategic goals and objectives.

• NICE provided grants for the creation of 5 Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS)
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*
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:

3.1 Identify and analyze data sources that support projecting present and future demand and supply of qualified cybersecurity workers

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

3.3 Facilitate state and regional consortia to identify cybersecurity pathways addressing local workforce needs

3.4 Promote tools that assist human resource professionals and hiring managers with recruitment, hiring, development, and retention of cybersecurity professionals

3.5 Collaborate internationally to share best practices in cybersecurity career development and workforce planning
NICE Cybersecurity Workforce Framework – Draft NIST SP 800-181

Cybersecurity Work Categories (7)

- 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

- Reference Resource for cybersecurity workforce development
As a mechanism to organize information technology (IT), cybersecurity, and cyber-related work, the NCWF helps organizations organize roles and responsibilities through the following components:

**Categories** – A high-level grouping of common cybersecurity functions;

**Specialty Areas** – Distinct areas of cybersecurity work;

**Work Roles** – 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.
National Initiative for Cybersecurity Education (NICE)


Resources

- Cyberseek [http://cyberseek.org/](http://cyberseek.org/) , built initially from a NIST/NICE grant to CompTIA/Burning Glass
  - Forum to identify and share best practices that help us as a nation make progress towards the NICE Strategic goals and objectives.
- NICE provided grants for the creation of 5 Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS)
## Securely Provision (7 Specialty Areas, 11 Work Roles)

<table>
<thead>
<tr>
<th>Category</th>
<th>Specialty Area</th>
<th>Work Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Management</td>
<td>Authorizing Official/Designating Representative</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Security Control Assessor</td>
<td></td>
</tr>
<tr>
<td>Software Development</td>
<td>Software Developer</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Secure Software Assessor</td>
<td></td>
</tr>
<tr>
<td>Systems Architecture</td>
<td>Enterprise Architect</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Security Architect</td>
<td></td>
</tr>
<tr>
<td>Technology R&amp;D</td>
<td>Research &amp; Development Specialist</td>
<td></td>
</tr>
<tr>
<td>Systems Requirements Planning</td>
<td>Systems Requirements Planner</td>
<td></td>
</tr>
<tr>
<td>Test and Evaluation</td>
<td>Testing and Evaluation Specialist</td>
<td></td>
</tr>
<tr>
<td>Systems Development</td>
<td>Information Systems Security Developer</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Systems Developer</td>
<td></td>
</tr>
</tbody>
</table>
## Operate and Maintain (6 Specialty Areas, 7 Specialty Areas)

<table>
<thead>
<tr>
<th>Category</th>
<th>Specialty Area</th>
<th>Work Role</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data Administration</td>
<td>Database Administrator</td>
</tr>
<tr>
<td></td>
<td>Knowledge Management</td>
<td>Knowledge Manager</td>
</tr>
<tr>
<td></td>
<td>Customer Service and</td>
<td>Technical Support Specialist</td>
</tr>
<tr>
<td></td>
<td>Technical Support</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network Services</td>
<td>Network Operations Specialist</td>
</tr>
<tr>
<td></td>
<td>Systems Administration</td>
<td>System Administrator</td>
</tr>
<tr>
<td></td>
<td>Systems Analysis</td>
<td>Systems Security Analyst</td>
</tr>
</tbody>
</table>
## Oversee and Govern (6 Specialty Areas, 14 Work Roles)

<table>
<thead>
<tr>
<th>Category</th>
<th>Specialty Area</th>
<th>Work Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oversee and Govern</td>
<td>Legal Advice and Advocacy</td>
<td>Cyber Legal Advisor</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Privacy Compliance Manager</td>
</tr>
<tr>
<td></td>
<td>Training, Education, and Awareness</td>
<td>Cyber Instructional Curriculum Developer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cyber Instructor</td>
</tr>
<tr>
<td></td>
<td>Cybersecurity Management</td>
<td>Information Systems Security Manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td>COMSEC Manager</td>
</tr>
<tr>
<td></td>
<td>Strategic Planning and Policy</td>
<td>Cyber Workforce Developer and Manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cyber Policy and Strategy Planner</td>
</tr>
<tr>
<td></td>
<td>Executive Cyber Leadership</td>
<td>Executive Cyber Leadership</td>
</tr>
<tr>
<td></td>
<td>Acquisition and Program/Project Management</td>
<td>Program Manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IT Project Manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Product Support Manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IT Investment/Portfolio Manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IT Program Auditor</td>
</tr>
</tbody>
</table>
### Protect and Defend (4 Specialty Areas, 4 Work Roles)

<table>
<thead>
<tr>
<th>Category</th>
<th>Specialty Area</th>
<th>Work Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect and Defend</td>
<td>Cyber Defense Analysis</td>
<td>Cyber Defense Analyst</td>
</tr>
<tr>
<td></td>
<td>Cyber Defense Infrastructure Support</td>
<td>Cyber Defense Infrastructure Support Specialist</td>
</tr>
<tr>
<td></td>
<td>Incident Response</td>
<td>Cyber Defense Incident Responder</td>
</tr>
<tr>
<td></td>
<td>Vulnerability Assessment and Management</td>
<td>Vulnerability Assessment Analyst</td>
</tr>
</tbody>
</table>
## Analyze (5 Specialty Areas, 7 Work Roles)

<table>
<thead>
<tr>
<th>Category</th>
<th>Specialty Area</th>
<th>Work Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analyze</td>
<td>Threat Analysis</td>
<td>Warning Analyst</td>
</tr>
<tr>
<td></td>
<td>Exploitation Analysis</td>
<td>Exploitation Analyst</td>
</tr>
<tr>
<td></td>
<td>All-Source Analysis</td>
<td>All-Source Analyst</td>
</tr>
<tr>
<td></td>
<td>Mission Assessment Specialist</td>
<td>Mission Assessment Specialist</td>
</tr>
<tr>
<td></td>
<td>Targets</td>
<td>Target Developer</td>
</tr>
<tr>
<td></td>
<td>Language Analysis</td>
<td>Multi-Disciplined Language Analyst</td>
</tr>
</tbody>
</table>
## Operate and Collect (3 Specialty Areas, 6 Work Roles)

<table>
<thead>
<tr>
<th>Category</th>
<th>Specialty Area</th>
<th>Work Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collect and Operate</td>
<td>Collection Operations</td>
<td>All Source-Collection Manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td>All Source-Collection Requirements Manager</td>
</tr>
<tr>
<td></td>
<td>Cyber Operational Planning</td>
<td>Cyber Intel Planner</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cyber Ops Planner</td>
</tr>
<tr>
<td></td>
<td>Cyber Operations</td>
<td>Partner Integration Planner</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cyber Operator</td>
</tr>
</tbody>
</table>
# Investigate (2 Specialty Areas, 3 Work Roles)

<table>
<thead>
<tr>
<th>Category</th>
<th>Specialty Area</th>
<th>Work Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigate</td>
<td>Cyber Investigation</td>
<td>Cyber Crime Investigator</td>
</tr>
<tr>
<td></td>
<td>Digital Forensics</td>
<td>Forensics Analyst</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cyber Defense Forensics Analyst</td>
</tr>
</tbody>
</table>
Cyber Workforce Education in Practice
A Critical Infrastructure (Lifeline Sectors) Perspective

National Association of Regulatory Utility Commissioners

Mark Troutman, Ph.D
Director, Center for Infrastructure Protection
George Mason University School of Business
mtroutma@gmu.edu
12 February 2017
About the Center for Infrastructure Protection

• Established at George Mason University in May 2002
• A research center as part of the School of Business since June 2015
• Specifically focused on the Private Sector – where over 80% of Critical Infrastructure Industries reside
• Located in Arlington, Virginia – Washington DC Metro Area
• Integrate the disciplines of policy, economics, business, law, and technology conduct comprehensive infrastructure protection research and education to improve the security and resilience of critical infrastructure industries
• A Think... Do... Teach organization
• Publish the monthly newsletter, The CIP Report, which highlights key infrastructure protection issues
Critical Infrastructure: “Assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on national security, economic security, national public health or safety, or any combination thereof.”

Security: “Reducing the risk to critical infrastructure by physical means or defensive cyber measures to intrusions, attacks, or the effects of natural or manmade disasters.” PPD 21

Resilience: “The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions...[it] includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.” PPD 21

16 Critical Infrastructure Sectors (Lifeline Sectors)
- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food & Agriculture
- Government Facilities
- Healthcare/Public Health
- Information Technology
- Nuclear Reactors, Materials and Waste
- Transportation Systems
- Water & Wastewater Systems
Education: Special Challenges of Infrastructure Protection

- Infrastructure Security and Resilience does not reside in a single department program; a unique area of security studies

- Infrastructure Security and Resilience is:
  - Interdisciplinary: Many different specialties
  - Interdepartmental/Interagency: Many different government departments
  - International: Crosses national boundaries
  - Intergovernmental: Different levels of government
  - Industry/Government: Private and Public Sector

- Identified Core Competencies (from 2009 NIPP)
  - Risk Analysis
  - Program Evaluation and Measurement
  - Protective Measures and Mitigation Strategy Development
  - Information Collection and Reporting
  - Technical and Tactical Expertise (Sector-Specific)
  - Program Management
  - Partnership Building/Networking
Education and Critical Infrastructure Protection

• Primary Education through High School
  – Basic Security Awareness – “See Something… Say Something”
  – **Cybersecurity Awareness and Online Safety**

• Technical School (Community College)
  – Technical Skills – Especially **Cybersecurity and Industrial Control Systems Security**
  – Critical Infrastructure Security Fundamentals

• Bachelors Degree (Baccalaureate)
  – Focus on operational management
  – Foundations of Critical Infrastructure Security
  – Risk Assessment and Mitigation
  – Partnerships and Information Sharing
  – **Cybersecurity and Future Trends (NICE Standards)**

• Advanced Degree (Post-Baccalaureate)
  – Transition from operations to strategic vision
  – Focus on management and leadership… **NICE (Workforce) NIST Cyber (Enterprise)**
  – Strategic Risk Assessment and Mitigation strategy development
  – Strategic resilience, business continuity, **Cybersecurity as a C and Board level function**
  – Partnership building at the local/state/federal level
48 credits – 42 core, 6 electives

Year One

Program Immersion

- Cohort Building
- Honor Code
- Academic Policies
- Tools for Teams

Module 1
Aug - Oct

- 653 Organizational Behavior
- 633 Statistics
- 6 credits total

Module 2
Oct - Jan

- 603 Managerial Econ
- 613 Financial Acct
- 7XX Track Course #1
  - 740 Intro to Global Bus
  - 741 Intro to Nat'l Security
  - 729 Intro to Critical Infra.
- 7.5 credits total

Module 3
Feb - Apr

- 612 Cost Accounting
- 643 Managerial Finance
- 6 credits total

Module 4
Apr - June

- 623 Marketing
- 703 Financial Markets
- 7XX Track Course #2
  - 742 Adv. Global Bus
  - 743 Adv. Nat'l Security
  - 733 Adv. Critical Infra
- 7.5 credits total

Year Two

Summer break

- July
- 1st half of August

Module 5
Aug - Oct

- 638 Operations Management
- 678 Business Strategy
- 750 Capstone – Part 1
- 7.5 credits total

Module 6
Oct - Jan

- 660 Management of IT
- 718 Leadership & Change Management
- 751 Corporate Strategy
- 7.5 credits total

Module 7
Jan - April

- 735 Systems Thinking
- 754 Capstone – Part 2
- 1-week Residencies (Mar)
  - EMBA 795 Global
  - EMBA 790 Natl. Sec.
  - EMBA 734 Crit Infra.
- 6 credits total

Graduation!

- Celebration Dinner
- Mid-May Ceremony

Capstone Presentations

Student Profile:

- Avg. Age: 40
- Avg. Professional Work Experience: 16
- Background: Varied
MS in Secure Information Systems (Cyber) Curriculum and Program Format

36 credits – 33 core, 3 electives

Year One

Module 1: Feb - Apr
- 520 Networking Principles (2)
- 620 Economics of Technology (2)
- 650 Enterprise Security Case Studies (1)
- Foundations of Cyber Security (2)

Module 2: Apr - June
- 511 Security Practices in the Enterprise (2)
- 620 Networking Security (2)
- 641 Innovation, Commercialization, and Entrepreneurship (2)
- 715 Capstone (1)

Module 3: Aug - Oct
- 614 Financial and Cost Accounting (2)
- 610 Organizations, MGMT, and Work (2)
- 643 Managerial Finance (2)
- 735 Capstone (2)
- 697 Special Topics (1)

Module 4: Oct - Jan
- 642 Enterprise Security Technologies (2)
- 611 Critical Infrastructure Protection (2)
- 750 Global Residency (3)
- 720 Capstone (2)

Module 5: Jan - April
- 630 Secure Info System Governance, Regulation & Compliance
- 611 Leadership and Change MGMT
- 711 Deriving strategic Value from IT Investments
- 641 Enterprise Security Threats
- 735 Capstone (2)

Summer Break
- July
- 1st half of August

Year Two

Module 3: Aug - Oct
- 614 Financial and Cost Accounting (2)
- 610 Organizations, MGMT, and Work (2)
- 643 Managerial Finance (2)
- 735 Capstone (2)
- 697 Special Topics (1)

Module 4: Oct - Jan
- 642 Enterprise Security Technologies (2)
- 611 Critical Infrastructure Protection (2)
- 750 Global Residency (3)
- 720 Capstone (2)

Module 5: Jan - April
- 630 Secure Info System Governance, Regulation & Compliance
- 611 Leadership and Change MGMT
- 711 Deriving strategic Value from IT Investments
- 641 Enterprise Security Threats
- 735 Capstone (2)

Student Profile:
- Avg. Age: 37
- Professional Work experience: 14 years
- Background:
Summary...

- Critical Infrastructure Security and resilience are shared outcomes of private industry and public sectors.
- "All Hazards" risk assessment and mitigation strategies are essential.
- Private Industry and Government have important role to ensure that critical infrastructure operations are safe, secure and resilient.
- Cybersecurity concerns are growing in all industries, especially Critical Infrastructure and "Lifeline" sectors.
- Cybersecurity education essential at all levels… Primary to Executive.
- Cyber security and critical infrastructure education is interdisciplinary and requires extraordinary critical thinking and problem solving skills.
- Partnership between Industry, Government and Academia are essential to create needed competencies and evolve them over time.
NARUC
Winter Committee Meetings

Committee on Critical Infrastructure