NARUC

Winter Committee Meetings

Committee on Critical Infrastructure

NARUC

Winter Committee Meetings

Cyber Workforce- Addressing the Gap

Panelists:

Aileen Alexander, Korn Ferry

Bill Newhouse, NIST

Mark Troutman, George Mason University

NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

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

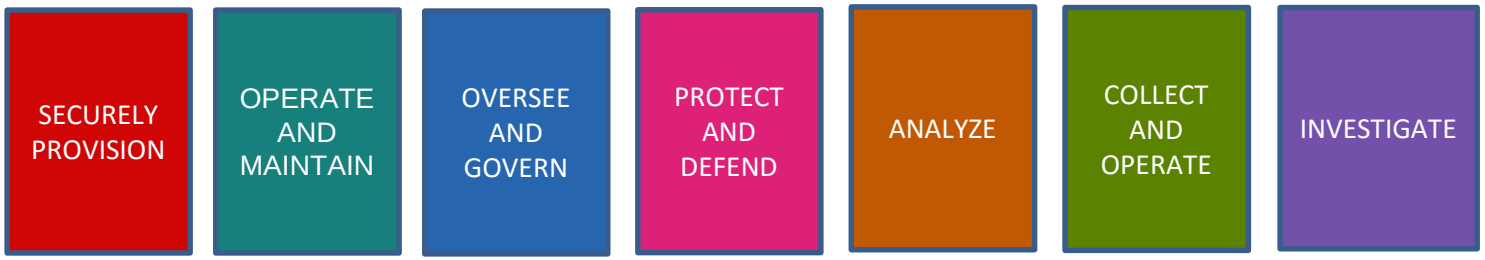
3.3 Facilitate state and regional consortia to identify cybersecurity pathways addressing local workforce needs

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)

- 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

- Cyberseek http://cyberseek.org/ , built initially from a NIST/NICE grant to CompTIA/Burning Glass
- 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)

Securely Provision (7 Specialty Areas, 11 Work Roles)

Category	Specialty Area	Work Role
Securely Provision	Risk Management	Authorizing Official/Designating Representative
		Security Control Assessor
	Software Development	Software Developer
		Secure Software Assessor
	Systems Architecture	Enterprise Architect
		Security Architect
	Technology R&D	Research & Development Specialist
	Systems Requirements Planning	Systems Requirements Planner
	Test and Evaluation	Testing and Evaluation Specialist
	Systems Development	Information Systems Security Developer
		Systems Developer

Operate and Maintain (6 Specialty Areas, 7 Specialty Areas)

Category	Specialty Area	Work Role
Operate and Maintain	Data Administration	Database Administrator
		Data Analyst
	Knowledge Management	Knowledge Manager
	Customer Service and Technical Support	Technical Support Specialist
	Network Services	Network Operations Specialist
	Systems Administration	System Administrator
	Systems Analysis	Systems Security Analyst

Oversee and Govern (6 Specialty Areas, 14 Work Roles)

Category	Specialty Area	Work Role
Oversee and Govern	Legal Advice and Advocacy	Cyber Legal Advisor
		Privacy Compliance Manager
	Training, Education, and Awareness	Cyber Instructional Curriculum Developer
		Cyber Instructor
	Cybersecurity Management	Information Systems Security Manager
		COMSEC Manager
	Strategic Planning and Policy	Cyber Workforce Developer and Manager
		Cyber Policy and Strategy Planner
	Executive Cyber Leadership	Executive Cyber Leadership
	Acquisition and Program/Project Management	Program Manager
		IT Project Manager
		Product Support Manager
		IT Investment/Portfolio Manager
		IT Program Auditor

Protect and Defend (4 Specialty Areas, 4 Work Roles)

Category	Specialty Area	Work Role
Protect and Defend	Cyber Defense Analysis	Cyber Defense Analyst
	Cyber Defense Infrastructure Support	Cyber Defense Infrastructure Support Specialist
	Incident Response	Cyber Defense Incident Responder
	Vulnerability Assessment and Management	Vulnerability Assessment Analyst

Analyze (5 Specialty Areas, 7 Work Roles)

Category	Specialty Area	Work Role
Analyze	Threat Analysis	Warning Analyst
	Exploitation Analysis	Exploitation Analyst
	All-Source Analysis	All-Source Analyst
		Mission Assessment Specialist
	Targets	Target Developer
		Target Network Analyst
	Language Analysis	Multi-Disciplined Language Analyst

Operate and Collect (3 Specialty Areas, 6 Work Roles)

Category	Specialty Area	Work Role
Collect and Operate	Collection Operations	All Source-Collection Manager
		All Source-Collection Requirements Manager
	Cyber Operational Planning	Cyber Intel Planner
		Cyber Ops Planner
		Partner Integration Planner
	Cyber Operations	Cyber Operator

Investigate (2 Specialty Areas, 3 Work Roles)

Category	Specialty Area	Work Role
Investigate	Cyber Investigation	Cyber Crime Investigator
	Digital Forensics	Forensics Analyst
		Cyber Defense Forensics Analyst

•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

A National View

GEORGE MASON UNIVERSITY | School of Business

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)

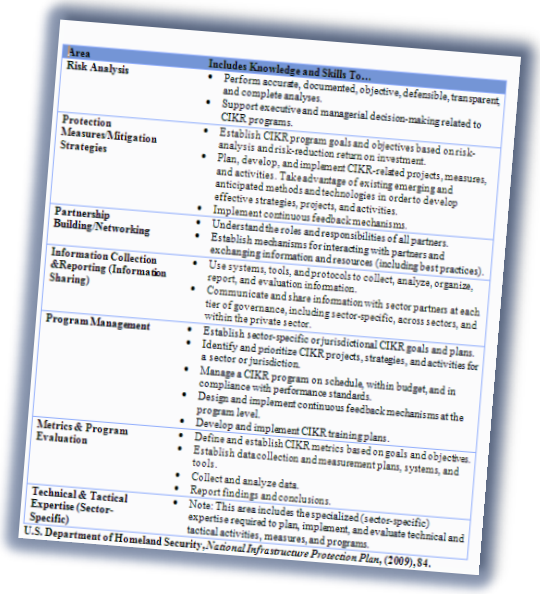
- Chemical
- Commercial Facilities
- ***Communications***
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- ***Energy***
- Financial Services
- Food & Agriculture
- Government Facilities
- Healthcare/Public Health
- Information Technology
- Nuclear Reactors, Materials and 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



Area	Includes Knowledge and Skills To…
Risk Analysis	• Perform accurate, documented, objective, defensible, transparent, and complete analyses. • Support executive and managerial decision-making related to CIKR programs.
Protection Measures/Mitigation Strategies	• Establish CIKR program goals and objectives based on risk-analysis and risk-reduction return on investment. • Plan, develop, and implement CIKR-related projects, measures, and activities. Take advantage of existing emerging and anticipated methods and technologies in order to develop effective strategies, projects, and activities. • Implement continuous feedback mechanisms.
Partnership Building/Networking	• Understand the roles and responsibilities of all partners. • Establish mechanisms for interacting with partners and exchanging information and resources (including best practices).
Information Collection &Reporting (Information Sharing)	• Use systems, tools, and protocols to collect, analyze, organize, report, and evaluation information. • Communicate and share information with sector partners at each tier of governance, including sector-specific, across sectors, and within the private sector.
Program Management	• Establish sector-specific or jurisdictional CIKR goals and plans. • Identify and prioritize CIKR projects, strategies, and activities for a sector or jurisdiction. • Manage a CIKR program on schedule, within budget, and in compliance with performance standards. • Design and implement continuous feedback mechanisms at the program level. • Develop and implement CIKR training plans.
Metrics & Program Evaluation	• Define and establish CIKR metrics based on goals and objectives. • Establish data collection and measurement plans, systems, and tools. • Collect and analyze data. • Report findings and conclusions.
Technical & Tactical Expertise (Sector-Specific)	• Note: This area includes the specialized (sector-specific) expertise required to plan, implement, and evaluate technical and tactical activities, measures, and programs.

U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, (2009), 84.

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

EMBA Curriculum and Program Format

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*

Observe Capstone

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

Program Immersion

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

Module 1
Feb - Apr

- 520 Networking Principles (2)
- 620 Economics of Technology (2)
- 650 Enterprise Security Case (2) 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)

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
- Cyber security 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