21st Annual National Defense Industrial Association
Systems and Mission Engineering Conference

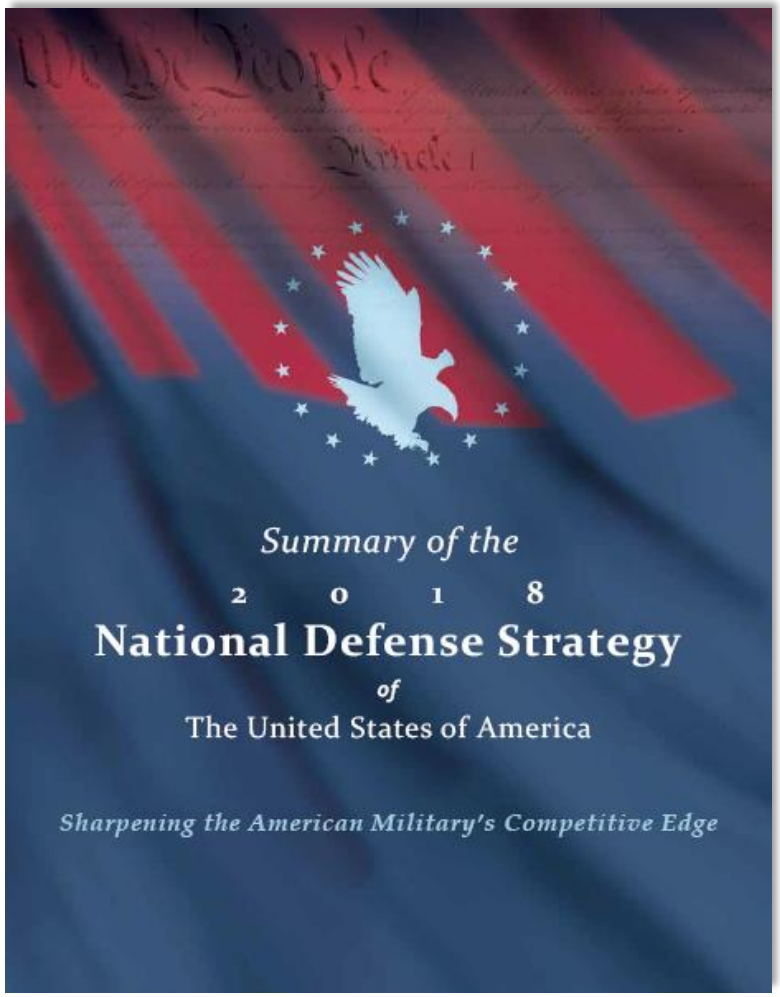
Engineering Cyber-Resilient Weapon Systems (CRWS) Workforce Development Workshop

Melinda Reed

Office of the Under Secretary of Defense for Research and Engineering

October 2018

Digital Environment Demands a Change



2018 National Defense Strategy

"Civilian workforce expertise. A modern, agile, information-advantaged Department requires a motivated, diverse, and highly skilled civilian workforce. We will emphasize new skills and complement our current workforce with information experts, data scientists, computer programmers, and **basic science researchers and engineers** — to use information, not simply manage it."

Diverse Weapon System Ecosystem Environments – to Include Cyberspace

Weapon System Ecosystems are complex – education and training needed to overcome challenges driven by application of general purpose requirements

Engineering Cyber-Resilient Weapon System Workforce Development

Problem Statement:

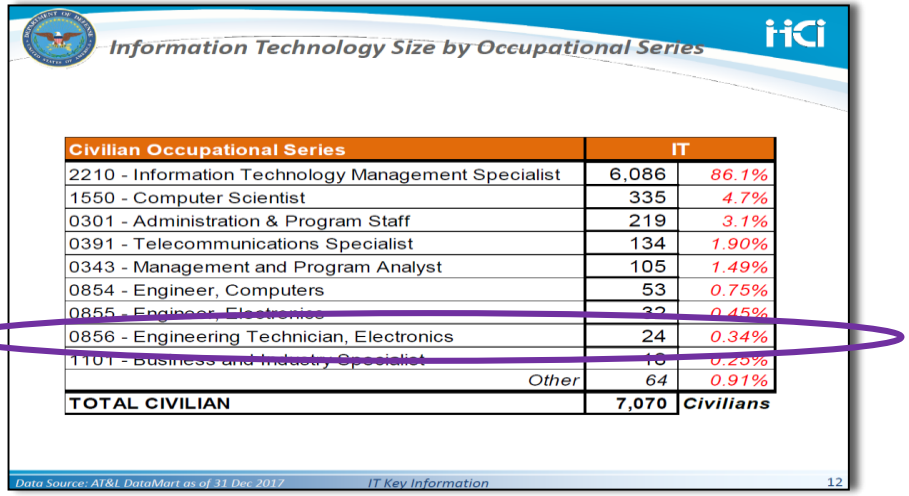
- *The evolving and complex nature of the challenges presented by critical systems operating in contested cyberspace environments requires unique skills beyond those addressed by information technology security education.*
- *DoD must develop the ability to engineer and assess the combined safety, security, and resilience in current and future systems in the presence of determined cyber adversaries.*

Workshop 6 (Jul 31– Aug 2 2018)
State of the Engineering Workforce; Cybersecurity Engineering

Goal: Identify skill sets and curriculum needs for our current and future engineering workforce

- **Understand engineering education gaps related to cybersecurity**
- **Develop Need's for today's engineering workforce**
- **Develop Need's for tomorrow's engineering workforce**

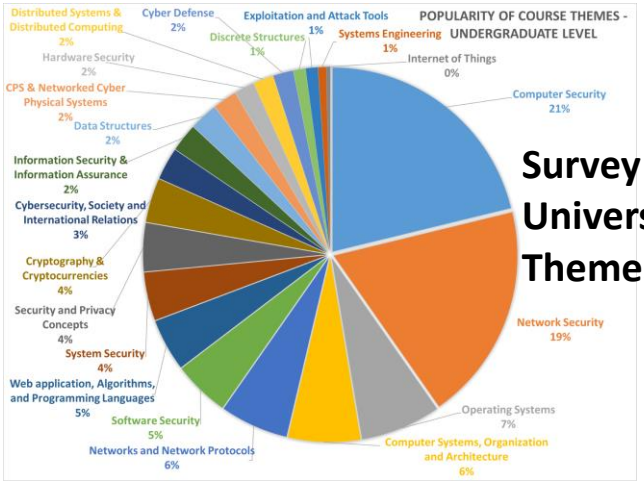
Sponsored by the SERC



Information Technology Size by Occupational Series

Civilian Occupational Series	IT	
2210 - Information Technology Management Specialist	6,086	86.1%
1550 - Computer Scientist	335	4.7%
0301 - Administration & Program Staff	219	3.1%
0391 - Telecommunications Specialist	134	1.90%
0343 - Management and Program Analyst	105	1.49%
0854 - Engineer, Computers	53	0.75%
0855 - Engineer, Electronics	32	0.45%
0856 - Engineering Technician, Electronics	24	0.34%
1101 - Business and Industry Specialist	18	0.25%
Other	64	0.91%
TOTAL CIVILIAN	7,070	Civilians

Data Source: AT&L DataMart as of 31 Dec 2017 IT Key Information 12



Survey of 104 Universities by Cours Themes

Composition and Approach
3 Panels, 2 Breakout Sessions

- **3 Perspectives**
  - DoD
  - Academia
  - Industry
- **Diverse Organizations**
  - Army
  - Navy
  - Air Force
  - Missile Defense Agency
    National Security Agency
    Industry
  - FFRDCs
  - Defense Acq University
- **Diverse Expertise**
  - Hardware Specialists
  - Software Specialists
  - Intelligence
  - Counterintelligence
  - Safety specialists
  - Anti Tamper Specialists
  - Systems Engineering
  - Technologists
  - Implementers

3 Panels

- **Panel 1: Government Engineering Workforce Challenges**
  - Air Force, Army, Navy, DAU Perspectives
- **Panel 2: Academic Programs**
  - University of Virginia, Georgia Institute of Technology, Embry Riddle (Aeronautical University)
- **Panel 3:How to Address the Challenges (Academia/Industry)**
  - Systems Engineering Research Center, Boeing, University of Connecticut

2 Breakout Sessions

- **Breakout Session 1:** Understand engineering education gaps and current needs related to cybersecurity
- **Breakout Session 2:** Anticipate and develop needs for tomorrow's engineering workforce

Diverse Expectations and Perspectives

Breakout Session Questions

Breakout Session 1

GOAL: Understand engineering education gaps and current needs related to cybersecurity

- What are the distinguishing characteristics of defense related engineered systems with respect to security education, skills, and competencies?
- What are the primary experienced gaps in workforce processes, competencies, and qualifications today?
- How do educators view these challenges and what are the primary ideas to address them?

Breakout Session 2

GOAL: Anticipate and develop needs for tomorrow's engineering workforce

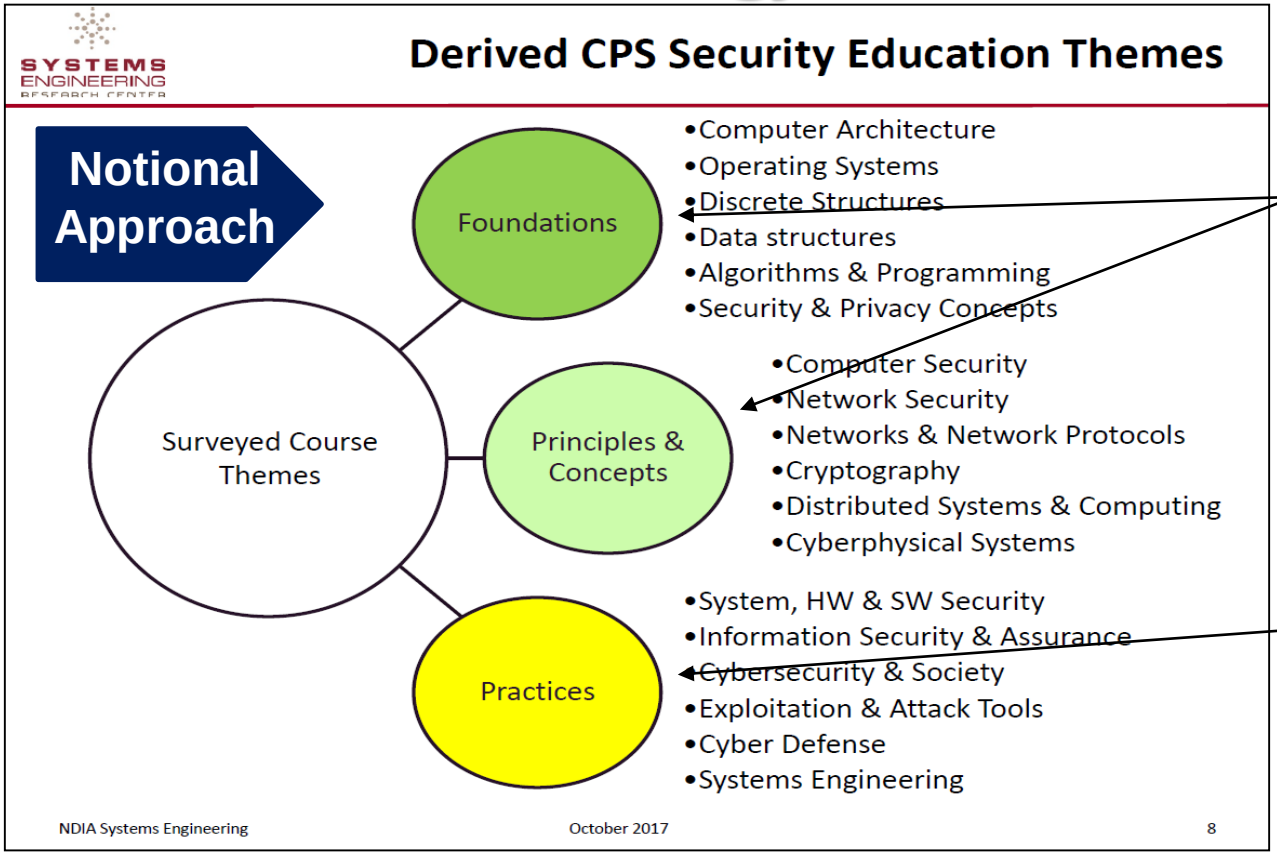
- In the context of engineered systems, at what levels should security education be addressed?
- What background competencies are needed to prepare students for that education?
- What are the types of curricula that would support the education needs? List some specific examples.
- How and where will people learn? What types of facilities and laboratories are necessary to meet the education challenges?

Participants placed into 4 Groups; Each Responded to Same Questions

Breakout Session Observations

- **Taxonomy**
  - Establish and extend security conceptual understanding
    - Deconflict security terminology
  - Work within existing engineering taxonomy rather than create something that is referred to as “cyber”
- **Fundamental principles of security are critical**
  - How do we design an inherently secure system?
    - Set of comprehensive security objectives
    - Simple rules and principles to drive models and design
  - Design Guidance
    - Has to be detailed enough to be useable but not too large to inhibit use
    - Must capture the concepts of malice and subversion
- **Education and Training are Different – We Need Both**
  - More flexibility with Master’s programs
  - Research projects drive education
  - Role of certification
- **Education/Training Needs and Priorities**
  - Policy and Governance
  - Program Execution
  - Prime contractor
- **Metrics**
  - Technical performance measures/metrics may suffice in near term
  - Need Basis to Demonstrate claims of “cyber resilient”
- **Testing**
  - Tools are not scalable and availability is growing faster than ability to put them to good use

Use Observations as Basis for Strategy and Roadmap



Foundations, Principles & Concepts

- **Integrate across specialty and security domains**
- **Broad applicability for application**

Practices capture application in "type-specific" context

- **Weapon system**
- **Capability**
- **Architecture and design patterns**
- **Technology**
- **Assurance**

Academia provides education on what we accept as standardized knowledge

Standardized knowledge must reflect set of principles that are standardized practice by industry and government

Next Steps

- SERC to Finalize Report on Education for Engineering Cyber-Resilient Weapon System Findings and Recommendations

- Develop Engineering Cyber-Resilient Weapon System Workforce Education and Training Strategic Roadmap

- Standardize knowledge for Engineering Cyber-Resilient Weapons System
  - Return to the Principles of Security Design
  - Principles of Security Design must be reflected in a design model

DoD Research and Engineering Enterprise
Solving Problems Today – Designing Solutions for Tomorrow










For Additional Information

Melinda Reed

Office of the Under Secretary of Defense for Research and Engineering

571.372.6562 | melinda.k.reed4.civ@mail.mil