WORKSHOP REPORT

Cyber Resilient Weapon Systems Workshop #6

– Preparing the Engineering Workforce for Cybersecurity Challenges

July 31 – August 2, 2018

Tom McDermott (SERC)
Melinda Reed (OUSD(R&E))
Michael McEvilley (MITRE)

SYSTEMS ENGINEERING RESEARCH CENTER

TABLE OF CONTENTS

INTRODUCTION

This workshop was the 6th in a series of U.S. Government workshops on engineering Cyber Resilient Weapon Systems (CRWS). The objective of this workshop was to develop a roadmap for education and training of the today's and tomorrow's engineering workforce in response to challenges presented by cyberspace. This workshop was hosted by the Systems Engineering Research Center (SERC) in order to engage across the government, academia, and industrial communities to leverage their combined interest and expertise in education and training.

The evolving and complex nature of the challenges associated with the engineering of dependable weapon systems for operation in contested cyberspace environments requires skills beyond those addressed by information technology and associated security education. The Department of Defense must develop the ability to engineer and assess the combined safety, security, and resilience in current and future weapon systems in the presence of determined cyber adversaries. The general goal of this workshop was to start the process of identifying skill sets and curriculum needs for the future defense government and contractor workforce. Specific goals of the workshop were to:

- Understand engineering education gaps related to cybersecurity
- Develop needs for today's engineering workforce
- Anticipate and develop needs for tomorrow's engineering workforce

Engineering resilient systems is viewed as a systems engineering (SE) challenge. This challenge spans all environments of operation inclusive of cyberspace, and all types of systems to include defense systems, with weapon systems comprising the specific focus of the CRWS 6 workshop. The SERC was asked to host and facilitate this workshop due to its broad relationship with engineering academia and its core mission as the primary engine for the U.S. government in SE research. The SERC mission is three-fold, to:

- Catalyze community growth among SE researchers and end users by enabling collaboration among many SE research organizations (who),
- Accelerate SE competency development through rapid transfer of its research to educators and practitioners (how),
- Transform SE practice throughout the government by creating innovative methods, processes, and tools that address critical challenges to meeting mission outcomes (what).

The collaboration in CRWS #6 between the Office of the Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE)) and the SERC along with industry organizations such as the National Defense Industries Association (NDIA) created a deep conversation between government, industry, and academia.

1.0. WORKSHOP AGENDA, STRUCTURE, AND AUDIENCE

The MITRE Corporation hosted the workshop at their conference facility in McLean, Virginia. Over 90 participants attended. The structure of the workshop was crafted to allow significant interchange and dialogue, with three panel discussions and two breakout sessions. The Agenda over two days is provided in Section 6.0. A third ½ day "hotwash" with government and academia principals was held to capture key actions and next steps.

Each breakout session was organized into four breakout groups. All breakout groups addressed the following common set of questions:

- **Breakout Session 1:** Understand engineering education gaps and current needs related to cybersecurity

  Question 1: What are the distinguishing characteristics of defense related engineered systems with respect to security education, skills, and competencies?

  Question 2: What are the primary experienced gaps in workforce processes, competencies, and qualifications today?

  Question 3: How do educators view these challenges and what are the primary ideas to address them?

- **Breakout Session 2:** Anticipate and develop needs for tomorrow's engineering workforce

  Question 1a/b: 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?

  Question 2: What are the types of curricula that would support the education needs? List some specific examples.

  Question 3: How and where will people learn? What types of facilities and laboratories are necessary to meet the education challenges?

The presentation materials were distributed to the meeting attendees. Requests for additional presentation materials should be addressed to Mr. Michael McEvilley (mcevilley@mitre.org). The output of the workshop was a large set of collected data in the breakout sessions and a set of actions and next steps identified in the Day 3 hotwash.

2.0. BREAKOUT SESSION RESULTS

The breakout session proceedings were captured as discrete statements, which were further refined and categorized into a set of mindmaps. The outline summary of the mindmap data is included in the appendix. The following sections presents a narrative summary of the results of the breakouts.

2.1. DISTINGUISHING CHARACTERISTICS OF DOD ENGINEERED SYSTEMS

In understanding engineering education gaps and current needs related to cybersecurity, one must address the characteristics of defense related engineered systems. DoD engineered systems have the following distinguishing and unique characteristics:

- the purpose that drives their system capabilities, characteristics, and performance measures,
- the potentially catastrophic effects associated with the failure to perform as intended,
- the mission context that drives their deployment and lifecycle management concerns,
- the engineering/development model that drives analysis and trades across the engineering disciplines.

Engineering domain knowledge, methods, and tools have not yet fully addressed the effect cyberspace has on for designing and evaluating safe and secure achievement of capability performance measures; and the knowledge, methods and tools in the Information Technology (IT) arena are not sufficient to address all the needs of DoD Weapon Systems. As a result CRWS education challenges must address the unique aspects of these systems and prepare the engineering community to address them in the Weapon System domain. The following characteristics set the stage for discussion of CRWS education and training gaps and needs.

DoD systems have a unique purpose: Because lethality is an end result of many of these systems, there is a dominant focus on safety. Processes to address security and resilience must be interrelated with safety.

DoD system characteristics: DoD systems employ combinations of real-time embedded systems, complex control systems, and interconnected information systems. Academia and industry now call these cyber-physical systems, although this term only partially reflects the complexity and uniqueness of DoD systems. Many systems have complex functionality, making cyber threat detection, system state monitoring, etc. a challenge of scale. Safety, dependability, and security need to be integrated together in the design process. The concept of "cyber resilience" must consider the effects of the cyber threat in a mission and operational context and balance the system design characteristics with the planned operational use. Multiple levels of classified data and ensuring their separation make for further challenges, driving a need to architect and design appropriate protection mechanisms. However, the system design characteristics of embedded and cyber-physical systems are very different than typical IT systems and must be linked closely to the engineering disciplines in system design. Cybersecurity education and training are not prevalent in the engineering skill codes yet, which must be addressed. In addition, cyber resilience drives an evolution of roles and responsibilities in the systems engineering domain, opening a number of gaps and challenges that were discussed in this workshop.

DoD systems have a unique mission and context: The operational context and mission of defense related engineered systems is different than those of the commercial world. DoD systems operate in contested environments and engineers must be trained to understand the ramifications and effects of attacks conducted in cyberspace. Engineers working on defense systems must have domain experience that includes the operational and mission context as well as the technical experience for the systems or subsystems they are developing and supporting. The end user (warfighter) is also different than general users. This includes cybersecurity aspects, which today is a domain area with limited numbers of experts. Both the lethality and warfighter capability needs have dissimilar quantifications of risk and cost models versus commercial systems. Mission resiliency is critical and must be addressed in a total mission context where continuity of operations has a unique perspective in the DoD. The unique mission and context place different education and training requirements than many other domains, and also require a total systems focus that emphasizes systems thinking and systems engineering methods and tools.

DoD system deployment and lifecycle management differ from commercial systems: DoD systems includes those on the forward edge of the battle area. The missions require deployment in close proximity to the enemy. That forward edge deployment allows the adversary to interact with the systems regardless of the global or tactical nature of their connectivity, and drives the need to think of different ways of doing things based on the nature of the connectivity. DoD systems can no longer rely on physical security ("we can't just say that the server is behind some machine room door and we don't have to worry about network security").

Lifecycle management for DoD systems does not align with that of commercial systems lifecycle management. This suggests that methods suitable for commercial systems cannot be applied to DoD systems with the assumption of equivalent results and effectiveness. DoD must address the operation of mixed new and legacy systems, each with longer and varying refresh periods. Many of the systems are isolated or are not connected to networks for long periods of time; any such connectivity may not be predictable. It is unrealistic with current DoD systems to assume that they can be patched regularly or that they are operated in a known secure and safe system-of-systems environment. Therefore, updates to these systems must be planned and synchronized within the limits dictated by operational constraints associated with mission execution. System refresh or update cycles are significantly longer than commercial systems, and hardware lifecycles can be much longer. Getting systems and software out the door first (the minimum viable product) cannot succeed in this environment but that is the model most students are learning today. DoD technology and software will always lag behind commercial, and engineers must adapt to outdated languages, processes, tools, and technology. One cannot assume security is an update in a future release. This mindset needs to be created early on in engineering education.

The nature of DoD system deployment and total system environment across the total system lifecycle must be considered in all SE activities. This requires understanding security and resilience concepts and how they apply to system architecture, design, operational use, supply chain, maintenance activities, and other needs critical to successful operations.

DoD Culture and workforce: There was acknowledgement in the workshop that the DoD culture is different than academia and industry and may present barriers to effectively addressing security and resilience. Cybersecurity practices benefit from information sharing but the DoD culture in addressing security is typically compartmentalized. Often new information about threats, attacks, incidents, impacts, and effective countermeasures is classified, further compounding the information sharing issues. This impedes effective information flow, sharing of bodies of knowledge, and collaboration on common issues. Building domain knowledge on the classified nature of the threat, attack, incidents, and impact – both training on the need for classification and to prevent over-classification – are unique aspects of DoD systems. This makes security education in the CRWS domain just a start, significant training, experience, and accumulation of domain knowledge will also be critical.

2.2. PRIMARY EXPERIENCE GAPS IN WORKFORCE

For the current workforce, there are primary cybersecurity experience gaps in processes, competencies, and qualifications. These gaps start with competencies at the enterprise level, where program management understanding of CRWS technical aspects must be developed. These include:

- Understanding of basic security tenets (e.g., access control) and their proper integration in weapon systems.
- Translating consequences/awareness of the cybersecurity situation to program management, to be addressed with education of cyber consequences, which translate vulnerabilities into ramifications for the delivery of capability that in turn has mission ramifications.
- How to properly identify, assess, and accept or mitigate cybersecurity risk
- Who has “authority” to accept risk – PM’s live in the acquisition world and are used to accepting acquisition risk but less versed in operational risk.
- Leadership must promote red team conversations with system and program staff - to identify vulnerabilities early.
- Weapon systems expertise is more siloed. PM’s need more system level understanding. The role of systems security engineering has changed, is more critical, and needs to be better addressed with education and training.

Programs lack dedicated cybersecurity experts, particularly those with required clearances. Systems engineering is not addressing security well enough and is not addressing the specific concerns of security emerging in today’s embedded and cyber-physical systems. Programs have gaps in cybersecurity domain and context knowledge at each level across different functional and lifecycle concerns. For instance, program management should have an understanding of cybersecurity technical aspects while the test community should be knowledgeable of software code acceptance practices. Another gap is in vulnerability and risk assessment. Certain processes and analyses are not widely understood nor sought for complete examination of the system. There is also a clear gap amongst incoming engineers and their understanding of software security versus those that are seasoned and have great domain experience with little cybersecurity awareness. There is not a fluid comprehension of tools that are current and those that whose use is limited to older systems. These range from the concept of attack trees to software code scanning tools and their effectiveness. Every engineer should get basic software assurance experience, learn common types of cyber security problems, and understand the concepts of software and system security testing. These should be applied at early stages of education. In addition to the tools, shared knowledge on the latest tools and methods is needed to account for the rapid changes that are the nature of the cybersecurity industry and the adversary.

Qualification and certification approaches for cybersecurity need to be developed and trained, at the proper clearance levels. The workshop participants were not able to express the need, existing IT certifications are a hammer to use but are only partially relevant to CRWS. The IT community has a large body of knowledge, education, and certification practices that must be adapted to the CRWS domain.

Industry standards and guidance must also be interpreted and applied or developed for the CRWS domain. Information and cybersecurity standards and guidance in recent years have evolved in the IT domain and certifications are oriented toward IT professionals. DoD policy that employs the Risk

Management Framework for DoD IT is informing, but unique criteria and training are needed for CRWS. While the NIST Special Publication 800-160 on Systems Security Engineering is a comprehensive guide, it's focus is directed to the Federal IT community. The System Security Engineering needs for the DoD are to be supplemented with specific practices and training in the Defense Acquisition Guidebook on System Engineering.

Other gaps include system security engineering in general. Cybersecurity bodies of knowledge and systems bodies of knowledge overlap too little and need to be integrated. It was acknowledged that while this is a systems issue, SE is still not a major topic in the education communities that address cybersecurity. Use cases in the CRWS domain need to be shared. The SE community and all engineering disciplines need to become aware of fundamental security principles. The hardware and software supply chain and their security are critical to resilient operations, supply chain practices also need to become core knowledge. Engineering can help improve knowledge of fundamental computing principles and aid the IT community, but broad sets of computing architectures and languages need to be addressed.

The DoD has to compete with commercial industry for an engineering talent pool whose numbers are insufficient to meet the demand across the application areas of cyber-physical and embedded systems. The growth in investment in the Internet of Things (IoT) and other commercial embedded systems (driverless cars, etc.) will place an increasingly high demand for cybersecurity-cognizant engineers in the commercial sector. When coupled with the development of cybersecurity certification, turnover within DoD will be high. This forecast gap must be addressed with a range of education opportunities such as internships, experimentation, and real world use cases.

2.3. EDUCATORS' VIEW ON CHALLENGES AND ADDRESSING GAPS

Understanding engineering education gaps and current needs related to cybersecurity should also be addressed through the viewpoint of educators in terms of the challenges and the principal ideas to address them. Fundamentally, educators can solve the problem at hand, however, they too are also limited by external factors such as curriculum, credit hours, and ability to incorporate impactful adjustments to satiate current and future gaps. Given the distinguishing characteristics for a defense related engineered system, there must be more research opportunities to direct academics to develop more education and training with integrated subject matter expertise from the field, and the ability to transfer progress to educators. With the continual communications between educators and defense, the curriculum can be modified according to real world challenges and suit a more tiered approach since there is no single solution for academia. For instance, education that covers the policy basis for defense related systems would aid in understanding the relevant policies and contract regulations that directly affect security, and perhaps enhance the engineering effectiveness in delivering solutions. In order to bridge the communication barrier, the differences in how government and academic enterprises and systems operate must be addressed so that educators are able to care enough to overcome challenges working with DoD, and vice versa. Universities and community colleges in close proximity to DoD bases are good places to start. Universities also follow research and there is little research funding going into the CRWS area at this point.

Academia must learn the need and value of cybersecurity as well. Universities and colleges should build cybersecurity into their general curriculum to build a common foundation for all students. Cybersecurity awareness is appropriate for everyone; however cybersecurity awareness should be integrated in to foundational courses to ensure it is taught in relevant context. This approach is more effective than teaching cybersecurity awareness as a separate class. The concepts are easier to understand when cybersecurity is taught in context of the curricula for other disciplinary classes. Use cases are an important learning tool, but the development of relevant use cases is difficult because of fear of giving away proprietary information. Making use cases widely available could be an area where the DoD could provide a useful service. The graduate level is appropriate to introduce classes that are dedicated to specialized topics in cybersecurity (also easier to get faculty to agree to teach due to scheduling and expertise challenges).

2.4. ADDED LEVELS OF SECURITY EDUCATION AND BACKGROUND COMPETENCIES

A broad message from the breakout sessions is to fold in cybersecurity to the curriculum at various levels appropriate to the education grade level and the nature of the discipline. Foundational principles can be taught from an early age and developed in a tiered effort to tailor a specific discipline and eventual position. An example of that would be as STEM initiatives increase, systems thinking principles can be taught as early as primary school. Robotics and robotic challenges have seen marked increases, providing great impact on the building blocks for cybersecurity in domains that are closer to CRWS. With added cybersecurity challenge competitions, the inclusion of courses and/or tournaments on hacking can illustrate the need for solid, secure coding and architecture. In undergraduate education, more rigorous foundational principles can be introduced as well as specialized content for the determined discipline — whether that be financial engineering, mechanical engineering, engineering management, architect, and more. There should be increased efforts for PhD's in systems engineering with cyber-physical system security foci. With other disciplines, reverse engineering is not as focused as it could be, and professional continuing education should be routinely reworked and evaluated. Subject matter experts should be involved in helping to regularly shape curricula that is relevant, incorporating the appropriate use case scenarios, and continuing to press towards future solutions.

2.5. CURRICULA TO SUPPORT EDUCATION NEEDS

Adding to, or enhancing, the current curriculum is one way to confront the educational needs to close the gaps and challenges cybersecurity is facing today. Certain courses that address secure systems design and architecting, software testing, and cyber can be incorporated with focused rigor on modeling, coding, and analytical problem solving skills. Students could also be acquainted with cybersecurity in courses such as circuits. Though one can propagate change through the current curriculum, there should also be a change in enterprise for both the DoD and academia. For instance, rather than simply defining the curriculum, it would be better to establish the learning objects or knowledge units (KUs). The Centers for Academic Excellence (CAEs), which NSA and DHS use, have criteria that have basic KUs that meet the required knowledge sets. With these, agencies should communicate with one another and review and update the KUs regularly. Also, better communication could help illustrate the current and future needs, so academia could accommodate to continually improve education and prepare the workforce. Bounding the problem for the systems engineer would also support the education needs. A framework for SE jobs including what they need to know, or even Security Systems Engineering competency job classes, could alleviate evolving gaps and challenges.

Some examples of knowledge areas and educational opportunities include:

- System security engineering in systems engineering programs. Including a strong background in functional analysis, security architecting, interface security and control, concepts of software code structure, and software and system evaluation and test.
- Experience in attack and defend teams, attack trees and attack surface identification. This can be combined with cyber tabletops that provide an operational context for learning.
- Modeling of any kind. Particularly modeling safety and security aspects using tools such as root cause analysis, fault trees, failure modes and effects analysis (FMEA), System Theoretic Process Analysis (STPA) etc.
- Methods for deploying secure systems and updating them once deployed.
- Hardware and software reverse engineering.
- Soft skills and Emotional Intelligence (EI). Very important for the virtual, on-line world.
- Testing in its unit, integration, systems, and penetration test forms.

- Certification curriculum - determine curricula to acquire certifications (renewable) complemented by curricula to get degrees (single events).

2.6. HOW AND WHERE WILL PEOPLE BE EDUCATED?

Establishing the curriculum, or goal of the curriculum, is necessary, but how and where people learn is also critical to the success of developing tomorrow's workforce. The varying modes in which content is delivered is important. Hands-on, practical applications can help engrain the materials and lessons learned. However, online programs can be easily accessed and allow for scalability. Looking at the delivery methods and improving each to have sufficient materials to convey best practices would potentially require a change in approaches to education for both academia and the DoD. Creating relationships between laboratories, other cybersecurity test ranges, and universities would open up the availability for both hands-on and online. It also could help elevate the case studies to be more relevant while enabling rapid-prototyping for different classes as challenges arise with cybersecurity. This, in turn, helps academia learn the need and worth of cybersecurity. Internships, on-the-job mentoring, and the ability for designers to see their product in operation are essential, but the different constraints of each should be evaluated at every organization.

Formal education needs to be addressed at every level of education.

- At the Professional level: consider certification training specific to the CRWS domain. This does not exist yet but an organization like ISSP could be approached to inform the development of a CISSP tailored to the needs of the CRWS domain. Professional training should not just cover cybersecurity but also software engineering certifications. This is the best level to introduce different disciplines and domains to the adversarial and subversion characteristics afforded by cyberspace. The military has "cyber" best practices, tactics and techniques that should be evaluated for use in more general education.

- At the University level: general studies should teach engineers how to produce higher quality secure software, introduce software and security architecture fundamentals, cybersecurity awareness and good coding practices in every discipline. Government standards and guidelines are good case studies for classes. At a minimum there should be a core cybersecurity 101 course that is tailored to the discipline of interest, but elsewhere cybersecurity principles should be embedded into existing curricula.

- At the High School level: This would be the best place to introduce cybersecurity hygiene and good early coding practices. Comparative code writing to introduce vulnerable versus secure code examples. Basic security architecture. These classes should also teach teaming and interpersonal skills.

- STEM: There is a need to foster interest in secure cyber-physical systems in middle and high school level. High school challenge programs such as robotics challenges could include security challenges. The government could sponsor challenges and develop "kits" for repeatable learning. Those with interest in coding should begin practicing safe versus vulnerable coding practices at this level.

Experience-building opportunities include:

- Internships – especially working in government cybersecurity labs. However interns need to be in an environment where they will succeed. Internships must be organized, funded, and mentored properly. Effort should be placed on introducing interns to several practices so they may make informed career decisions.

- Field trips to operations centers – to discover the impact of malware on these systems.

- Student competitions – like the Air Force Association's Cyber Patriot youth education program. Robotics competitions are also an opportunity space.

- On-the-job practice – which would be effective for training best practices, gaining hands-on experience, developing soft skills and team skills, and understanding resilience.

- Workshops – with real examples to introduce people to the threat mindset and to connect the threat-mindset with systems thinking, planning, and execution.

- In Formal Education – professional education, on-line courses and certifications, trade schools, and military education. Trade schools are excellent avenues but need to be recognized in government job qualifications. Military training can be more effective than other institutions: partnerships should be explored.

2.7. CURRENT AND FUTURE CURRICULUM

Proper cybersecurity education is absent in today's curriculum. In order to strengthen the future workforce, cybersecurity should have an integrated, system-level perspective throughout curricula. Distinct application and focus areas should be available. Fundamentally understanding the requirements, the exposure, vulnerability and associated risks, and analyses that perpetuate security within cyberspace would reduce vulnerabilities and tighten the coupling amongst the various architectures and systems within the designs. Fortifying cybersecurity education would start early in K-12 and progress through detailed syllabi in universities. Barriers between academia and DoD should be assessed and evaluated to adapt for the appropriate interactions to provide domain and context knowledge with the associated understanding of risks within the system.

Background competencies integrate foundational engineering and computer science knowledge areas with tiered approaches to security. Everyone should understand the consequences of poor security, along with basic secure design principles and methods. Everything has software, and good software coding practices should be a core foundational skill. Security foundations include formal mathematics and logic, formal modeling methods, state machine modeling, and network and operating systems design. These are core application areas in computer science and computer engineering, and need to become more foundational.

2.8. SYSTEMS ENGINEERING THE SOLUTION

Cybersecurity has become a critical pillar in defense related engineered systems, however, a developed holistic approach to integrating the varying aspects of cybersecurity into the engineered design is lacking. This ranges from education and the distinguishing characteristics of the DoD to the interplay amongst the differing layers within the engineered system itself. Several of the involved systems are silo'd, often treated individually, and context fluctuates depending on the original design requirements. Breach of communication and/or knowledge at the various levels creates a cascading effect, making implementation of sound cybersecurity principles reactive instead of proactive and more physical-centric. There is need for a shared vision of the end-state with a cohesive, integrated plan to achieve it, engaging the communities necessary for best benefit.

2.9. DOMAIN AND CONTEXT KNOWLEDGE

The DoD provides unique domain experience, where the purpose, operational context, and mission supported by defense related engineered systems are vastly different than those in the commercial sector. There are evident gaps in processes, competencies, and qualifications for the domain and context knowledge at each level of ecosystem. It is important for academia and DoD to work together to reduce the chasm, and enable learning for the specific domain and context necessary for success. Adjusting the current educational structure requires participation and input from the DoD, with opportunities for hands-on and online learning. The levels of architecture incorporated in each system should be approached through the appropriate viewpoint(s) for cybersecurity to be integrated through systems engineering.

2.10. FACILITIES AND LABORATORIES

Examples of virtual reality cyber-physical ranges and simulation were presented and discussed. Simulations will be very important to address the cyberspace domain, both to support many small cohorts and to protect expensive equipment form damage. Simulations and exercises should span multiple levels from table-top wargames down to the cyber-physical control systems being attacked/defended. The National Science Foundation should consider funding virtual simulation and hardware in the loop labs for this purpose.

Basic hands-on lab experience needs to be introduce, starting with simple systems and security concepts in low-cost IoT "playgrounds." These can be scaled to more complete systems and then to DoD Cyber ranges.

2.11. JOBS, SKILLS, AND KNOWLEDGE UNITS

There are a number of example programs that can be assessed and adopted or tailored to define the appropriate knowledge units (KUs). Look at the NSA/DHS Centers of Academic Excellence for examples of foundational curricula in universities. Also review the NICE Cybersecurity Workforce framework for foundational knowledge, skills, and abilities (KSAs) – the categories would be common but engineering roles need to be added. The Association of Computing Machinery (ACM) has recently updated both their Computer Science and Electrical and Computer Engineering curricula guidance to include cybersecurity competencies. The Navy COOL (Credentialing Opportunities On-Line) provides a framework for certification in the CRWS domain and can help identify transition gaps. Finally, certification programs specific to the CRWS domain need to be developed as the hammer to enforce safe practices.

3.0. FINDINGS AND RECOMMENDATIONS

The breakout sessions and subsequent discussions created a rich data set describing the education and training gaps and solution space for CRWS. The following summarizes findings and recommendations from two perspectives: where should the DoD focus education and training, and where should the SERC focus their research on human capital development.

1. The services are in many ways leading the way in education and training for cyber-physical security. The services should share best practices, programs, and guidance across the community. In particular, these should be shared with educators so some of these become academic case studies.

2. A future CRWS workshop should review service level and defense industry (CITAG) efforts and guidance to look for commonalities across competencies, processes and practices, etc.

3. A discussion with the National Science Foundation should promote the need for Academic Centers of Excellence in CPS security in CRWS related domains.

4. The community lacks a lexicon/taxonomy to adequately describe the cyber-physical system security domain. At one end there is a published taxonomy in the IEEE to describe dependable and secure computing systems – but it needs to be updated to reflect the cyberspace domain. At the other end there is the U.S. military's Joint Terminology for Cyberspace Operations – which needs to be linked to the appropriate engineering and computing domains. There is a need to develop a formal taxonomy and lexicon to link these together, in order to inform the needed competency framework.

5. There is a need to develop a formal competency framework. This can be informed by the NICE framework with the goal to address engineering competencies, specializations, and roles.

6. System Security Engineering (SSE) is an acknowledged competency gap in the CRWS domain. Although the NIST 800-160 SSE special publication is comprehensive, it was not intended to define specific methods, practices, roles, etc. There is a

need to develop shorter application specific interpretation guides and use these to drive education and training outcomes (guidance, 2-pagers, reminder cards, etc.).

7. An investigation of CPS certifications and their value to the CRWS domain needs to be conducted. This might be working with ISSE to develop a tailoring of the CISSP, or might be a separate framework. Initially this should be studied, and recommendations made back to DoD leadership.

8. Pursue a series of STEM activities for secure CPS. Develop a reusable "kit" to inform and mentor STEM challenge activities related to securing robotic systems. Partner with STEM robotics competitions to add capture the flag type challenges. Develop education modules in secure and safe coding practices.

9. Prototype a cyberspace-realistic virtual reality simulation for a relevant CRWS (aircraft, missile, etc.) in an unclassified domain that can be distributed to and used in university education settings. This might be done by use cases related to discipline (aerospace, mechanical, etc.) but must be a multidisciplinary team based experience.

10. Develop (initially) a series of DAU workshops on securing CRWS, working from war-room/tabletop domains down to example forensic studies of real attacks. Partner with industry and academia. Use these to help determine primary course opportunities in the leadership, program management, and acquisition domains (the sample Professional Education course developed by the University of Virginia on SERC Research Task 175 might be a model for this).

11. In the research domain, the process to develop and prune system hazard, fault, and attack trees to determine cybersecurity requirements is immature in application to CRWS, resulting in incorrect assumptions and rework. It would be useful to collect and model the pathology of these decisions to inform both engineering assumptions in practice and inform use cases for education and training.

There are a number of other initiatives in the DoD CRWS community and the NDIA Systems Security Engineering committee that are integrally linked with education initiatives. Follow-on activities should remain cognizant of these initiatives and use them to inform education initiatives.

4.0. ACKNOWLEDGEMENTS

The authors would like to express thanks to the academic participants in this workshop who generously shared their knowledge and experience. It was a unique opportunity to bring the community together. Thank you to MITRE for hosting the event, to the SERC and ASD(R&E) for planning and facilitating, and to all the attendees for the open discussions, ideas, and information exchange.

5.0. WORKSHOP PARTICIPANTS

Nickee Abbott
Ryan Albert
Michael Ambroso
Robert Appleton
Radu Babiceanu
Jason Batchelor
Brandy Barrere
Raheem Bayeh
Jack Bonner
John Bowden
Paul Bresnowitz
Steven Canup
John Chandy
Jesse Crips-Sorger
Tim Denman
Christopher Dopita
Holly Dunlap
Steve Dunn
David Eccles
Mike Eison
Christian Fiore
Andre Florence
Dawn Folck
Paul Fontanez
Crystal Gargani
Rodney Gatch
Judy Gonce
Wayne Hammer
Jeff Hester
Barry Horowitz
Newman Hsiao
Michael Hubbard
Nita Jones-Coleman
Jared Kaib
Kafayat Kelani
Mike Kinney
Julie Konnor
Douglas Krueger
Bob Landry
Bradley Lanford
Matthew Lee
Robert Lozano
Paul Lyons
David Madden
Logan Mailloux
Laura Martin
Paul Martinell
Richard Massey
Jeffery Mayer
Michael McCracken
Elizabeth McDaniel
Thomas McDermott
Michael McEvilley
Michael McLendon
Bryan Misitis
Michele Moss
Kenneth Nidiffer
Scott Niebuhr
Patricia Olkowski
Sharon Parish
Bradly Paul
Jon Paulikonis
David Pearson
Kara Perry
Matthew Picerno
Kristyn Plunkett
Paul Popick
Paul Ragard
Steve Rajotte
Andrew Ramos
Melinda Reed
Raymond Richards
Roy Rogers
Robert Salvia
Ronnie Scott
Elizabeth Scruggs
Robert Smith
Alan Sorensen
Brad Swearingen
Robert Sweeney
Elijah Varga
Dinesh Verma
Eric Weisel
David A. Wheeler
William Young

6.0 WORKSHOP AGENDA

DAY 1 AGENDA	Presenter (s)
MITRE Welcome and Security Orientation	Mr. Michael McEvilley (MITRE)
Workshop Welcome and Introduction	Dr. Dinesh Verma (SERC)
Context and Rationale for the Workshop: **"Preparing the Engineering Workforce for Cybersecurity Challenges"**	Ms. Melinda Reed (DASD/SE)
PANEL 1: What are the Government Engineering Workforce Challenges? • Mr. Steve Rajotte (Cyber Workforce Development, Air Force Cyber Resiliency Office for Weapon Systems) • Mr. Matthew Picerno (Cyber focal, Army ASA(ALT) office of the Chief Systems Engineer) • Mr. Steven Camp (Combat System Security Integration, Naval Surface Warfare Center Dahlgren Division) • Mr. Tim Denman (Cybersecurity Learning Director, Defense Acquisition University)	**Moderator:** Ms. Melinda Reed (DASD/SE)
PANEL 2: What is Academic doing today? • Dr. Barry Horowitz (Munster Professor of Systems and Information Engineering, University of Virginia) • Dr. Raheem Beyah (Interim Steve W. Chaddick School Chair, Electrical and Computer Engineering, Georgia Institute of Technology) • Dr. Radu Babiceanu (Assoc. Professor and Masters Coordinator of Systems Engineering, Embry-Riddle Aeronautical University)	**Moderator:** Mr. Tom McDermott (SERC)
BREAKOUT SESSION 1: **Understand engineering education gaps and current needs related to cybersecurity**	**Facilitators:** McDermott, Horowitz, Babiceanu, Chandy
Discussion, Reflections and Insights	All
DAY 2 AGENDA	**Presenter (s)**
First Breakout Session Outbriefs and Discussion	**Facilitators**
Panel 3: What should Academia do about this? • Dr. John Chandy (Assoc. Professor and Assoc. Department Head, Electrical and Computer Engineering, University of Connecticut) • Mr. Richard Massey (Boeing Corporation, Technical Fellow) • Mr. Tom McDermott (Deputy Director, SERC, Stevens Institute of Technology)	**Moderator:** Dr. John Chandy (UConn)
BREAKOUT SESSION 2: **Anticipate and develop needs for tomorrow's engineering workforce**	**Facilitators:** McDermott, Horowitz, Babiceanu, Chandy
Session 2 Outbriefs, Discussion, Reflections and Insights	All

APPENDIX

- BREAKOUT SESSION COMMENTS ORGANIZED IN MINDMAPS

BREAKOUT SESSION 1: Understand engineering education gaps and current needs related to cybersecurity

1. What are the distinguishing characteristics of defense related engineered systems with respect to security education, skill, and competencies?
   A. Unique Mission and Context
      1- Lethality engineering - because lethality is the end view, much stronger focus on security
      - For the most part, DoD systems are designed to inflict force tremendous amount of casualty or force on our adversaries by intent and design. There is a concern if you change one bit in that computer that will lessen the power.
      - Lethal systems, much more focus on safety & security, learn from safety but adapt to security

      2- Contested environment;
      - Tactical community needs to train SE's on threat issues

      3- Mission impact;
      - Engineers need to know operational context.
      - Engineers need to understand weapon systems
      - Unique domain experience… radar not same as aircraft not same as kinetic systems, "Care abouts" are different
      - Security education for weapon system not as prevalent… e.g. access control
      - End user is unique and specific vs. broad market

      4- Mission Resiliency
      - Don't say denial of service, say "the weapon won't work!" (Operational context)
      - More understanding of complexity and diversity in the design phase (in education)
      - Continuity of Operations (COOP) – challenging for weapon systems

   B. System Deployment
      1- every one of DoD computer related systems or cyber related systems is considered to be on the forward edge of the battle area…have to deploy them overseas in the area of the enemy. Now that we are in the cyber arena, that forward edge is where the adversary can reach right into our computers where ever we are. …That makes us want to think of different ways of doing things.
      2- From a battle front perspective, the enemy wants to get into our systems. That makes us want to think of different ways of doing things.
      3- What distinguishes us is that we can't just rely on physical security …we can't just say that the server is behind some machine room and we don't have to worry about network security… Cybersecurity introduces a whole new set of vulnerabilities.
      4- Tighter relationship between physical security and system security

   C. DoD Lifecycle Characteristics
      1- It can't be a Beta version. That's right, we have to release and use the complete version
      2- DoD lifecycles out of sync with commercial, need to address legacy systems, longer refresh periods
      3- In the Navy, we say we don't patch. Our systems are so complex…all of the baselines have been certified to work together in an integrated manner
      4- The software may be obsolete or unusable by the time it is released. COTS products. We assume that if it's out there on the market that it is good to go but it needs to be checked and tested to ensure that it is doing what it is supposed to be doing
      5- The minute we go into baseline architecture, it has to be redone within a specific timeframe.
      6- Getting the software out of the door first, I think students especially now, when they see Google apps always in Beta, you can see the error.
      7- Lifecycles longer than IT systems… some not connected to networks for periods of time.

8- Refresh periods are longer… costly to update. e.g. ships
9- Hardware lifecycle much longer
10- Cost to upgrade and patching can be significantly higher and problematic for weapon systems… recertify. Ramifications to systems. Regression testing… primary, secondary, etc…
11- IT systems secure through network (not HW)… weapon systems are isolated… interfaced through HW.
12- Integration of old hardware or software to latest engineering process, training
13- Tech, HW components will lag behind commercial

D. Primarily Embedded and Cyber-Physical Computing
1- Lower level – secure logic
• Can we protect SoS interfaces as part of protecting the individual system.
2- Look at functional level
• Functional is easier to understand than technical
3- We have 3 level systems that have binaries.
4- Connectivity is intermittent (for updates) and chain of connections longer, updates & patches problematic
5- Detection is difficult… baselining modes, and system states is very difficult… too many system perturbations to know maybe know what "something is wrong" looks like. Is there a sensor to monitor and bound "normal" system behavior? Just observing - not part of the "system". Find "out-of-norm", e.g. power consumption.
6- Limited time redundancy capabilities
7- Learn from what Safety has done… safety has clout… cyber doesn't
8- IT always on, always connected. Vs intermittent… ramifications to patching.
9- Weapon system - physics of the system can help track intrusion. E.g. temperature…

E. Quantification of risk/cost very different
1- Safety, Reliability and availability can be paramount vs IT systems… dire consequences
2- Supply chain is very important
3- Safety and security were applied similarly for different reasons.
4- Sensitivity of the application, and data differ with criticality and safety
5- Supply chain transparency very important for defense systems vs. commercial

F. DoD Culture and Workforce
1- We don't want to share information…; Between hallways and/or cubicles…we can't / don't share information. I've learned more on Google than from the person sitting next to me.
2- We have our IT standards, they are impossible
• RMF is useful but controls focus on IT, need system specific RMF to requirements decomposition
• Controls were specific to information system, relating and realizing to RMF takes times
• Not just to rely on RMF checklist to get ATO
• Quantify the risk is not available for defense systems, by going through the RMF frame work
3- We have to be very careful when we push requirements to DoD that we are not sending info on things that we cannot do.

G. Security Classification Issues
1- Need to teach students about classification, What is classified, how do you know what is classified… Students understand in general how do you make things classified…next level…
2- To over classifying system security
3- Classification issues limits body of knowledge and knowledge transfer

2. What are the primary experience gaps in workforce processes, competencies, and qualifications today?
A. Sharing intelligence because things can change rapidly.
1- Designers need to be more knowledgeable of vulnerabilities and potential ramifications.

B. Understanding available tools

1- Code scans and how to prioritize them.
2- System Theoretic Process Analysis for Security (correlate with safety)
3- Attack surfaces/trees;
4- Every student to should get trained in static analysis to get a software assurance experience, Concept of testing should be applied by developers at early stages of education
5- Overly-general rule of thumb: If your document about developing secure software/systems doesn't discuss buffer overflow, injection, and cross-site scripting, then it fails to say anything detailed enough to be useful. We need to make sure that our software developers have a *clue* about the common kinds of problems they are trying to prevent!!

C. Security, safety competencies at the enterprise level, need program management understanding of cybersecurity technical aspects
1- Red team conversations with system and program staff… identify vulnerabilities early.
2- How to properly assess where risk reside on matrix, criticality vs likelihood.
3- Process is needed similar to safety process for identify risks and who has authority to make decisions. Operational vs acquisition.
4- Who has "authority" to accept risk… PM lives in world of acquisition accepting acquisition risk and not operational risk.
5- Translating consequences/awareness to program management… address with education of cyber consequences… translate vulnerabilities into mission ramifications.
6- Weapon systems expertise is more silo'd…. need more system level understanding to larger impact expectations.
7- Basic security tenets (i.e. access control) not prevalent in weapon systems

D. Qualifications… programs lack dedicated cyber… with proper clearances
1- Test community not qualified and knowledgeable to fully assess software code acceptance
2- Not sure what we need, do commercial certifications meet our needs?
3- Only hammer is IATT, ATO.
4- IT has large body of education, certification processes, body of knowledge… IT community more mature.

E. Need Systems Security Systems Engineering applied to entire lifecycle.
1- Use cases
2- Need Cyber folks know a little about systems… systems folks know a little about cyber… collaborate
3- Thought processes for both design and breaking into pieces;
4- Operational views;
5- Systems Engineering is not a major topic in the academic community (only 14 universities with PhD programs)
6- Weapon systems expertise is more silo'd…need more system level understanding
7- Requirements (where are common requirements in security)

F. Requires fundamental security principles (e.g., design principles such as those from Saltzer & Schroeder),

G. Don't own supply chain… use of COTS, need understanding of all components

H. Talent pool DoD can recruit from is the least compensated, new folks get certs and leave, turnover
1- The SMART (scholarship preservice) program. Once they've completed their assignment they are gone b/c they can make more money! Unlimited leave in the govt.

I. Computer science became focused on coding practice since late 90s, less on how the computers work
1- Gap in understanding programming languages, hardware, and architecture
2- Schools pushing out graduates with latest technology – what about legacy systems?

J. Older workforce reluctant to learn new processes/use new tools, new workforce experience gap

K. Theoretically, an engineering student should be able to come in after graduation and hit the ground running but they aren't ready.
1- Navy have opportunities to bring in kids from HS 9-12 grade into the Warfare sites. … We have an engineering program with Morgan State University … They come back the next summer and have their clearance We need to let these

students go out break something, trouble shoot, learn in the process.

2- Risk and put people out there. … In the gov't if you con them to come in to the …It is absolutely key to get the kids in early and expose them; you can get lifers.

3- Also 4-6 weeks isn't enough time to get them spun up on a project to be affective.

4- Interns can learn from working in the real world/office, however they do not have clearances to be able to actual do anything.

L. Almost everything is/can be reused. Here's a quick list. They are not explaining how to verify software.

1- origin analysis / software composition analysis (reuse rampant)

2- clearly require whitelisting, discuss assurance cases

3- identify what the common weaknesses are, how to find the common weaknesses, & how to prevent/counter common weaknesses,

4- validating input, error handling, static/dynamic analysis (what they are, when to use them, what their advantages and disadvantages are),

3. How do educators view these challenges and what are the primary ideas to address them?

A. Educators can solve problem, but they are also limited by external factors, such as curriculum, number of credit hours, etc.

B. Building of a simulation for students to get training

C. Not much hacking training available for hardware, Hacking courses should done very often, Train hacking with licensed or with some controls

D. Are issues with education from infrastructure or communications?

E. A way to apply a tiered approach to address gaps… no single solution for education.

F. Engage and streamline research

G. Look at other industries (e.g. automotive) to learn from for building critical skills

H. Curriculum changes based on faculty

I. Universities are developing curriculum IAW proximity to and need of employment source

J. Do educators care enough about the DoD to overcome the challenges of working with the DoD?

K. DAU do more workshops integrating subject matter expertise for organizations

L. CPS working group has good progress – extend it to a framework task areas specific to CPS, NIST 800-160.

M. How to transfer progress to faculty

N. Massachusetts is doing a certification program development funded by state government

O. No one has put forward funding to direct academics to develop more training

P. Add needed materials to current courses.

Q. Teach fundamentals/teach how to learn;

BREAKOUT SESSION 2: Anticipate and develop needs for tomorrow's engineering workforce

1. What are the types of curricula that would support the education needs?

A. Secure systems designed in capstone classes.

B. Attack and defend teams.

C. Modeling of any kind.

D. Analytical skills + problem solving.

E. Functional analysis.

F. Security architect.

G. Concepts of code structure.

H. Software testing.

I. JTAG (way to plug in and get access to the underlining electronics), for example, is appropriate for debugging but can be used nefariously (so introduce that concept in conjunction with the engineering topic).

J. Cyber tabletops…to find into you can't from drawings

K. Identify the attackers

L. Attack surface of a system – need to identify

M. Exposure through I/Fs – how well are your interfaces controlled?

N. Every sys requires updates from time to time

O. e.g. failed tech for security – USB but still use USB

P. Hardware reverse engineering as an attack vector

Q. What makes for a good security analysis of sys of sys – sys level analysis of security

R. Red teams working together when designing the system

S. Important techniques - root causes analysis, fault trees

T. Key Skill – need to be able to assess risk

U. Need more operational viewpoint

V. Distinguish characteristics of system

W. Resilience into measurement of requirements – possible?

X. TPMs for cyber?

Y. Need soft skills and Emotional Intelligence (EI). Very important for the virtual, on-line world. Example, software coding where people are geographically diverse and coding occurs 24x7.

Z. Rather than define the curriculum, it's better to define the learning objectives or knowledge units
1- We have pen testers, but we also need system testers.
2- Add cybersecurity when teaching circuits.

AA. Develop the framework for SE jobs including what they need to know

1- bounding the problem for the systems engineer

BB. Dedicated SSE master's programs vs SSE in an SE master's

CC. Question: Do we need a certification curriculum added to the university curriculum? No but need a list of curriculum objectives that should be harmonized.

1- CSSIP… extend to WSSIP… weapon system SIP… address uniqueness for embedded systems… certificate program to standardize baseline of education…

2- Determine curricula to get certifications (renewable) complemented by curricula to get degrees (single events)

DD. Students are not thinking of attack surfaces, 1 context - environment requires resiliency, 2 no focus on attack surfaces, instill thought processes to now only get something to work but how to break it- operational usages and views, 3 fallacy that we think educators are going to solve the problem; they teach fundamentals; learn how to learn

2. Matching jobs with cybersecurity critical thinking skills

A. What set of KUs?
1- NSA/DHS CAE
2- NICE Workforce KSA
- Also look at NICE Framework for KSAs required for different position descriptions (first look at objectives, then find courses that meet those objectives). Look at both and do delta analysis.

3- ACM CSEC17
- Look at ACM? It is currently reviewed and updated every 5 years (was every 10 years).

4- CISSP is too managerial
- As an aside note, CISSP is more of a managerial certification as it pertains to managerial concepts, not so much concentrated on Cybersecurity.

5- Also look at Navy Cool – competency tool like NICE.
- Competency tools like Navy/AF COOL can help identify transition gaps

6- SSE competency job class… what will define that… to address ad hoc cyber job filling

B. Efforts for apprenticeships in DoD (Change the bureaucracy)

C. Determine Best Practices (task to FFRDCs) – link back to education

D. Agencies need to talk to each other and review these KUs on regular basis

E. Centers for Academic Excellence (CAEs) (NSA and DHS use) have criteria that have basic Knowledge Units (KUs) that meet the required knowledge sets. There are 100 universities that fulfill these CAE requirements with their curriculum.

F. Needs to be reviewed and updated regularly. Example, need to make sure known common vulnerabilities (e.g., buffer overflows, error handling, etc.) are covered and add if missing.

G. Creating a role and just changing a job description… need to mature the role for proper qualification for "certification"

H. Easy stuff outside of DoD – operators do not understand cyber

I. Teaching how to design and develop? Actual management of the system? Role of operators maintaining security. Diff between training operators vs skills to develop

J. Defense – policy, impact, weapon system environment

3. Academia need to learn the need and worth of Cybersecurity as well.

A. Cybersecurity awareness is appropriate for everyone; however Cybersecurity should be sprinkled in to foundational courses rather than making Cybersecurity a separate class.

B. Topics introduced at different levels depending on knowledge.

C. Use cases are difficult because of fear of giving away proprietary information that wouldn't be acceptable – challenge is everyone has to agree on making the use case available.

D. Context is also important – knowing what is fine in an engineering sense but not fine when in the hands of a hacker.

E. Dedicated cybersecurity curricula is not so important. Better to sprinkle in cybersecurity.

F. Must cover learning objectives with cybersecurity as an added benefit.

G. Easier to understand when cybersecurity is taught in context of the curricula for the classes.

H. Undergraduate level – sprinkle in with foundational courses.

I. Graduate level - that's when it would be more appropriate to introduce classes dedicated to cybersecurity (also easier to get faculty to agree to teach due to scheduling and expertise challenges).

J. Build in cyber into curriculum, Build a foundation

4. How and where will people learn?

A. Internships

1- Expose interns to 5-6 processes during their internships to let them make informed decision on what they want to pursue.

2- Internships – needs to be structured properly and excite students

3- Internships. Internships are good but there are a lot of constraints. Needs to be organized properly. Needs to be funded. Time is a big constraint because internships are typically only 6-8 weeks. Also, need a dedicated mentor to lead the intern to be successful (need a culture of mentorships within the company). Expectations need to be well understood upfront and need to be managed. Interns need to be put in an environment where they'll succeed.

4- Interns working gov't cyber labs

B. Practice

1- Design – Attack – Re-design process exercises

2- Teaching Best Practices – How much cyber is enough?
3- Now what (critical thinking)?
4- Introduce resilience to exercises
5- Project-based exercises and training
6- Soft skills and team building is important
7- On-the-job training
8- Hands on, practical application, doing stuff!
9- Develop and train on the job combined with mentoring. There are many that enjoy the flexibility of online training.

C. Formal Education
1- Professional education at colleges and secondary school systems
2- On-line courses and certification programs
• Online approaches allow scalability but doesn't work for all classes or all people
3- Military training can be more effective than university education
• One person's experience is that AF Military education training for cybersecurity is better than university training. Need to look at that model.
• Lessons learned in DoD – transfer into education
4- Trade Schools – Are excellent avenues for Cybersecurity trained and educated, however, the government (and others) are looking to check specific educational boxes and tech schools are not on the approved list. If some trade school grads apply, they will eventually leave.
5- Difference between on-line, in-person, and hybrid learning models. People learn differently, so may need to offer multiple approaches.

D. Consider non-conventional approaches. Outreach with High School students (meets, hacking competitions, robotics).

E. Field trips to operation centers – let them discover malware.
1- Gives exposure to see how things tie together.
2- Increase the pipeline of cybersecurity folks – important is also the culture (human factors).

F. Student competitions.
1- Examples, Cyber Patriot, CCDC, and other CTF type competitions

G. Workshops

H. Challenges
1- May have security classification requirements imposed on training some systems
• Sandia and Honeywell labs adjust clearance levels
• What does it take to educate cleared individuals and at what education level
• Universities educating at the classified level?
2- Cost challenges to implement training sophistication
3- Government challenges in retaining/hiring cyber experts – need to be more flexible

I. We need to encourage innovation and opportunities – sometimes we deny opportunities to people due to their MOS or other job classification. We can't solve complex problems if we don't expose people to different environments and expect them to grow. Can't pigeon hole people. People need to grow in their natural capabilities and passions. Example – designers need to see their products in operation. Need to excite people!

5. What types of facilities and laboratories are necessary to meet the education challenges?

A. Research facility to learn processes that students re going to work on.
1- Laboratory to include systems engineering and pen testing.
2- Specific equipment, virtualization, modeling, coding.
3- Lab for IoT "playground"

B. Simulation

1- Visualization, simulation, exercises, cyber table-tops
2- Modeling and simulation labs might be a resource to leverage
3- Simulations (physical part, very important). Working within a small cohort for hands on training, works well for many versus online or remote training.

C. VR
1- National Science Foundation (NSF) virtual labs.

D. DoD CyberRange
2- DoD cyber range – difficult to get test time. Should be a relationship between cyber ranges and University. Having a security clearance is likely a problem.

6. In education –are many of the key topics covered?

A. Need engineering background in the requirements for positions
B. Security education -how does it differ? What do we need to comply with? Why doing security for a DoD system different? Need to understand policy to provide that a system is really secure
C. From education standpoint – workforce is more than just embedded systems – there is IT
D. "Cyber Physical" has larger/broader recognition
E. Who designs systems should have a background in appropriate skills and technology
F. Talking about sys engineers, or cyber engineers? Disjoint groups / disciplines?
G. How do we add to curriculum based on skills that are needed?
H. We are missing systems engineers who have cyber security knowledge
I. Common arch easier to make an engineer cyber or vice versa?
J. Need to change thought process to include security
K. What about failure to meet performance requirements?
L. Tech manager process - where is described re: management
M. Not just form security perspective - also need to form sys integration perspective
N. the experience learned before working and after day is on the job – what is the difference?
O. Tiered approach – understand the role of different SW practices
P. Teach skills and then learn when to apply
Q. Experience ? Processes, competencies, and qualifications?
R. Analogy to safety issues?
S. How to build up a workforce to build the systems
T. Cyber needs to be more integrated
U. sharing of intelligence about adversaries is important and should be more common

7. Professional: Consider CERT training in this domain, approach ISSE about a tailored CISSP

A. Incumbent workforce need training on topics to defend their domains
B. Certified programmer similar to Professional Engineer (PE)
C. Next level is more focused on discipline (e.g., fault injections on power grid for an engineer).
D. Enable government to assess proper secure coding
E. SCRM building up standard for trusted systems IAW DoDI 5200
F. Through training… vulnerabilities testing, Training materials need to be generalizable
G. Influencing requirements before test… AF cyber campaign plan… engagement with operations community… repurpose them for cyber focus. Use of maintenance and test systems. Acquisition language guidebook for cyber specific contract language. Derived requirements further down the lifecycle for driving design decision… how to mitigate shortfalls, how to

reduce observable risk… how to present from a mission perspective.

H. Navy making cyber considered as another risk within a program through application of standards… apply through each competency.

I. TTPs have a wealth of information, AF cyber hygiene best practices… top 5 best practices, if nothing else

8. University level

A. University: teach engineers how not to allow poor quality code, introduce software and security architecture fundamentals, cyber awareness and good coding practices in every discipline, standards and government guidelines are case studies for classes

B. Teach core competencies in bachelor's degree

C. teach engineers how not to allow poor quality code

D. many university programs that don't teach software architecting, matching master's program with undergrad for architecting… or better to get experience first. Smarthome architecture standard into a college course could be a starting place… which includes security

E. Should be at a minimum a cybersecurity 101, Tailor cyber 101 training to application of interest… supply chain, systems engineering, program management, logistics, etc, typical ISyE curriculum doesn't include cyber

F. If student using IT systems on campus… requires cyber awareness training. Comparative to manufacturers plant and safety… everyone is trained is made aware

G. Change existing courses (with case studies) vs all new dedicated course

H. Cross pollinate… know cyber but may not know how to integrate

I. At college level, include team activities

J. Reverse engineering would be at the graduate level.

9. High School level

A. This would be a good place to introduce good cyber hygiene for early coding skills

B. Introduce skills for more than just code that works… susceptible to hack awareness… how to write it secure.

C. Is there an accredited group to develop and introduce programs into high school curriculum?

D. Limited volume of resources to apply for cyber hygiene.

E. Ethical hacking and secure code writing to defend

F. Do comparative code writing… this is vulnerable… this is not.

G. Good design includes architecting… cross domain solutions… flaws came first in architecture.

H. At pre-college level, teach teaming skills

10. STEM support

A. STEM: Introduce security challenge into robotics challenge programs

B. Foster interest in concepts in middle and high schools (part of STEM advocacy)

C. Discussed high school robotics challenges, could they include a security challenge?

D. 20-30 Minute in high school course to start thinking about hacking

E. Security hygiene… get H.S. staff to become knowledgeable

F. Just writing software that works… learn "hackable" aspects of their code… learn both sides… work and survive… make it part of the "competition"

G. Safety should be interrelated

H. Will DoD influence STEM programs for additional funding to fund "great ideas"

I. Need to build up a kit (of stuff) that is repeatable

J. International robotics competition… talk to directors to see if they are interested in bringing in a cyber aspect to the competition. Involve industry

K. Is it conceivable to add information assurance, cybersecurity, etc… into DoD STEM incentives?

11. What background competencies are needed to prepare students for that education?

A. Introduce security as tiered approach: user, trusted, trusted crypto…

B. Other drivers could be the attack surfaces and the functionality to be met.

C. EE, CE, SE, CS degree or programs.

D. Mathematics & Logic.

E. Understand the consequence of poor security

F. Everything has code.

G. Formal modeling (methods) built into curriculum.

H. State machine modeling.

I. I.e., in course on operating systems in computer science, bring up and incorporate cybersecurity

J. Partly driven by what counts as accredited to hiring managers

K. Computer engineer on flight platform – design principles (e.g., least privilege) but depends on discipline (software is different than testing).

12. In the context of engineered systems, at what levels should security education be addressed?

A. Need to raise awareness early in life.

B. Start with something early and then build upon it.

C. There are different types of users, there are designers, and there are also system architects.

D. In the context of systems engineering, what is the difference between systems engineers and security engineers?

E. Every system has security requirements – task is to identify them and flow them down.

F. For security, government is usually the driver.

G. Things that can go wrong in the context of the mission

H. Make cyber component introductions in other technical classes (including electives)

I. Not just curricula, but support activities

J. Not just with degrees, but proven demonstration of skills

K. Topics introduced at different levels as the background competencies are introduced

L. All levels but how deep depends on your level of education and discipline (awareness to expert).

M. Everyone should get cyber awareness training (contracting, finance, engineering, etc.).

University or Research Organization

1. Stevens Institute of Technology
2. University of Southern California
3. Air Force Institute of Technology
4. Auburn University
5. Carnegie Mellon University
6. Georgetown University
7. Georgia Institute of Technology
8. Massachusetts Institute of Technology
9. Missouri University of Science and Technology
10. Naval Postgraduate School
11. North Carolina Agricultural & Technical State University
12. Pennsylvania State University
13. Purdue University
14. Southern Methodist University
15. Texas A&M University
16. Texas Tech University
17. University of Alabama in Huntsville
18. University of California - San Diego
19. University of Maryland
20. University of Massachusetts Amherst
21. University of Virginia
22. Wayne State University