National Defense Industrial Association (NDIA) System Security Engineering (SSE) Committee

Holly Dunlap
Holly.Dunlap@Raytheon.com
SSE Committee Chair

December 2017

NDIA SSE Committee Accomplishments

- **NDIA Cyber Resilient & Secure Systems Summit, April 18 – 20th**
- **NDIA SSE & SwA Co-Sponsored with the Joint Federated Assurance Center (JFAC) a (2) Day Government SwA Gap Analysis Workshop. June 22nd & 23rd.**
- **USAF System Security Engineering Acquisition Language Guidebook**
- **NDIA SE Conference 2017 include 25+ SSE track breakout sessions**
- **Guest Speakers**
  - **AF SES Cyber Technical Director**
    - Mr. Daniel Holtzman, Cyber Resiliency Office for Weapon Systems (CROWS) AFLCMC/
  - **OSD SE PPP Deputy Director, Ms. Melinda Reed**
    - Mr. Michael McEvilley, Mitre on behalf of Melinda Reed
  - **AF Aircraft Cyber Threat Working Group (ACTWG)**
    - Col Masterson, Deputy Associate Director of Engineering & Technical Management Deputy Director, Cyber Resiliency Office for Weapon Systems (CROWS)
  - **University of Virginia, Systems Engineering Research Center (SERC)**
    - Mr. Peter Beling

Challenges from Government to Industry

- **Government wants examples from Industry:**
  - Issues to learn from
  - Techniques that work
- **Need help from Industry:**
  - How to improve security with technology that doesn't require redesign
  - How to improve security quickly and efficiently
  - Increase customer confidence in the resiliency & security of the systems we deliver
- **Together we need to address:**
  - What does cyber resiliency look like?
  - How do we measure cyber resiliency?
  - How do we execute and implement cyber resiliency?

Additional key findings:

- Trying to do risk management in an policy/process environment. Need to develop use cases and test cyber system security risk management methods.
- Knowledge of how the system is designed is knowledge of where the risk is, Government does not always have that detail. Government does not fundamentally know how these systems work nor how they are being used. Need help from industry to better understand the system design & capabilities.
- We need to stop taking a reactive approach to our solution. Move away from threat based, b/c it's considered reactive. How do you get the "good" guys to look forward.

Specific Actionable Opportunities

- **DoD Risk, Issue, and Opportunity Management Guide**
  - Cybersecurity, Opportunity to shape.
- **Safety Community**
  - JOINT SERVICES-SOFTWARE SAFETY AUTHORITIES
  - Investigate Cyber Considerations - Joint Weapons Software System Safety Process
- **Acquisition / RFP & SOW – Due July 15th (Competed Summer 2017)**
  - Proposed Section L & M, Review & Comment.
  - AF SSE Guidebook, Review and Comment
- **Systems Engineering Research Center (SERC)**
  - University of Virginia
  - Resilience research efforts, analytically-based decision-support tools
  - Seeking industry partnership to test methods and tools
  - Peter A. Beling
    Associate Professor and Interim Chair
    Department of Systems and Information Engineering
    University of Virginia
    434-982-2066
    beling@virginia.edu

NDIA Government SwA Gap Analysis Workshop

Generate feedback from industry on the recent DoD and Defense Science Board Task Force reports on SwA capability gaps within the DoD.

Collect industry's SwA challenges and capability gaps as you develop, sustain, and support our Nation's warfighting capabilities.

Provide JFAC with industry input to prioritize existing and future funding to address the Department's capability gaps.

Workshop pre-work

- **DSB Task Force report on Cyber Supply Chain**
- **JFAC SwA TWG Capability Gap Analysis**
- **Voice of Customer (VOC) Gap Analysis Worksheet & Instructions**

USAF SSE Acquisition Language Guidebook Section L&M

- **Section L**
  - Present the system security view of the platform architecture which enables system resiliency in a cyber contested environment
  - Present the critical mission thread analysis methodology which identifies the system mission critical functions and system mission critical components (hardware, software, and firmware) directly effecting KPPs.
  - Present the system security risk assessment methodology
  - Present the system security risk mitigation and countermeasure approach
  - Present the verification and validation approach to prove effectiveness of system security and system survivability in a cyber contested environment
  - Present how system security has been integrated into lifecycle considerations
- **Section M** ***(one-to-one mapping to section L)***
  - The proposal demonstrates that the system security view of the platform architecture provides sufficient details of the approach to support (future) assessments of cyber resiliency, system security, and system survivability to meet the KPPs while operating in a cyber contested environment
  - The proposal demonstrates that the critical mission thread analysis methodology directly contributes to the identification of system mission critical functions and system mission critical components (hardware, software and firmware) identification
  - The proposal demonstrates that the system security risk assessment methodology directly contributes to the system security risk mitigation approach
  - The proposal demonstrates the system security risk mitigation approach supports the decision making process to reduce the system security risks impacting KPPs
  - The proposal demonstrates that the verification and validation approach will provide assurance that the system security requirements have been meet
  - The proposal demonstrates that system security lifecycle considerations have been included in the overall system lifecycle plan

NDIA SSE Committee Plans for 2018

- **Government Working Groups**
  - Technical Performance Measures
    - Incorporate SSE into current TPMs
  - Risk
    - Draft appendix to DoD ROIM Guide for assessing Cybersecurity Risk
  - System Security Technical Review (SETR) Criteria
    - Clarify system level vs. component level criteria
  - Cyber Resilient Software
    - How to design in resiliency; standards and/or best practices
  - Safety
    - Learn from mature safety processes and incorporate cybersecurity risk to safety

- **NDIA SSE Committee Projects Being Considered**
  - Explore approaches for transitioning from Categorizing the System (Step 1) to Selecting Controls (Step 2) of RMF
    - Identified as gap during SE Conference
  - Provide Recommendations for Cybersecurity Risk Guidance
  - Data Item Description Review (not included in previous acquisition language guide)
  - Provide input on DoDI 8140.01, Information Assurance Workforce Improvement development (replacement of DoDI 8570.01)
  - Explore integrating cybersecurity evaluations into the safety community established processes.

Enhance collaboration and information sharing between Industry and Government

Backup

NDIA Cyber Summit Event Purpose

NDIA Systems Engineering Division held a "Top SE Issues Workshop", August 2016

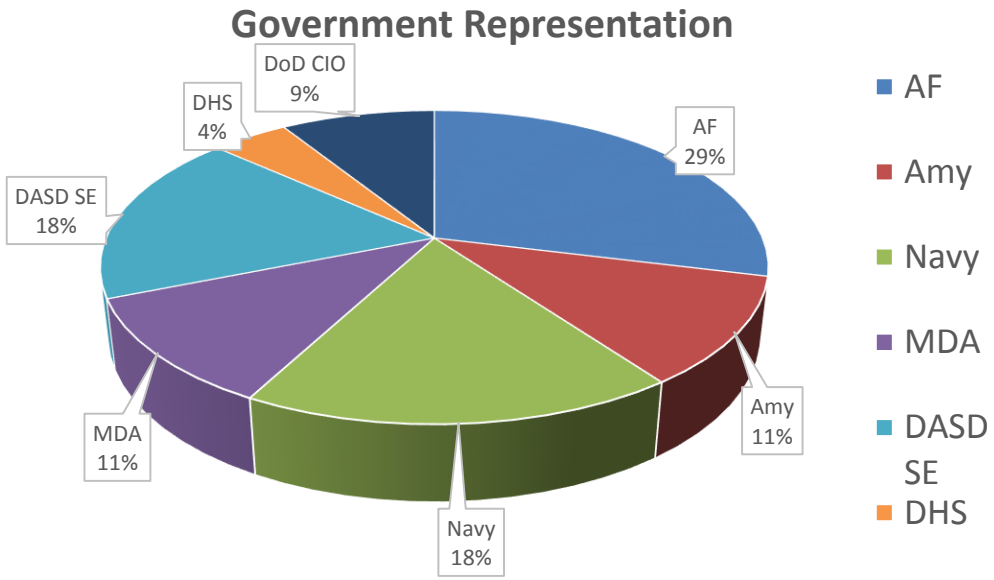
Cyber Resilient & Secure Weapon Systems was identified as a Top SE Issue

System survivability in a cyber contested operational mission environment is critical. We need to elevate the system security risk to the program risk register to ensure a security focus. We need well defined methods, processes, standards, metrics and measures, along with skilled professionals to integrate system security into our product development lifecycle.

***NDIA – National Defense Industrial Association**

Who Attended

- **175 Attendees**
  - 33% Government
  - 67% Industry



Industry Representation

Raytheon	DBS
NGC	Electronic Warefare associates
MITRE	Ensility
BAE Systems	GTRI
Boeing	INL
Booz Allen	Innovative Defense Technologies
Draper	Riverside Research
BAH	SAIC
Lockheed	SEI
Star lab	SRI International
Aerospace Corporation	STR
General Dynamics	Synexxus
Rolls Royce	Tri Guard Risk Solutions
Textron	
US falcon	
Vencore	
ACET	
ARAR Technology	
BDA/DE	

What We Talked About

Word Cloud

"Cyber Resiliency" in all 27 Topics

27:
Cyber Resiliency

10:
Risk Based Analysis
Mission Thread Analysis
Architecture
Carbon Based Units
Taxonomy

8:
RFP Language
Legacy Systems
Techniques that Work
Culture

7:
Test and Evaluation
Compliance Checklist

6:
SE Responsibility

5:
SSE Role
Domain Expertise
Risk Management Framework
Bake-in
Measurement
Supply Chain
Sustainment

Key Take Away from Services & OSD

- **Affects everyone, responsibility of everyone**
- **SE responsibility to design and deliver systems that are resilient to cyber threat.** Transitioning from Network IT responsibility due to cyber association to SE responsibility to integrate security focus / risk management into the systems we design and deliver.
- **Over 70% of systems in sustainment, how is sustainment addressed**
- **Industry needs to stop promoting magic beans**
- **Acquisition guidance needs to transition to contracts**

- **Biggest challenge is the Carbon Based Units (People)**
- **Risk Management Framework Results**
  - Need to:
    - Improve risk focus instead of compliance & checklist focus
    - Domain expertise is imperative
    - Converge to eliminate duplication and conflicts
    - Test early & often.
  - Not identifying risks correctly, security is coming from IT backgrounds when the security is being applied to mission systems

Key Take Aways

- **Focus on mission assurance & not compliance.**
- **Must understand how systems function and the CONOPS**
- **Security must be integrated within Systems Engineering & throughout the system lifecycle**
- **Trace controls (“counter-measure”) to specific real-world attack**
- **Cybersecurity testing needs a more structured & integrated approach**
  - Not based on test till the money runs out.
  - How do we produce evidence that provides increased confidence in the system?
- **Need government support to include system security as part of proposals (Section L & M)**

Key Take Aways

- **Need to collaborate to work smarter.**
  - Both Government & Industry want to work together.
- **Everyone is learning. Need to provide customers with risk, cost, performance based trade options.**
- **Mission thread analysis – move from information assurance to mission assurance**
  - Deliver mission assurance through resiliency
  - Assume the attacker is already in the systems.
- **How do we create design standards as enablers and not restrainers?**
- **Post cyber event often results in refining and defining roles & responsibilities and (re)organizational structure. Communication and process are a common theme.**
- **Convergence (integration) before divergence.**
  - Policy, standards, guidance

NDIA Government SwA Gap Analysis Workshop

Sponsors: NDIA SSE & SwA Committee & OSD Joint Federated Assurance Center (JFAC)

Background:

In July 2016, the JFAC SwA Technical Working Group identified 63 DoD capability gaps that prevent the effective planning and execution of software assurance within the DoD acquisition process. The gaps were organized into seven categories:

(1) life cycle planning and execution; (2) SwA technology; (3) policy, guidance, and processes; (4) resources; (5) contracting and legal; (6) metrics; and (7) federated coordination

As chair of the JFAC Steering Committee, Ms. Kristen Baldwin, Acting Deputy Assistant Secretary of Defense for Systems Engineer (DASD(SE)), recently approved the analysis and directed the Technical Working Group to develop a strategy to address the identified gaps.

In February 2017, a Defense Science Board Task Force issued a report on cyber supply chain with two (out of a total of 25) overarching recommendations to USD(AT&L):

(1) Strengthen lifecycle protection policies, enterprise implementation support, and R&D programs to ensure that systems are designed, fielded, and sustained in a way that reduces the likelihood and consequence of cyber supply chain attacks.

(2) Direct development of sustainment Program Protection Plans for critical fielded weapons systems. Military Service Chiefs should designate fielded weapons systems for development of initial sustainment PPPs to demonstrate their effectiveness.