NDIA Systems Engineering Conference

NDIA System Security Engineering Committee

October 2017

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

Welcome

- **Purpose of NDIA & SSE Committee**
- **Introductions**
- **SSE Track Agenda Review**
- **System Security Engineering Committee 2017 Accomplishments**

SE Division Mission

- ***To promote the widespread use of systems engineering (SE) in the Department of Defense (DoD) acquisition process in order to achieve affordable and supportable weapon systems that meet the needs of the military users. To provide a forum for the open exchange of ideas and concepts between government, industry and academia. To develop a new understanding of a streamlined SE process.***
- ***The SE Division seeks to effect good technical and business practices within the aerospace and defense industry. It focuses on improving delivered system performance, including supportability, sustainability, and affordability. The division emphasizes excellence in systems engineering throughout the program life cycle and across all engineering disciplines and support functions.***

Introductions & Around the Room

NDIA SSE Track Review

NDIA SSE Committee Accomplishments

- **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.
  - Acquisition Language

NDIA Cyber Resilient & Secure Weapon System Summit 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.

Top SE Issue:
Cyber Resilient & Secure Weapon Systems

- **Due to the evolving and persistent cyber system security threat that impacts our interconnected systems, focused attention is required. The following main points also include tenants of engineered resilient systems and mission assurance:**
  - **System Security risks** must be added to the **program risk register** to ensure that security doesn't get traded away to system technical capabilities and cost reduction efforts.
  - Well defined **metrics** and **measures** are needed to conduct trades: cost, risk, and performance.
  - **CONOPS** and **SoS** along with **System critical mission threads** are essential to initiate and focus the system mission functional criticality analysis.
  - **Integration of the security specialties** into the **system security architecture view** needs to be defined and methods developed.
  - NIST SP 800-160 establishes a foundation for System Security Engineering best practices. We need to develop **education and awareness training** to include a range of proficiencies for different **security specialties** with experience in mission system platforms and embedded systems, along with a **range of acquisition professionals.**

Top SE Issue Report Recommendation

- **NDIA System Security Engineering Committee with support from the NDIA Systems Engineering Division to convene a joint government/industry activity such as a workshop or summit, to dialog the relevant issues.**

- **A Summit** is recommended to bring Government, Industry, and FFRDC working groups together to share **developments, strengths, gaps, opportunities, and recommendations**. The NDIA System Security Engineering Committee hosted a 3 day NDIA Program Protection Summit in May 2014 and is preparing for a Spring 2017 follow-up.
- The new System Survivability KPP values are intended to define objective values for a capability solution and derived from operational requirements of the system**. Connecting the SS KPP, Cyber Resiliency metrics**, and **System Security Specialty Risk Mitigations** offers a compelling means to conduct risk, performance, cost trades and compare one solution to another.
- **Verification** and **validation criteria** need to be identified and methodologies established to achieve same.
- **Cyber Resilient** and **Secure System** requirements **SOW & RFP** along with **Sections L&M** evaluation criteria guidance needs to be matured with metrics and measures to ensure a holistic approach for managing system security risks.

NDIA SSE Committee Meeting Agenda
June 28, 2017 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) AFLCMC/
- **University of Virginia, Systems Engineering Research Center (SERC)**
  - Mr. Peter Beling

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.

NDIA Government SwA Gap Analysis Workshop Objectives:

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

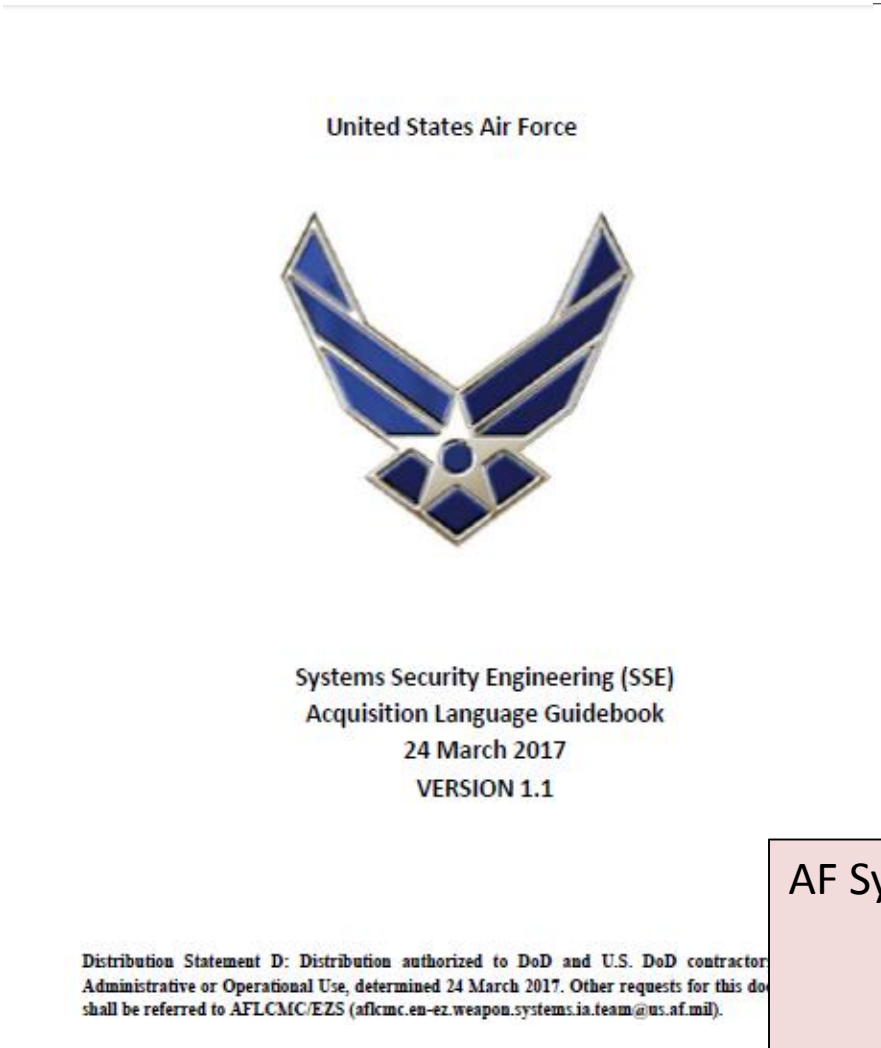
Collect industry's SwA challenges and capability gaps as you develop, sustain, and support our Nation's warfighting capabilities.

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**

AF SSE Acquisition Language Guidebook Review & Comment



United States Air Force

Systems Security Engineering (SSE)
Acquisition Language Guidebook
24 March 2017
VERSION 1.1

Distribution Statement D: Distribution authorized to DoD and U.S. DoD contractor
Administrative or Operational Use, determined 24 March 2017. Other requests for this do
shall be referred to AFLCMC/EZS (aflcmc.en-ez.weapon.systems.ia.team@us.af.mil).

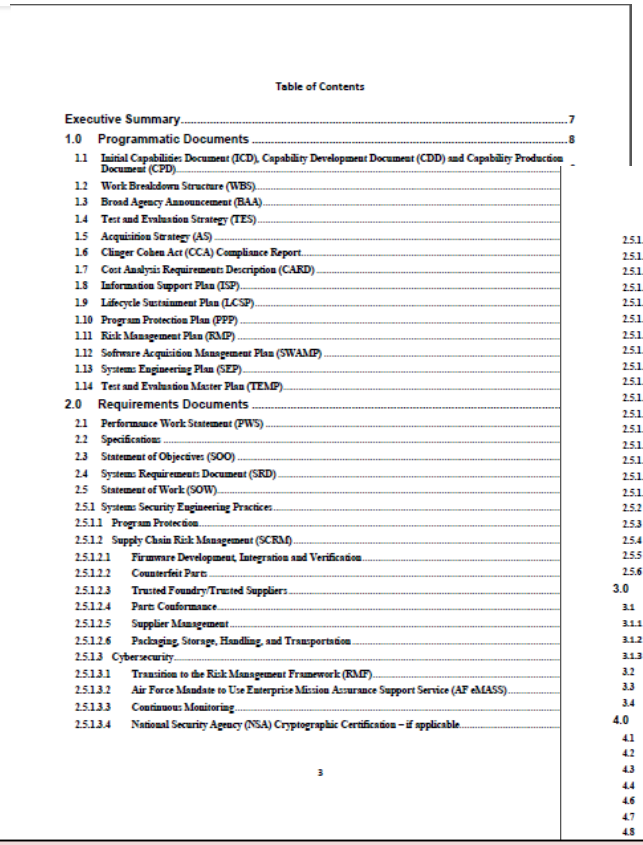


Table of Contents

AF System Security Engineering Acquisition Language Guidebook

Please submit comments by July 15, 2017 to: Cory.L.Ocker@Raytheon.com and copy Holly.Dunlap@Raytheon.com using the Comment Resolution Matrix.

You are also welcome to send your comments to the AF directly.

AFLCMC/EN-EZ System Security Engineering Team (aflcmc.en-ez.weapon.systems.ia.team@us.af.mil).