NDIA 22nd Annual Systems and Mission Engineering Conference

NDIA System Security Engineering Committee

October 2019

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

Cory Ocker
Raytheon
NDIA SSE Committee Co-Chair
Cory.Ocker@Raytheon.com

Agenda

- **NDIA SSE Committee Mission, Goals, Objectives**
- **2019 Year to Date Summary**
  - Projects & Initiatives
  - Information Exchange
  - Industry SSE Representative
- **Projects & Initiatives**
  - USAF Weapon System Program Protection and System Security Engineering Process Guidebook
  - NDIA Critical Program Information (CPI) Assessment and Identification Guide (CAIG)
  - DoD DRAFT Software Acquisition Pathway Policy Guidance
  - Cyber Secure & Resilient Approaches for Feature Based Variation Management
  - IEEE, NDIA, INCOSE System Security Symposium April 2020

System Security Engineering Committee Mission

Mission

To promote System Security Engineering integration into the Systems Engineering and Mission Assurance processes in the Department of Defense (DoD) acquisition of weapon systems. To foster the development of System Security Engineering methods, tools, techniques, and processes required for the role of System Security Engineers. To provide a forum for the open exchange of ideas and concepts between government, industry, FFRDC and academia. To develop a new understanding of System Security Engineering and the critical role it plays to ensure system survivability in a cyber contested environment.

** Federally Funded Research & Development (FFRDC)*

System Security Engineering Committee Mission

Goals

The System Security Engineering (SSE) Committee seeks to:

- ***Advance SSE technical and business practices within the aerospace and defense industry.***
- ***Focuses on improving delivered system security performance including survivability, resiliency, and affordability.***
- ***Promote and emphasize excellence in systems security engineering throughout the program life cycle and across engineering and non-engineering disciplines required for a holistic approach to system security and program protection.***

System Security Engineering Committee

Objectives

- ***Lead projects in areas that challenge the role and responsibility unique to System Security Engineering.***
  - *Projects may include but are not limited to providing a system security engineering industry perspective on draft or current System Security Engineering relevant government policies, government instructions, industry standards, industry best practices, customer requirements, risk management, etc.*
- ***Support security specialty projects and initiatives by providing a system security engineering perspective that directly effects and interfaces with system security engineering.***
- ***Encourage and promote the advancement, education, and skill development of the role of system security engineering.***

System Security Engineering Committee

How do we operate?

NDIA Systems Engineering Division (SED) Planning meeting in December.
Attended by OSD & Services Executive Leaders & NDIA SED Committee Chairs
OSD & Services communicate their plans and priority needs for the next year.

Committee Chairs work with their committee to draft a list of priority challenges & candidate projects.

1st meeting of the year, present both the Government SSE challenges and Industry SSE challenges.

The Committee then reviews and proposes projects to address the challenges / needs.

This process establishes the plan for the year. However as opportunities and needs are presented throughout the year, the committee has the opportunity to consider updating the plan.

The SSE Committee typically meets the afternoon of the NDIA Systems Engineering Divisional meetings which are posted on the NDIA Systems Engineering website. We also send out an e-mail to NDIA SSE Committee members so please let us know if you'd like to be added to the committee email list.

We welcome and encourage participation at all skill levels.

Welcome and highly encourage committee members to lead projects and foster collaboration with other security specialty committees and working groups.

***** The number of projects, workshops, collaborations etc. along with the depth, quality, and level of rigor is dependent on the committee members commitment.**

2019 NDIA SSE Committee Overview

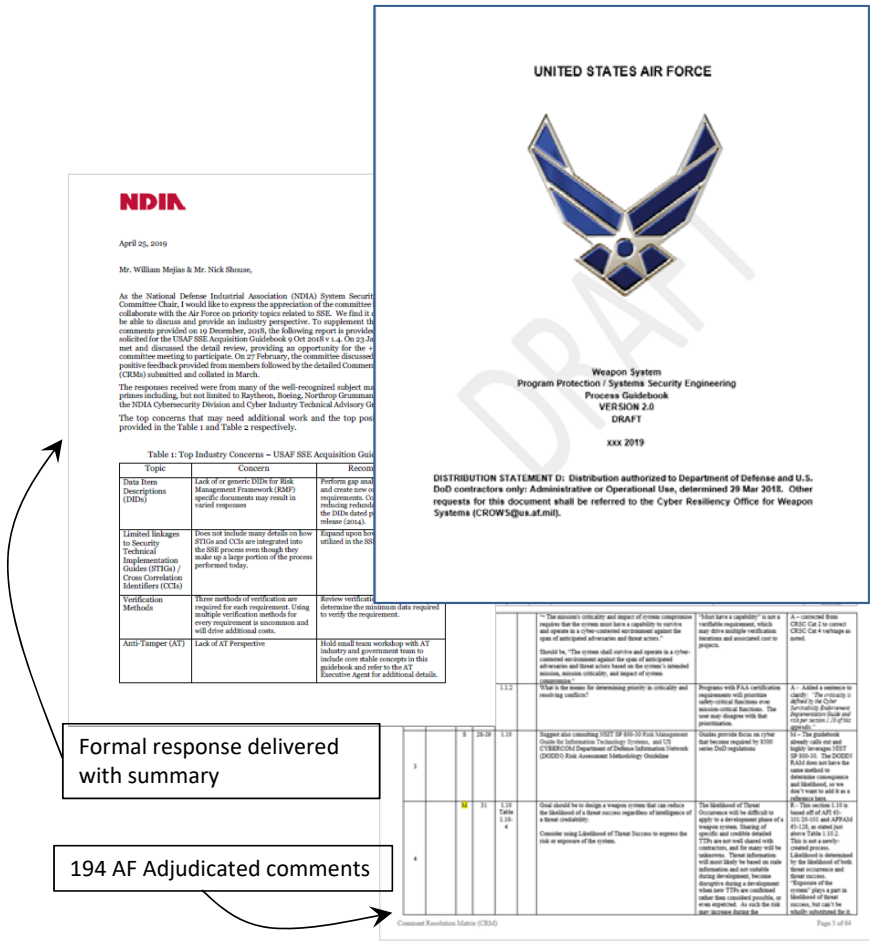
Activity	Title
Projects & Initiatives	• USAF Weapon System Program Protection and System Security Engineering Process Guidebook • NDIA Critical Program Information (CPI) Assessment and Identification Guide (CAIG) • DoD DRAFT Software Acquisition Pathway Policy Guidance • Cyber Secure & Resilient Approaches for Feature Based Variation Management • IEEE, NDIA, INCOSE System Security Symposium April 2020 • NDIA Systems & Mission Engineering Annual October Conference • NIST SP 800-160 Developing a Cyber Resilient Systems Vol 2 *A Systems Security Engineering Approach*
Information Exchange	• DASD(R&E) Sponsored SEI SwA Products, PM & Designer Guide • DoD Cyber Workforce Management • SAE G32 Cyber Physical Systems • ASD(R&E) Cybersecurity Challenges – Protecting DoD Unclassified Information • NAVAIR CyberSafe • AF CROWS Program Protection and System Security Engineering Tools • ASD(R&E) CRWS Workshop Series
Committee Chair Rep.	• SecNav Cybersecurity Advisory Panel Meeting • Collaboration on Quality in the Space & Defense Industries Forum, March 2019

AF System Security Acquisition Guidebook

- Provided approximately 2 formal reviews per year since 2015.
  - Highly valuable and successful Industry & Government collaboration.
  - Directly saw the changes and edits incorporated from the feedback provided.
  - Matured process for distribution, collection, and reporting.
- Lessons Learned
  - Distribution of anything other than public release is painful. (We continue to learn this lesson year after year…)
  - Collection and attribution
    - Use AMRDEC SAFE
    - One response per company.
    - Companies and individuals preferred to limit attribution.
    - Provided a report summary.
    - Acknowledged contributing companies and organizations.
    - Provided reports to contributors per request.
- Guidebook language is being reflected in SOWs! Not just AF but Navy as well.
- Current Version:

  Weapon System Program Protection / Systems Security Engineering Process Guidebook Version 2.0
- **Thank you!**

  Mr. Daniel Holtzman
  Mr. Nick Shouse
  Dr. Ken Barker
  Mr. William Mejias



CAIG

Critical Program Information Assessment & Identification Guide

Background

- **Industry experience: CPI ID often not accurate, consistent, nor repeatable:**
  - Well-meaning teams can come to different conclusions
  - Teams motivated to find no CPI can identify much less CPI than sincere teams
- **Government experience: CPI ID often not horizontal within/across companies & DoD**
  - Service & MDA CPI tools largely based on OSD CPI Decision Aid, 2009
    - Services uses different questions; can lead to different results
    - Updated definition of CPI in DODD 5200.39, May 2015There was disagreement with many points during the coordination process
- **Raytheon offered to the LO/CLO TSC & OSD to develop a CPI Guide**
  - Coordinate with Primes through Cabal; services; OSD

Approach

- **Develop a Guide providing a more consistent, repeatable, and accurate process**
    - Common approach for all
- **DASD/SE: Develop the guide from the perspective of the CPI identifier in the field**
    - Don't worry about the myriad of current approaches
    - Do what is right

Must Identify the Crown Jewels Before You Can Protect Them

CAIG

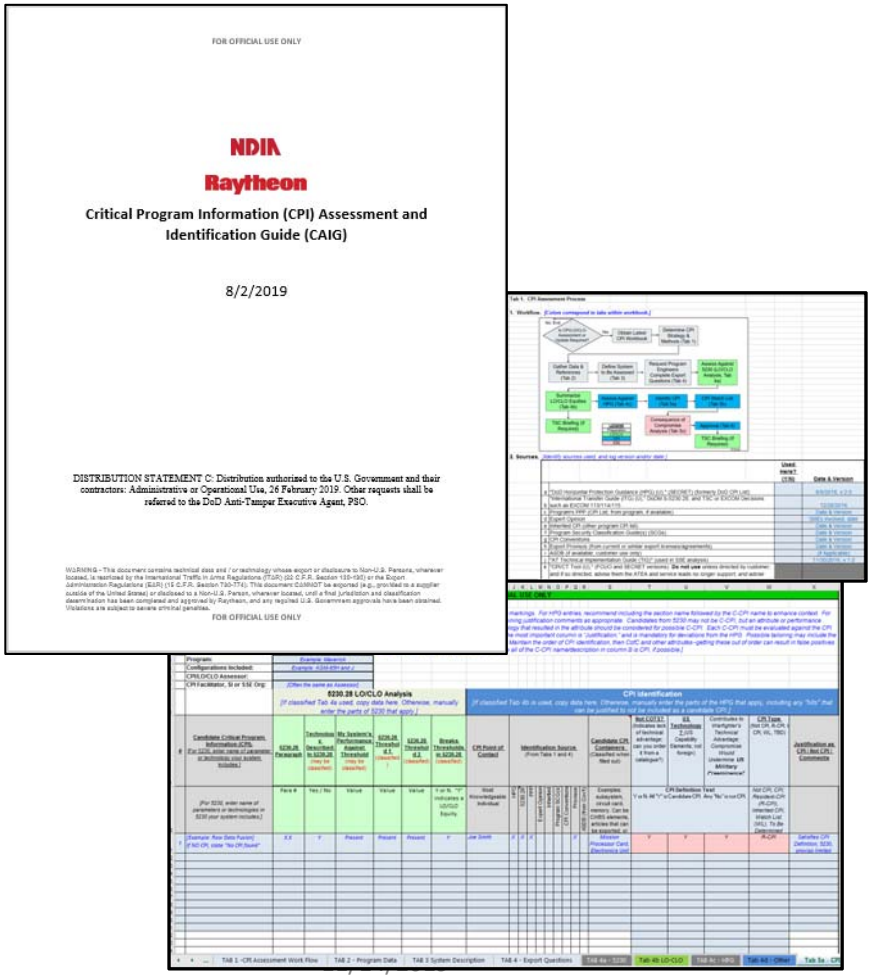
Critical Program Information Assessment & Identification Guide

Two Parts: Guide & Workbook

- **CPI Assessment and Identification Guide (CAIG)**
  - Narrative description of CPI ID process (complements Workbook)
    - CPI policy & guidance
    - CPI ID strategy
    - Application and conventions
    - Best Practices / Warnings / Tips
- **CPI/LO/CLO Workbook**
  - Leads CPI facilitator through CPI/LO/CLO process
  - Ensures thorough documentation
- **Multiple iterations and beta testing**
  - Comments incorporated from Primes, USAF, USN

NDIA CPI Workshop on June 5, 2019

- **Hear from USG and Primes**
- **New tool proposed as a best practice**
  - CPI Assessment & Identification Guide (CAIG
  - CPI / LO / CLO workbook
- **DOD ATEA Web site to maintain latest version**
  - https://at.dod.mil/



Thank you!

- **Champion and Principal Author**
  - Ninja Donatelli
- **LO/CLO Tri-Service Committee**
  - Todd Spates (OUSD(R&E)
  - Kevin “Klingon” Kirk (USAF)
  - Russ Bodine (USA)
  - Emily Burkholder (USN)
  - Dr. Jim Bober (MDA)
- **Ray Shanahan (OUSD(R&E), formerly DASD/SE)**
- **Stephanie Brockway (DASD/SE)**
- **Service AT Leads**
  - Russ Bodine / Matt Bondy (USA)
  - Bill Walters (USN)
  - Lt Col Nathan “Wolf” Pitcher (USAF)
  - Robert Donath (MDA)

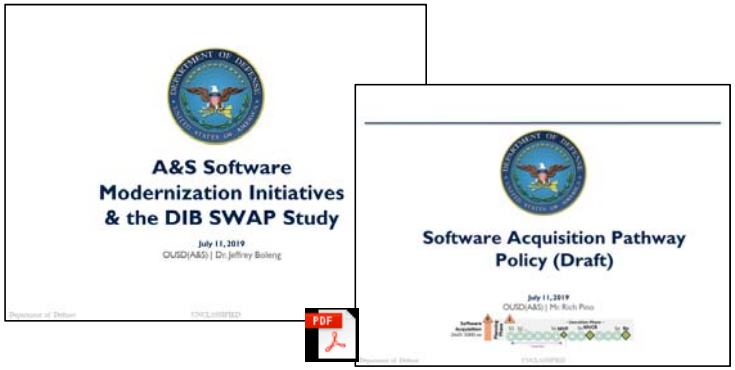
- **NDIA**
  - David Chesebrough
  - Holly Dunlap
- **The AT “Cabal”**
  - Todd Burns / Brian Gleason (Boeing)
  - Tate Keegan (BAE)
  - George Kalb (NGC)
  - John Halpin / Karen Christensen-Grubb (LMCO)
  - Lori Masso, Eric Herr (Raytheon)
- **USG Reviewers**
  - USAF (Matt Perticone)
  - USN (Bill Walters)
- **Staff**

Workshop Attendees

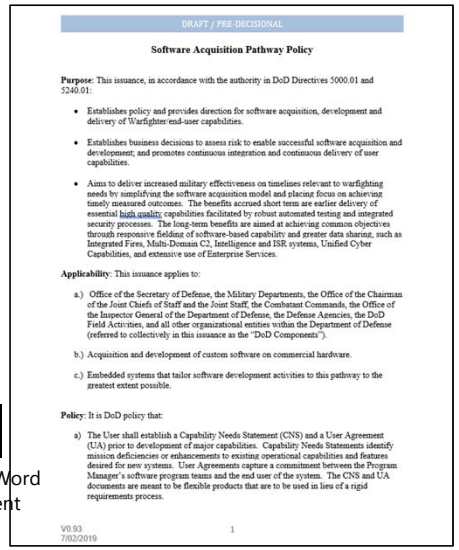
- Sponsors:
  - NDIA
  - OUSD(R&E)
  - Raytheon
- OUSD/A&S
- DAU
- HQDA ASA ALT (USA)
- NAVAIR (USN)
- NAVSEA (USN)
- NSWC Dahlgren (USN)
- ATEA (SAF/AQL) (USAF)
- AFMC AFLCMC/EN
- SAF/AQRE
- USCG
- MDA/EIR
- MDA/DEB
- USSOCOM
- Booz Allen Hamilton
- Boeing
- British Aerospace
- Honeywell
- Lockheed Martin
- Northrop Grumman
- Raytheon

DoD Software Acquisition Pathway (Draft)

- **OUSD (A&S) is seeking industry feedback on draft (1) Software Acquisition Pathway Policy and (2) Business Decision Guidance.** (aka "Software 5000.02")
- **Cross-divisional NDIA review kickoff held at NDIA HQ (7/11/19)**
  - Systems Engineering; ADAPT; Integrated Program Management; Cyber
- **Industry comments widely solicited (various means) thru 8/2/19**



Adobe Acrobat Document



DRAFT / PRE-DECISIONAL

Software Acquisition Pathway Policy

Purpose: This issuance, in accordance with the authority in DoD Directives 5000.01 and 5240.01:

- Establishes policy and provides direction for software acquisition, development and delivery of Warfighter/end-user capabilities.
- Establishes business decisions to assess risk to enable successful software acquisition and development; and promotes continuous integration and continuous delivery of user capabilities.
- Aims to deliver increased military effectiveness on timelines relevant to warfighting needs by simplifying the software acquisition model and placing focus on achieving timely measured outcomes. The benefits accrued short term are earlier delivery of essential high quality capabilities facilitated by robust automated testing and integrated security processes. The long-term benefits are aimed at achieving common objectives through responsive fielding of software-based capability and greater data sharing, such as Integrated Fires, Multi-Domain C2, Intelligence and ISR systems, Unified Cyber Capabilities, and extensive use of Enterprise Services.

Applicability: This issuance applies to:

a.) Office of the Secretary of Defense, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (referred to collectively in this issuance as the "DoD Components").

b.) Acquisition and development of custom software on commercial hardware.

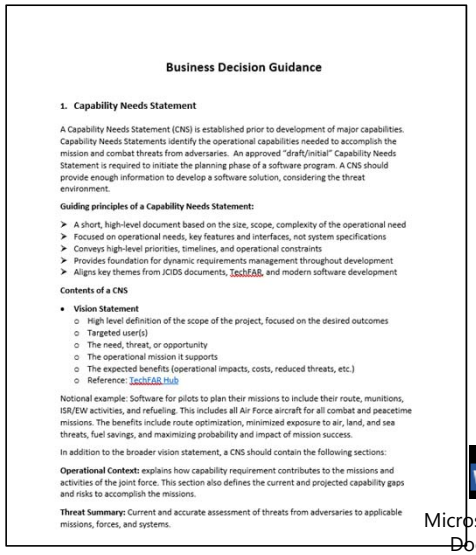
c.) Embedded systems that tailor software development activities to this pathway to the greatest extent possible.

Policy: It is DoD policy that:

a) The User shall establish a Capability Needs Statement (CNS) and a User Agreement (UA) prior to development of major capabilities. Capability Needs Statements identify mission deficiencies or enhancements to existing operational capabilities and features desired for new systems. User Agreements capture a commitment between the Program Manager's software program teams and the end user of the system. The CNS and UA documents are meant to be flexible products that are to be used in lieu of a rigid requirements process.

V0.93
7/02/2019
1

Microsoft Word Document



Business Decision Guidance

1. Capability Needs Statement

A Capability Needs Statement (CNS) is established prior to development of major capabilities. Capability Needs Statements identify the operational capabilities needed to accomplish the mission and combat threats from adversaries. An approved "draft/initial" Capability Needs Statement is required to initiate the planning phase of a software program. A CNS should provide enough information to develop a software solution, considering the threat environment.

Guiding principles of a Capability Needs Statement:

- A short, high-level document based on the size, scope, complexity of the operational need
- Focused on operational needs, key features and interfaces, not system specifications
- Conveys high-level priorities, timelines, and operational constraints
- Provides foundation for dynamic requirements management throughout development
- Aligns key themes from JCIDS documents, TechFAR, and modern software development

Contents of a CNS

- **Vision Statement**
  - High level definition of the scope of the project, focused on the desired outcomes
  - Targeted user(s)
  - The need, threat, or opportunity
  - The operational mission it supports
  - The expected benefits (operational impacts, costs, reduced threats, etc.)
  - Reference: TechFAR Hub

Notional example: Software for pilots to plan their missions to include their route, munitions, ISR/EW activities, and refueling. This includes all Air Force aircraft for all combat and peacetime missions. The benefits include route optimization, minimized exposure to air, land, and sea threats, fuel savings, and maximizing probability and impact of mission success.

In addition to the broader vision statement, a CNS should contain the following sections:

Operational Context: explains how capability requirement contributes to the missions and activities of the joint force. This section also defines the current and projected capability gaps and risks to accomplish the missions.

Threat Summary: Current and accurate assessment of threats from adversaries to applicable missions, forces, and systems.

Microsoft Word Document

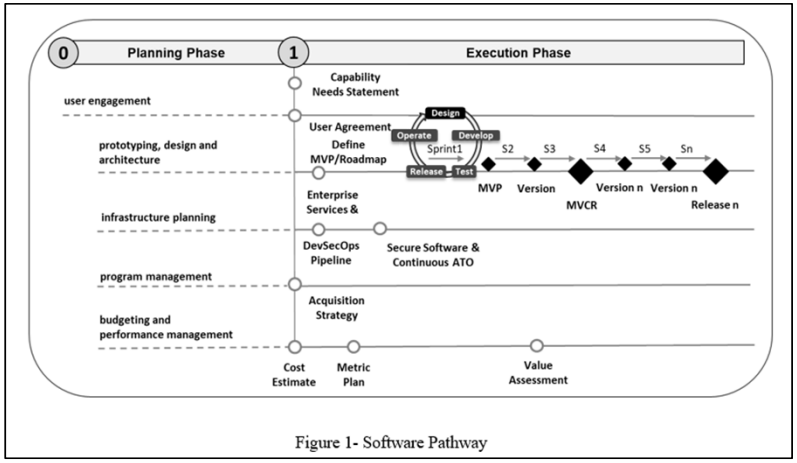


Figure 1- Software Pathway

Summary Level Industry Feedback

Generally very favorable industry feedback on A&S SW policy and guidance. Support DoD intent and direction.
A few areas of concern: SE; Security; Metrics.

General	Key Inputs
• Positive overall concepts, approach, direction • Like Minimally Viable Capability Release (MVCR) concept • …but some terms differing from common industry usage (e.g., MVP) can be confusing for adoption)	• Very strong industry consensus that integration with Systems Engineering must be included • Scope should also apply to custom SW on custom HW /embedded to the extent practical (leverage benefits broadly; few programs are pure SW/COTS) • Strengthen Security integration with Engineering across all aspects of life cycle (DevSecOps) – concept, roadmap, architecture, design, development, test, delivery, … • Security objective is much broader than continuous ATO ► secure, resilient cyber systems – must be designed in • Over-achieved significantly on SW metrics – well beyond prior input recommendations (DSB, DIB SWAP, PSM, NDIA, …) and industry practice. Lack linkage to information needs, actions.

Substantial consensus on these inputs across industry (companies, stakeholder groups)
Many details provided in consolidated commenting spreadsheet and other attachments.

Extensive participation, discussion, and feedback from System Security Engineering (SSE) Committee

Key Take-aways:

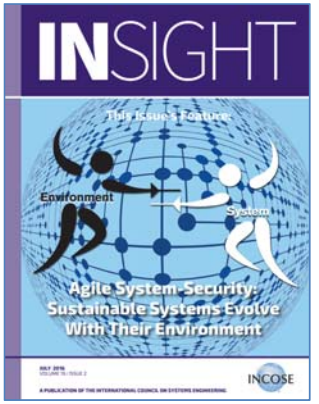
- Security is framed in a way of compliance; to reach Approval to Operate is not to reach a secure system.
- The focus on DevSecOps will contribute significantly to the concept of continuous ATO, but the document omits the need for Application level cybersecurity.
- As many of our products are systems of systems, a holistic appreciation of all security specializations (Cyber, IA, AT, SSE, SwA, SCRM) is necessary; Compliance to RMF Controls only buys a minimum level of assurance and doesn't adequately cover the security specialties in an integrated risk managed trade space.
- Importance of MVCR security requires elevation, fielding a 'minimum' introduces environmental, intended use, and configuration control concerns. A greater definition of a sustainment support community is necessary.
- The push to 'leverage enterprise services' and the level of interaction with the test strategy seems to ignore embedded systems.
- With the shift from monolithic requirements to more agile methodology, cost estimation will be a problem. The top recommendation cited to improve cost estimates is to "define the team size and makeup", which is great for defining how much will be spent but a poor way to determine how much the work should cost. This also assumes a dedicated workforce with the right skills are available. This may work for top priority programs but will be challenging to scale to all programs with the gap in talent.
- While the idea of user testing of an MVP allows for flexibility in terms of capability and design, security is best designed into the architecture from the onset, major revisions may lead to vulnerabilities.
- The flexibility of CNS/UA/MVP is an exciting prospect, but firm high-level requirements are necessary to drive core architecture.
- The document fails to capture the need for systems-level thinking and the involvement of systems engineers and architects.
- Lessons learned include the short story incremental development and review cycles are good but the traditional major reviews are still needed to ensure the big picture isn't lost while focusing on detailed iterative developments.

- **Many additional detailed security-related comments provided in attached notes and commenting spreadsheet**

Microsoft Word Document

Project Charter: Cyber Security in Product Lines

- **Title:** Cyber Security Techniques for Product Line Engineering
- **Project Leadership:** Beth Wilson (SSE WG), Bobbi Young (PLE WG)
- **Customers:** CAB company systems engineers that are engaged in PLE development
- **Project Participants:** Interested members of SSE WG and PLE WG. INCOSE & NDIA
- **Project Description:** The team will evaluate potential techniques to work systems security into the product line design so that the results of the systems security implementation can be used by all the receiving programs that use the product line assets. The team will explore existing PLE and SSE efforts related to architecture and patterns.
- **Objective:** Bring systems security into product line design
  - **Goal**: Identify techniques for implementing systems security as part of product line design
  - **Goal**: Identify patterns for product line architectures that addresses systems security
  - **Goal**: Identify variation management approaches for secure and resilient product line assets
- **Process:**
  - **Timeline:**
    - **IW18**: Include in SSE WG and PLE WG to determine interest, identify project participants
    - **IW18 – IS18**: Monthly virtual meetings to make progress
    - **IW19**: Report results to SSE and PLE working groups
    - **IS19**: Present paper or tutorial on results
  - **Deliverables**: IW presentation, IS paper/tutorial, INCOSE webinar



Proposal approved at IW18

SSE in PLE Project Goals and Objectives

***Project Vision:* Bring systems security into product line design**

- **Goal #1: Identify/develop techniques for implementing systems security as part of product line design**
  - Objective 1.1: SSE/PLE techniques aligned with security standards
  - Objective 1.2: SSE/PLE techniques aligned with business sectors
  - Objective 1.3: SSE/PLE techniques to develop secure and resilient product line assets
  - Objective 1.4: SSE/PLE techniques to perform meaningful security assessment of PL assets
  - Objective 1.5: Guidance for implementing SSE/PLE techniques
- **Goal #2: Identify/develop patterns for product line architectures that addresses systems security**
  - Objective 2.1: Security patterns for product line development representing standard solutions
  - Objective 2.2: Notional examples where SSE is best implemented inside PL
  - Objective 2.3: Notional examples where SSE is best implemented in deployed solution
  - Objective 2.4: Guidance for implementing SSE/PLE patterns
- **Goal #3: Identify/develop variation management approaches for secure and resilient product line assets**
  - Objective 3.1: Requirements approaches for SSE flow-down from PL to solutions
  - Objective 3.2: SSE variation management approaches for PL assets
  - Objective 3.3: Test approaches for PL and deployed solution verification (no gaps, no duplicates)
  - Objective 3.4: Systems security techniques for continuous monitoring of deployed solution
  - Objective 3.5: Guidance for implementing SSE/PLE design approaches
  - Objective 3.6: Communication plan (initial and ongoing) to joint SSE/PLE community

Project Team

Name	Affiliation	Email Address	SSE	PLE
Beth Wilson	Retired	wilsondrbeth@aol.com	INCOSE/NDIA	INCOSE
Bobbi Young	Raytheon	bobbi.young@raytheon.com		INCOSE
Suzanne Hassell	Raytheon	shassell@Raytheon.com	NDIA	
Nate Simcoe	Honeywell	nathan.simcoe@honeywell.com	SSE	
Rick Dove	Paradigm Shift International	dove@parshift.com	INCOSE	
Gerry Ourada	Lockheed Martin Aero	gerry.l.ourada@lmco.com	NDIA	
Christopher Giudice	Honeywell	christopher.giudice@honeywell.com		INCOSE
Jim Teaff	Raytheon	James.K.Teaff@raytheon.com		INCOSE
Deb Thomas	Raytheon	Deborah.R.Thomas@raytheon.com	SSE	
Matt Hause	PTC	mhause@ptc.com	INCOSE	INCOSE
Ly Vessels	Honeywell	ly.vessels@honeywell.com	SSE	
Brian Haan	SAIC	Brian.haan@saic.com	INCOSE	

IEEE NDIA INCOSE
System Security Symposium
April 6-9, 2020

SYSTEMS SECURITY
symposium

The IEEE-INCOSE-NDIA Systems Security Symposium seeks research papers and application studies that focus on the development of secure, safe, and resilient systems. This symposium attempts to address the convergence of cybersecurity, safety, and engineering with interest in the effective application of security principles, methods, and tools to complex systems such as cyber-physical systems, autonomous systems, transportation vehicles, medical devices, large IoT systems, and other systems of interest. Preference will be given to papers and case studies that bridge theory to practice.

Systems Security Symposium 2020
Topics

- Systems Security Work Focused on Advancements in Theory, Practice, and Education
- Engineering of Safe, Secure, and Resilient Systems
- Examples of Mission/Systems Assurance and Assurance Cases
- Model Based Engineering focused on Security, Safety, Trust, Resiliency
- Affordable and Scalable Approaches to Hardware, Software, Firmware Assurance
- Novel Architecture Design and Analysis Examples or Trade-Space Studies
- Trust of Complex Systems with Emphasis on Cyber-Physical Systems
- Security considerations for machine learning / artificial intelligence
- Large-Scale DevSecOps and Agile Approaches for System Development
- System Security Design Considerations for Cloud Environments
- Verification, Validation, and Evidences for Secure System Development
- Extensions of Formal Methods to System-Level Evaluation
- Cybersecurity in Manufacturing and Supply Chains
- Case studies to include automotive, transportation, space, and others
- Cyber-Physical System Event Detection, Investigation, Forensics, and Malware Analysis
- Tailored Risk Management Approaches for Large Complex Systems
- Attack/Defense Modeling, Simulation, and Characterization
- Techniques for Cyber Risk Buy Down in Legacy Systems, Infrastructure, and Enterprises
- Policy, Ethical, Legal, Privacy, Economic, and Social Issues

http://www.ieeesystemssecuritysymposium.org

Questions?