NDIA System Security Engineering Committee

February 2019

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

Cory Ocker
Raytheon
Cory.Ocker@Raytheon.com

System Security Engineering Committee Meeting Agenda

2/05/2019 1:30 PM – 3:30 PM EST, Lockheed Martin Crystal City

- **Top 2019 Priorities for the NDIA SSE Committee**
- **NDIA Iterative Software Development and Acquisition Working Group Update**
  - NDIA Systems Engineering Division Chair, Joe Elm
- **Review, Edit, and Finalize Committee Charter** (Available in the backup slides)
- **Approach to the Review of the AF SSE Acquisition Guidance v 1.4**
- **NDIA INCOSE IEEE System Security Symposium March 16 – 19, 2020**
- **JFAC Software Assurance Guidebook and SOW Language**
  - OSD Joint Federated Assurance Center SwA Deputy Director, Tom Hurt
  - NDIA SwA Committee Chair, Ken Nidiffer
    Principal Systems and Software Engineer
    Carnegie Mellon University, Software Engineering Institute.
- **INCOSE SSE Committee Tasks and Collaboration Opportunities**

Top Priorities for 2019

- **Review and Comment on AF SSE Acquisition Guidance v 1.4 to provide an industry perspective.**
- **Cyber appendix to the DoD Risk, Issue, and Opportunity Management Guide.**
- **Provide input on DoDI 8140.01, Cybersecurity Workforce Management development (replacement of DoDI 8570.01)**
- **Continue collaboration with INCOSE SSE Committee, SAE Cyber Physical Systems, NDIA Electronics Division, AF CROWS, JFAC, AF CITAG, etc.**
- **IEEE, NDIA, INCOSE System Security Symposium**

AF SSE Acquisition Guide 1.4 Review & Comment

Valuable opportunity to influence AF programs RFP system security requirements.

We have been through several rounds of reviews. We are seeing pretty dramatic changes and improvements.

Completed an interim review of AF SSE Acquisition Guidebook v 1.4 in December.
Continue 2018 effort in 2019 and initiate a thorough review of v 1.4.

Each Company / Organization (No individual solo responses.)

- Each company provides a **Top 5 List of Concerns**, requested changes, recommendations, etc.
- Each company is encouraged to provide **3 positives**.
- Each company provides a single set of **detailed comments** using the comment resolution matrix (CRM).

NDIA SSE Committee

- Committee meeting to discuss developing a **Top 10 List of Concerns and Top 5 List of Positive Comments**
  - Active committee members will be provided the collective lists of Top 5 Concerns and Top 3 Positives prior to the meeting.
  - Iterate and refine if needed to develop the NDIA SSE Committee Top 10 List of Concerns and Top List of Positive Comments.
- Collate detailed comments using the Comment Resolution Matrix (CRM). doc from each company. Company names will be removed from the detailed CRM before collating and providing to the AF.
- Finalize and develop detailed report for the AF.

** See backup slides for detailed dates and review process

IEEE NDIA INCOSE
System Security Symposium
March 17 – 19, 2020

SYSTEMS SECURITY
symposium

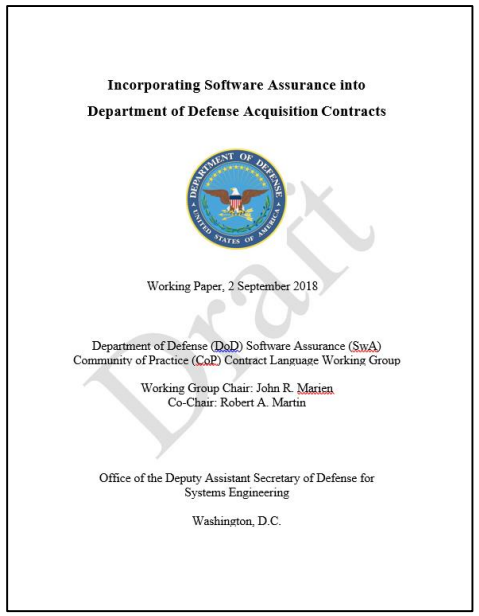
This symposium attempts to:

- Bringing together multiple industries such as defense, aerospace, medical, transportation, etc.
- Address the convergence of cybersecurity and engineering with interest in the effective application of security principles, methods, and tools to complex systems such as cyber-physical systems, autonomous systems, IoT devices, transportation systems, medical devices, and other systems of interest.

The conference caters to both practitioners and academics, providing a forum to exchange ideas and experiences on technology, methodology, applications, study cases, and practical experiences.

Note that unlike typical NDIA conferences, this one will require submission of either full 8-page research papers or 1-3 page papers on case studies and practical experiences for consideration.

OSD Joint Federated Assurance Center Software Assurance Acquisition Language & SEI Software Assurance Guidebooks



Incorporating Software Assurance into
Department of Defense Acquisition Contracts

Working Paper, 2 September 2018

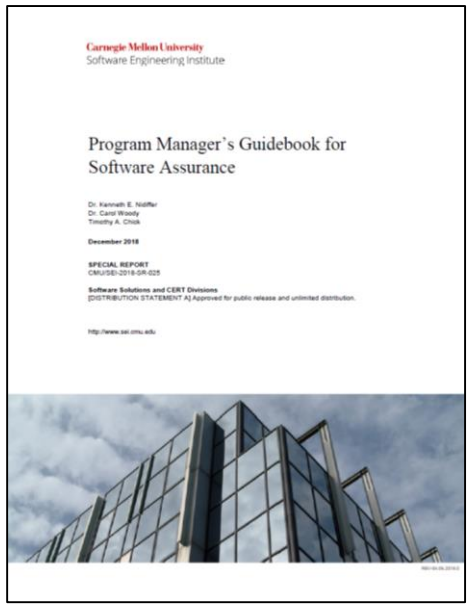
Department of Defense (DoD) Software Assurance (SwA)
Community of Practice (CoP) Contract Language Working Group

Working Group Chair: John R. Marien
Co-Chair: Robert A. Martin

Office of the Deputy Assistant Secretary of Defense for
Systems Engineering

Washington, D.C.

Draft



Carnegie Mellon University
Software Engineering Institute

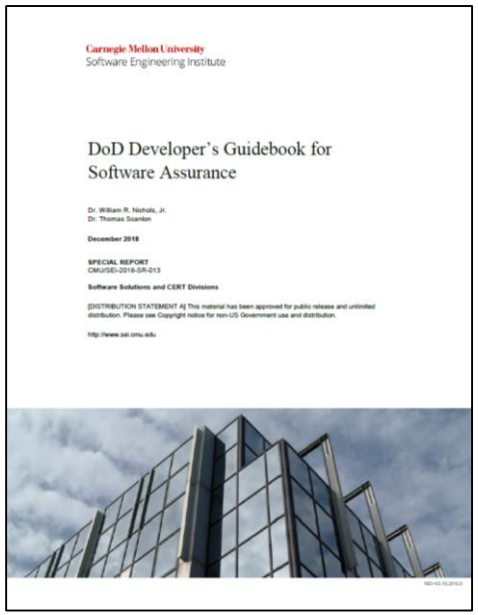
Program Manager's Guidebook for Software Assurance

December 2018

SPECIAL REPORT

Software Solutions and CERT Divisions

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=538771



Carnegie Mellon University
Software Engineering Institute

DoD Developer's Guidebook for Software Assurance

December 2018

SPECIAL REPORT

Software Solutions and CERT Divisions

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=538756

Backup

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.**

AF SSE Acquisition Guide 1.4 Review & Comment

Valuable opportunity to influence AF programs RFP system security requirements.

We have been through several rounds of reviews. We are seeing pretty dramatic changes and improvements.

How do we, NDIA SSE Committee, provide an industry perspective in the most valuable and efficient way possible?

Each Company / Organization (No individual solo responses.)

- Each company provides a **Top 5 List of Concerns**, requested changes, recommendations, etc.
- Each company is encouraged to provide **3 positives**.
- Each company provides a single set of **detailed comments** using the comment resolution matrix (CRM).

NDIA SSE Committee

- Committee meeting to discuss developing a **Top 10 List of Concerns and Top 5 List of Positive Comments**
  - Active committee members will be provided the collective lists of Top 5 Concerns and Top 3 Positives prior to the meeting.
  - Iterate and refine if needed to develop the NDIA SSE Committee Top 10 List of Concerns and Top 3 Positive Comments.
- Collate detailed comments using the Comment Resolution Matrix (CRM). doc from each company. Company names will be removed from the detailed CRM before collating and providing to the AF.
- Finalize and develop detailed report for the AF.

AF SSE Acquisition Guide 1.4 Review & Comment

- **Review is not constrained to any specific section, but majority of recent changes consolidated in a few key areas**
  - 1.1.1 ICD, CDD, CPD
  - 1.10 Risk Management
  - 2.2 SRD and System Specifications
  - 2.3 Statement of Objectives (SOO) and Statement of Work (SOW)
  - Attachments 1 and 2 (new)
- **Top 5 Concerns**
  - The top 5 list is not constrained by the comment matrix format.
  - Propose (1) summary bullet and (3) supporting bullets to describe why. What is the importance? What is the impact?
- **Top 3 Positives**
  - The top 3 list is not constrained by the comment matrix format.
  - If available, identify programs that have used this guidance and describe the benefits it had on the program

Provide all feedback, comments, lists to:
Cory Ocker - Cory.L.Ocker@Raytheon.com
Holly Dunlap – Holly.Dunlap@Raytheon.com

Schedule


february
2019
MONDAY
TUESDAY
WEDNESDAY
THURSDAY
FRIDAY
SAT/SUN
28 January
29
30
31
1 February
2/3
4
5
6
7
8
9/10
11
12
13
14
15
16/17
18
19
20
21
22
23/24
25
26
27
28
1 March
2/3
4
5
6
7
8
9/10
Top 5 List of Concerns
3 Positive Comments
SSE Committee Meeting
1:30 – 3:30 PM EST
SSE Committee Meeting
Top 10 & 5 Lists


march
2019
MONDAY
TUESDAY
WEDNESDAY
THURSDAY
FRIDAY
SAT/SUN
25 February
26
27
28
1 March
2/3
4
5
6
7
8
9/10
11
12
13
14
15
16/17
18
19
20
21
22
23/24
25
26
27
28
29
30/31
1 April
2
3
4
5
6/7
Detailed Comments
via CRM
Deliver Final Report to AF

Cyber appendix to the DoD Risk, Issue, and Opportunity Management Guide

- Presented planned organization at NDIA SE Conference
- Matches sections, ToC, and format of main guide
- Drafting appendix language in work
- Need other volunteers for content generation

IEEE NDIA INCOSE
System Security Symposium
March 17 – 19, 2020

SYSTEMS SECURITY
symposium

This symposium attempts to:

- Bringing together multiple industries such as defense, aerospace, medical, transportation, etc.
- Address the convergence of cybersecurity and engineering with interest in the effective application of security principles, methods, and tools to complex systems such as cyber-physical systems, autonomous systems, IoT devices, transportation systems, medical devices, and other systems of interest.

The conference caters to both practitioners and academics, providing a forum to exchange ideas and experiences on technology, methodology, applications, study cases, and practical experiences.

Note that unlike typical NDIA conferences, this one will require submission of either full 8-page research papers or 1-3 page papers on case studies and practical experiences for consideration.

IEEE NDIA INCOSE
System Security Symposium
March 17 – 19, 2020

SYSTEMS SECURITY
symposium

Call for Paper Key Dates:

- **July 31, 2019**: Special Sessions & Tutorial Proposals
- **August 30, 2019**: Initial Manuscript & Abstract Deadline
- October 31, 2019: Acceptance Notification
- January 31, 2020: Final Paper Deadline

Looking for additional
Technical Program Committee
members to help review submissions.

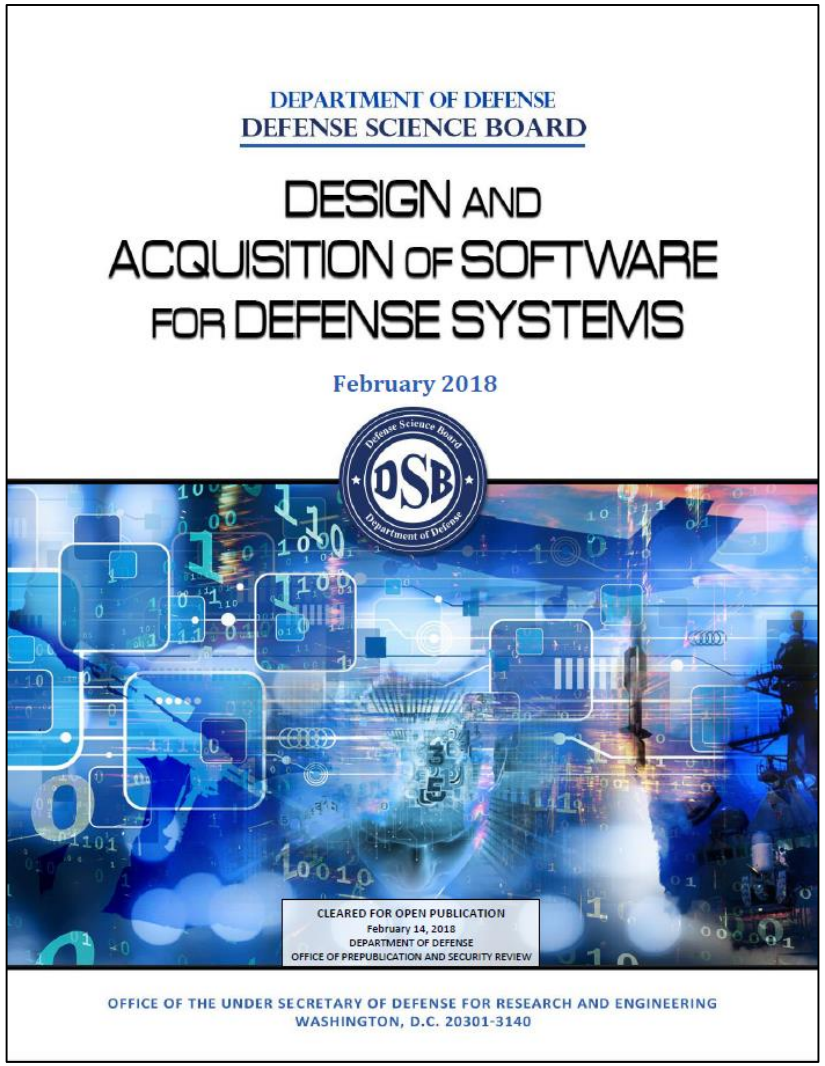
If interested, contact **Steve Holt**
smdholt@gmail.com

IEEE NDIA INCOSE
System Security Symposium
March 17 – 19, 2020

Areas of Interest Include:

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
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

NDIA Iterative Software Development and Acquisition Working Group Update



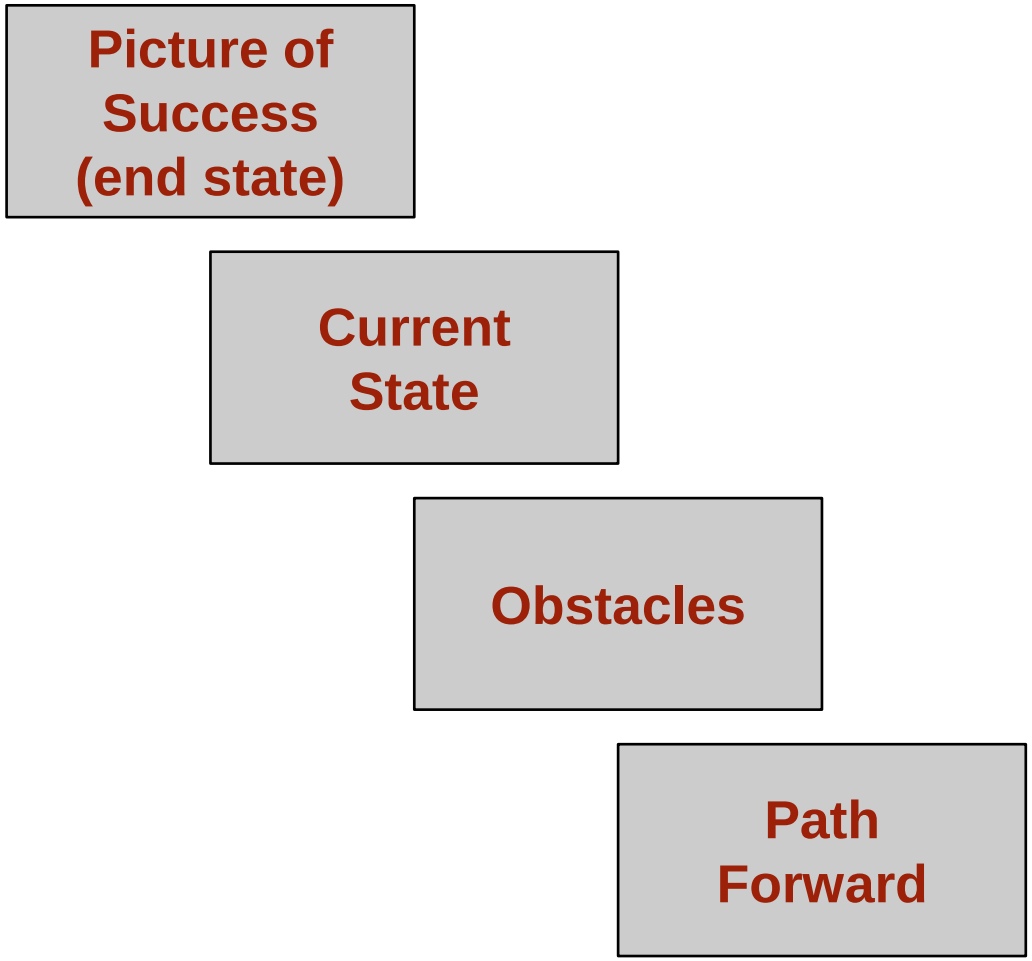
- Defense Science Board (DSB released a report in Feb-2018 containing seven recommendations regarding software design and acquisition
- Section 868 of NDAA 2019 mandates implementation of these recommendations within 18 months
- Continuous Iterative Development and Acquisition Working Group (CIDAWG) formulating industry perspective for implementing recommendations

NDIA Iterative Software Development and Acquisition Working Group Update

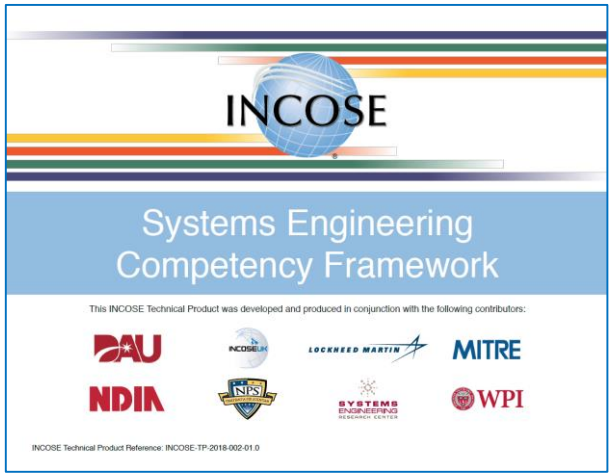
1. **Software Factory** – A key evaluation criteria in the source selection process should be efficacy of the offeror's software factory.
2. **Continuous Iterative Development** – DoD and defense industrial base partners should adopt continuous iterative development best practices for software, including through sustainment.
3. **Risk Reduction and Metrics for New Programs** – For all new programs, starting immediately, implement best practices in formal program acquisition strategies (multiple vendors and down-selects, modernized cost and schedule measures, status estimation framework)
4. **Current and Legacy Programs in Development, Production, and Sustainment** – For ongoing development programs, PMs/PEOs should plan transition to a software factory and continuous iterative development.
5. **Workforce** – The U.S. Government does not have modern software development expertise in its program offices or the broader functional acquisition workforce. This requires Congressional engagement and significant investment immediately.
6. **Software is Immortal: Software Sustainment** – RFPs should specify the basic elements of the software framework supporting the software factory… reflected in source selection criteria
7. **IV&V for Machine Learning** – Machine learning is an increasingly important component of a broad range of defense systems, including autonomous systems, and will further complicate the challenges of software acquisition.

NDIA Iterative Software Development and Acquisition Working Group Update

1. Software Factory
2. Continuous Iterative Development
3. Risk Reduction and Metrics for New Programs
4. Current and Legacy Programs in Development, Production, and Sustainment
5. Workforce
6. Software is Immortal: Software Sustainment
7. IV&V for Machine Learning



INCOSE Collaboration – Competency Model Project



Joint Effort:

- NDIA SED SSE, Education & Training Committee
- INCOSE SSE WG, Competency WG

2015 Effort:

- Identified SSE roles and activities
- Tested competency framework taxonomy

Next Steps:
Formalize
SSE Roles and
Competencies

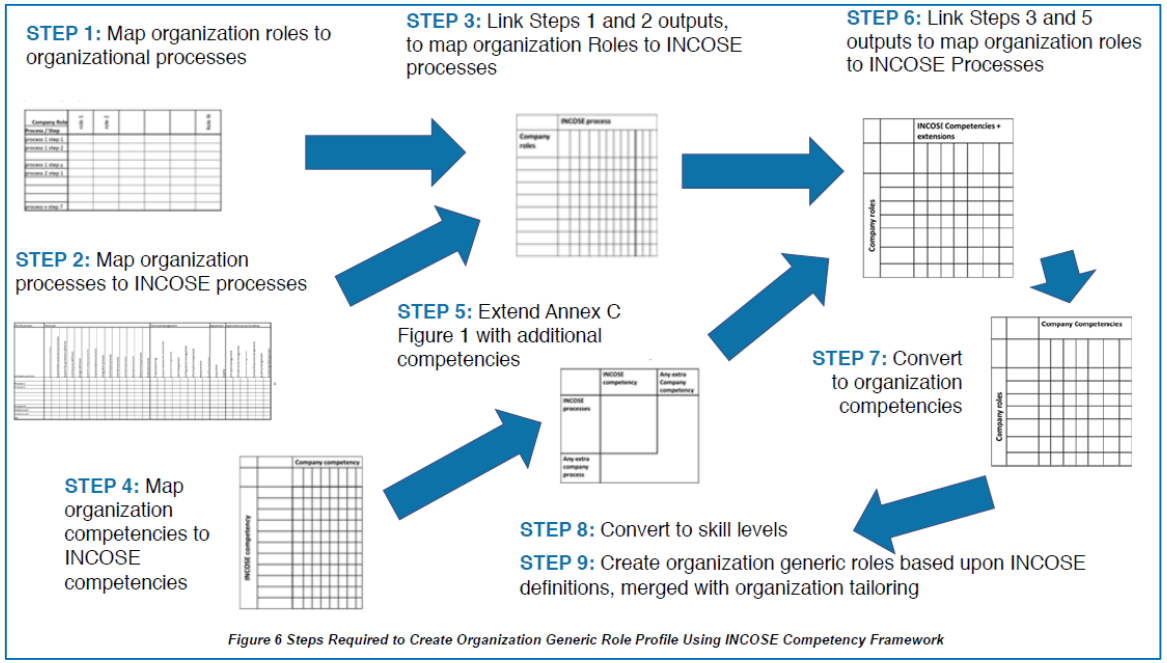


Figure 6 Steps Required to Create Organization Generic Role Profile Using INCOSE Competency Framework

Beth Wilson
INCOSE SSE WG Co-Chair

Holly Dunlap
NDIA SSE Committee Chair

2015, 2019 Planned

INCOSE Collaboration – Competency Model Project

Systems Engineering Role-Based Competency Model
Role – System Security Engineering
Role Description: System Security Engineering (SSE) is a specialty engineering discipline within Systems Engineering (SE) focused on ensuring a system can function under disruptive conditions associated with misuse and malicious behavior. SSE involves a disciplined application of SE principles in analyzing threats and vulnerabilities to systems and assessing and mitigating risk to the information assets of the system during its lifecycle. It applies a blend of technology, management principles and practices, and operational rules to ensure sufficient protections are available to the system at all times.
Why it matters: Appropriate SSE activities are needed because an adversary may attempt to sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.

Activities: Supply Chain Risk Management, Cyber Security, OPSEC, Software Assurance, Anti-Tamper

Joint Effort:

- NDIA SED SSE, Education & Training Committee
- INCOSE SSE WG, Competency WG

INCOSE SE Competency Model Taxonomy:

SE Role	A collection of interrelated and interdependent activities assigned to a person in a contextual environment such as Systems Engineering
Activity	A specified pursuit defined by a set of essential functions and desired outcomes that enable the successful accomplishment of one's role
Category	A grouping of closely related competencies considered essential to an individual's ability to successfully perform an activity
Competency	An observable and measurable pattern of knowledge, skills, abilities, behaviors, and other characteristics that an individual needs to successfully perform an activity
Description and Why It Matters	A depiction of the competency that clearly defines its essential function, desired outcomes and reasons for why the competency is needed
Knowledge Skills Abilities Behaviors	The measurable characteristics of proficiency that make up a competency

SSE Committee 2018 Summary

- System Security Engineering Committee 2018 Accomplishments
- Issues & Needs
- SECNAV Cybersecurity Advisory Panel Meeting with NDIA Delegation
- Formulating a 2020 Early Spring System Security Symposium sponsored by NDIA, INCOSE & IEEE
- Draft New NDIA SSE Committee Charter

NDIA SSE Committee 2018 Accomplishments

- **SSE Committee Project - Risk, Issue, and Opportunity (RIO) Management Guide for Cybersecurity.**
- **Office of the Secretary of Defense (OSD) Systems Engineering (SE) Cyber Resiliency Weapon Systems (CRWS) Workshop #6, Workforce Development, July 2018**
- **AF Cyber Resiliency Office of Weapon Systems (CROWS) Industry Round Table – April 25th & September 20th, 2018**
- **AF Life Cycle Industry Days, Weapon Systems Cyber Security / Resiliency Panel, September 13, 2018**
- **AF System Security Engineering Acquisition Language Guidebook v 1.3 Review and Comment**
- **NIST SP 800-160 Volume 2, Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems. Review & Comment. Joint project with INCOSE SSE Committee.**
- **SAE Cybersecurity Workshop, January 22-23, 2018**

  This jointly sponsored SAE and NHTSA Vehicle Cybersecurity Workshop brought together experts from various sectors and government agencies dealing with cyber physical systems (CPS), including leading CPS thinkers from information technology, Industrial Control Systems, Internet of Things, Platform Information Technology, and embedded systems. Discuss actionable next steps and collaboration opportunities that would help address challenges unique to CPS architectures, including software, firmware, and hardware.
- **SAE International Cyber Physical Systems Security Meeting, September 25th, 2018**
- **Collaboration with AF Aircraft Cybersecurity Industry Technical Advisory Group (CITAG)**
- **SSE Committee representative, Thierry Wanji , supporting the NDIA ISDA DSB Software Acquisition Report.**
- **Navy Cybersecurity Task Force Advisory Board meeting – NDIA SSE Committee Chair Member of the NDIA delegation, November 15th at the Pentagon**
- **Planning a joint NDIA, INCOSE, IEEE System Security Symposium end of March / beginning of February 2020 in DC Area. Working on dates and details.**

Issues & Needs

- Electronic file sharing of documents to include FOUO and other unclassified documents which require encryption.
- This is a significant problem.
- Army Knowledge Share is no longer an option.
- We have over +300 members on our SSE Committee distribution list.
- Right now the best we have is point to point sharing which is inefficient and not a good use of experts premium time.
- This is true for not only committees but also for sharing NDIA Systems Engineering Division briefings from government partners.
- Telecon and web based support for Divisional and Committee meetings with proper microphones, acoustics, speakers, etc so more members in government and industry can participate.

Securing the Navy's Cyberspace Domain

- Secretary of the Navy, Richard Spencer, issued a memo directing a comprehensive cybersecurity review. October 12, 2018
- **Cybersecurity Advisory Board:** Michael J Bayer, William H. Swanson, John M. B. O'Connor, and Ronald S. Moultrie.
- **NDIA delegation** met with the advisory board on November 15th at the Pentagon.

- Questions for the NDIA Delegation:
  1. How do you consider the state of cybersecurity talent and awareness in the private sector and industry?
  2. Do you see any warning signs with the supply chain and how does the private sector factor that into their risk matrix?
  3. What role do you think culture plays to achieve success related to cyber in the private sector and industry?
  4. What is the biggest threat in the private sector and industry?
  5. How does the private sector and industry receive / share vulnerability, threat, compromise information and how do they want to receive / share it?

Some potential follow up actions for NDIA are:

- A discussion led by the big 5 CISOs on supply chain security/visibility, "low-hanging fruit" , and ideas about a future state.
- An update of the Cybersecurity for Advanced Manufacturing study, once a Government "sponsor" is identified
- An NDIA "Securing the DIB" initiative focused on out reach and education of the businesses that are in the lower tiers of the supply chains.

SECNAV Cybersecurity Advisory Panel Meeting
NDIA Delegation

- **General Herbert "Hawk" Carlisle, USAF (ret),** CEO, NDIA
- **MG James Boozer**, UAS (ret), Chief of Staff, NDIA
- **Dave Chesebrough**, VP Divisions, Leading the NDIA Securing the DIB initiative
- **Mike Papay,** Chief Information Security Officer, Northrop-Grumman representing the Big 5 CISOs
- **Lt Gen William Bender,** USAF (ret), Strategic Account Executive, Government Relations, Leidos
- **Dr. Mike Mcgrath**, McGrath Analytics (small business), former DASN (RDT&E) and PM at DARPA
- **Kaye Ortiz,** ANSER and Defined Business Solutions (small business), Electronics and Cybersecurity Division, leader of the second Cybersecurity for Advanced Manufacturing Study done for DASD Systems Engineering
- **Holly Dunlap,** Strategic Planning & Technical Intelligence, Raytheon, chair of the Systems Security Engineering Committee of the Systems Engineering Division
- **Robert Metzger**, Attorney, Rogers Joseph O'Donnell, one of the authors of the Mitre Deliver Uncompromised report
- **Ezra Hall,** Director Aerospace and Defense, Global Foundries, leads microelectronics trust and assurance committee for the Electronics Division
- **Titako "Rocky" Takapu**, Principal Member of Technical Staff, Draper Lab involved with System Security Engineering and designing and building secure architectures
- **Jeffrey C. ("J.C.") Dodson**, Global Chief Information Security Officer (CISO), Vice President, Cybersecurity, BAE Systems