NDIA System Security Engineering Committee
April 2019

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

Cory Ocker
Raytheon
Cory.Ocker@Raytheon.com

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**

System Security Engineering Committee Meeting Agenda

4/09/2019 1:30 PM – 5:30 PM EST, Lockheed Martin Crystal City

Call in information: (877)336-1275 Access Code: 3019886

Agenda:

- **Opening Remarks NDIA SSE Committee Chair, Holly Dunlap**
- **Deep Dive review of SwA products (Ken Nidiffer, Software Engineering Institute)**
  - SEI Program Manager's Guidebook for Software Assurance
  - SEI DoD Developer's Guidebook for Software Assurance
- **Update from ASD(R&E) on Engineering Cyber Resilient Weapon Systems activities (Melinda Reed)**
- **INCOSE/NDIA System Security Engineering/Product Line Engineering Project Update (Beth Wilson)**
- **DoD 8140, Cyberspace Workforce Management, Instruction and Manual Update (OSD CIO's office, John Koprowski and Michele Moss)**
- **Anti-Tamper Cabal Industry Draft Critical Program Information Identification Guide – Coming Soon**
- **NDIA INCOSE IEEE System Security Symposium, 6-9 April, 2020**

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.

Finalizing

** See backup slides for detailed dates and review process

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

SYSTEMS SECURITY
symposium

General Chair
Bob Rassa
IEEE Systems Council
RCRassa@Raytheon.com

Technical Program Chair
Holly Dunlap
NDIA
Holly.Dunlap@raytheon.com

Technical Program Co-Chair
Logan Mailloux
United States Air Force
Logan.mailloux@us.af.mil

Technical Program Committee:
Steve Holt
IEEE Systems Council
smdholt@gmail.com

Kathleen Kramer
IEEE Aerospace & Electronic Systems Society
kramer@sandiego.edu

Tom McDermott
Systems Engineering Research Center
tmcdermo@stevens.edu

Beth Wilson
INCOSE
wilsondrbeth@aol.com

Melinda Reed
OUSD (R&E)
melinda.k.reed4.civ@mail.mil

For Information Contact:
Shelby Lussier
slussier@conferencecatalysts.com

Location
Marriott Crystal Gateway
Crystal City, VA, USA

SUBMISSION DEADLINES
July 31, 2019
Special Sessions & Tutorial Proposals

August 30, 2019
Initial Manuscript & Abstract Deadline

October 31, 2019
Acceptance Notification

http://www.ieeesystemssecuritysymposium.org

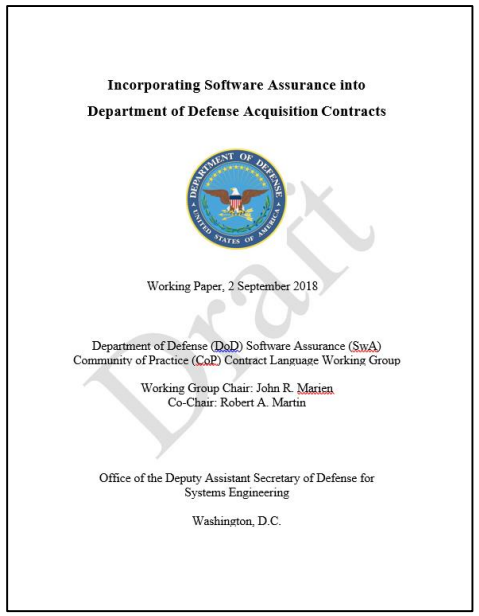
SYSTEMS SECURITY
symposium

IEEE NDIA INCOSE
System Security Symposium
April 6-9, 2020
http://www.ieeesystemssecuritysymposium.org

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

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

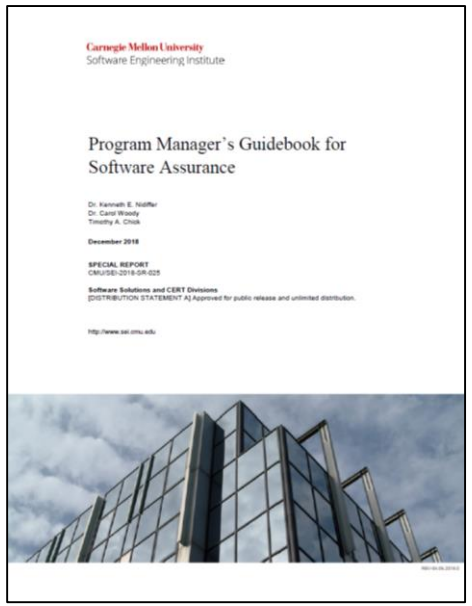
Department of Defense (DoD) Software Assurance (SwA)
Community of Practice (CoP) Contract Language Working Group

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

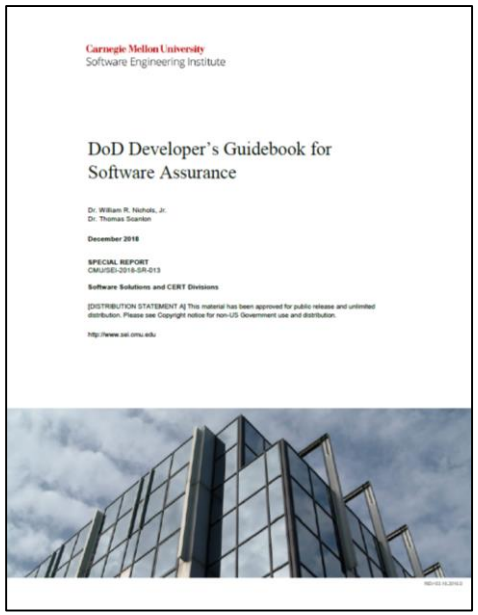
Program Manager's Guidebook for Software Assurance

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

Secretary of the Navy Cybersecurity Readiness Review

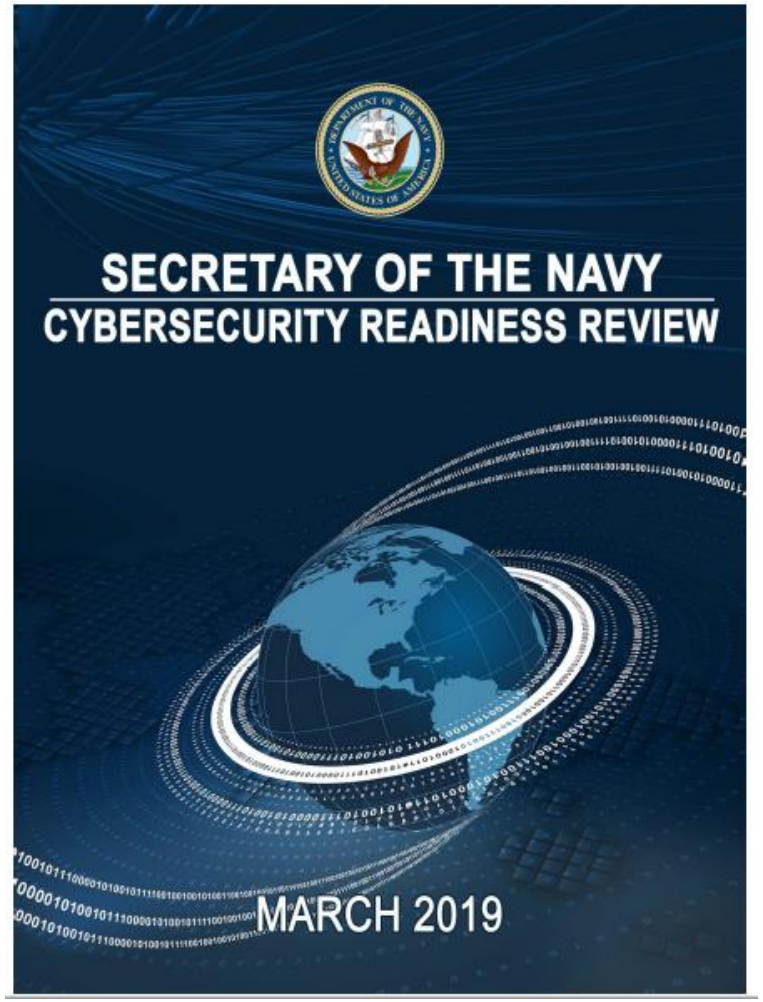
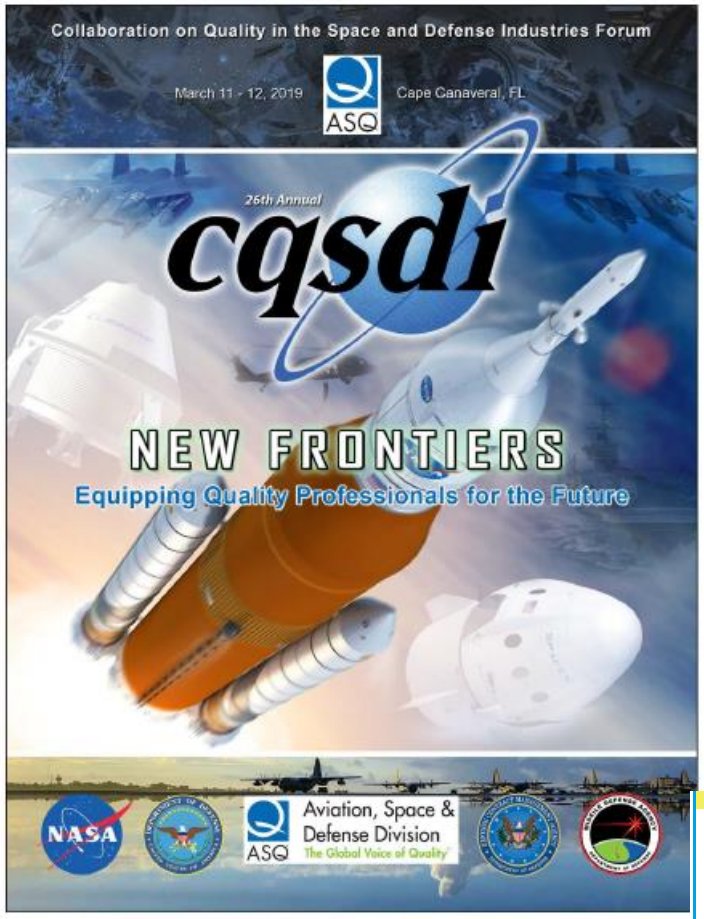


Table of Contents

Quality in the Space and Defense Industry

March 11-12, 2019
Cape Canaveral, FL



Session 1 Panel

Cyber Physical System Security: Control of Satellites in Space, UAV Hardware, Malware

Abstract: Cyber Physical Systems Security (CPSS) is an emerging and important field to ensure quality, reliability, safety, and security of cyber physical systems. Cyber physical systems includes Industrial Control Systems (ICS), Internet of Things (IoT) systems, Platform Information Technology (PIT) systems, and embedded systems. There is a need for government, industry, and academic collaboration and action to address vulnerabilities unique to microelectronic parts and security of Cyber Physical Systems (CPS).

Attacks are often the result of exploited vulnerabilities in cyber physical systems. The intent of the attacks may include economic espionage, denial of services,or more nefarious intentions. Systems level hackers study the system to determine the vulnerabilities that enable an attack. Cyber physical systems are susceptible to successful attacks due to unintended vulnerabilities introduced with the integration of complex hardware, software, and firmware supporting the critical infrastructure of the system without a holistic integrated approach to close the gaps in the multiple areas of concern.

Dan DiMase (Moderator), President & CEO, Aerocyonics
Gloria Danna, SAE CyberSecurity for Commercial Vehicles
Holly Dunlap, Sr. Principal Engineer, Raytheon
Dr. Brian Cohen, Research Staff Member, Information Technology and Systems Division of the Institute for Defense Analyses (IDA)

The panel will emphasize solutions from a systems engineering perspective that includes analysis of the system operating environment defined by the operational, functional, and architectural systems engineering elements can help close the gaps. The discussion will include the need for a common lexicon of terms and metrics to assess vulnerabilities associated with design of the system resulting in a more robust and resilient CPS. The discussion will address gaps in the resiliency of hardware assurance and security from persistent and dynamic threats to cyber physical systems.

The panel includes participation from government, industry, and academia who recognize a need for action in developing a systems engineering approach to standardization of cyber physical systems security, and will include ideas how to:
- Advance the knowledge of how vulnerabilities are introduced and exploited in cyber physical systems
- Identify best practices for addressing different areas of concern
- Develop a detailed taxonomy for cyber physical system security
- Establish and standardize methods for identifying vulnerabilities in cyber physical systems that could be introduced at any point in the CPS life cycle
- Develop cost-effective design and evaluation methods for use in cyber physical systems security design that includes assessing effectiveness of solutions.

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

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.