NDIA System Security Engineering Committee

February 2025

Cory Ocker
NDIA SE Division Vice Chair
NDIA SSE Committee Chair
Cory.L.Ocker@rtx.com

Agenda

- **NDIA SED F2F Planning Meeting Summary**
- **FAR CUI Proposed Rule**
- **CUI Sanitization Project**
- **FAR Cyber Workforce Proposed Rule**
- **CISA/FBI Product Security Best Practices Update**
- **Update on open FAR cases**
  - Supply Chain Software Security (SSDF) – last updated 5/30/2024
  - Cyber Threat and Incident Reporting and Information Sharing (SBOM) – Report delayed since 4/17/2024

NDIA SED F2F

Time	Topic	Who
8:15 – 8:30	**Opening and Objectives**	Dr. Suzette Johnson Laura Hart and Cory Ocker
8:30 – 10:00	Stakeholder Digital Transformation Priorities Around the room. Share a few words or slides and their top 3 – 5 priorities	Government Partners /Stakeholders
10:05 – 10:20	Break	
10:20 – 10:40	Introduction to the Stakeholder Traceability Approach	Laura Hart
10:40 – 12:00	Committees share their quad chart summary and traceability matrix/roadmap Use committee input to build a NDIA SED integrated Digital/SE roadmap	Architecture, DEE, ADAPT, SSE
12:15 – 1:15	Lunch	
1: – 2:35	Continue: Committees share their quad chart summary and traceability matrix/roadmap Use committee input to build a NDIA SED integrated Digital/SE roadmap	M&S, SoS ME, ATC, T&E Division
2:35 – 3:00	Discussion: Strengths, Gaps and Opportunities	
3:00 - 3:15	Break	
3:15 – 4:15	Feedback from our Stakeholders	Government Partners /Stakeholders
4:15 – 4:30	Retrospective	Cory Ocker
4:30 – 5:00	Review actions, Wrap-up/Closing	Suzette Johnson

Full briefings can be found here: https://www.ndia.org/divisions/systems-engineering/division-meetings

Opportunities Identified from SED F2F

- Opportunities
  - Translate our capabilities to usability in other application areas (pull vs push)
  - Tailor value to the audience/discipline
  - Create various use cases across the digital threads
  - Better identify and engage in collaboration to be a force multiplier
  - Model interfaces and transitions between different phases of development
  - Engage with other organizations to increase output
  - Rebirth systems engineering term
  - Communication/marketing opportunity to show business case; manageable objectives w/ feedback loop
  - Submit Papers to NDIA Magazine
  - Restoring Freedom's Forge: American Innovation Unleashed | CTO Palantir Defense Reformation
  - Engage with manufacturing division to identify areas where SE drives pain in manufacturing
  - Evaluate incremental contracting looking across the value stream
  - Individual companies to drive a common message on the benefits of systems engineering in delivering capabilities facilitated by NDIA
  - Where are accredited degrees coming from to help push institutionalization of SE in both USG and Industry

FAR CUI Proposed Rule – Comments due 17 March

- Summary – adds CUI requirement across the federal government with a form to identify CUI data leveraging DFARs-like guidance
- Comments being collected above the SSE committee level within NDIA
- From Cybersecurity Division, concerns focused around:
  - Will this eventually require a CMMC-like verification program?
  - CUI Marking Regime is disjointed and inconsistent (DoD v Commercial, EAR/ITAR v CUI)
  - CUI Identification occurs at the of solicitation (which hasn't worked in the past)
  - Is the SF-XX, Controlled Unclassified Information, tailored by programs or just "yes, there is CUI"
  - When does CUI end in the supply chain? -> Drives sanitization
  - Legal protections in contracts
  - Claims that DIB generated data is CUI

*https://www.federalregister.gov/documents/2025/01/15/2024-30437/federal-acquisition-regulation-controlled-unclassified-information

CUI Sanitization

Lessons Learned

- **Guidance required for sanitizing CUI in order to limit flow of sensitive data down the supply chain; Sanitizing CUI will also save money by reducing the flow of DFARS network requirements**
  - Current lack of guidance drives personal risk when appropriately trying to limit the flow of sensitive data
- **Identification of protected information is the biggest issue**
  - Multiple sources of guidance provide pieces of identification, but not complete (ITAR/EAR -> Export Category, SCG -> CTI (partial) / OPSEC / PROCURE, Proprietary - > PROPIN)
- **Need a common venue for providing guidance to sanitize CUI**
  - Risk based approach applied to all programs would be preferred
  - For program specific information, the SCG is an option, but not included on all programs
  - Contract currently provides marking/distro guidance in many different places that should be consolidated
  - Program specific checklists would be an option to drive programs to consider nuances associated with their systems
- **Clarify the differences between FCI, CUI, and Publicly Releasable**
  - 3 options for data
    - Marked publicly releasable
    - Unmarked FCI
    - Marked CUI
  - Need policy that clarifies this direction

If interested in supporting CUI Sanitization Project, please contact cory.l.ocker@rtx.com

FAR Cyber Workforce Proposed Rule – Comments due 4 March

- Summary – adds Cyber Workforce requirements across the federal government expanding DFARS-like guidance
- Comments to be submitted from the NDIA SSE Committee
- Comments received:
  - "Information technology support services and cybersecurity support services" is unclear. Does that include standalone products delivered to the government through acquisition channels and the product cybersecurity support along with it?

https://www.federalregister.gov/documents/2025/01/03/2024-30504/federal-acquisition-regulation-strengthening-americas-cybersecurity-workforce

America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search

Topics | Spotlight | Resources & Tools | News & Events | Careers | About

Home / News & Events / Cybersecurity Advisories / Alert / CISA and FBI Release Updated Guidance on Product Security Bad Practices

ALERT

CISA and FBI Release Updated Guidance on Product Security Bad Practices

Release Date: January 17, 2025

RELATED TOPICS: CYBERSECURITY BEST PRACTICES, CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

In partnership with the Federal Bureau of Investigation (FBI), CISA released an update to joint guidance Product Security Bad Practices in furtherance of CISA's Secure by Design initiative. This updated guidance incorporates public comments CISA received in response to a Request for Information, adding additional bad practices, context regarding memory-safe languages, clarifying timelines for patching Known Exploited Vulnerabilities (KEVs), and other recommendations.

While this voluntary guidance is intended for software manufacturers who develop software products and services in support of critical infrastructure, all software manufacturers are strongly encouraged to avoid these product security bad practices.

CISA and FBI urge software manufacturers to reduce customer risk by prioritizing security throughout the product development process. For more information and resources, visit CISA's Secure by Design webpage or learn how to take CISA's Secure by Design Pledge.

https://www.cisa.gov/news-events/alerts/2025/01/17/cisa-and-fbi-release-updated-guidance-product-security-bad-practices

OSD Research and Engineering (R&E) Test Resource Management Center (TRMC) Cyber Test Technology (CTT) Model Based Systems Engineering (MBSE) Hackathon

- **Builds on the OSD R&E DTE&A Hackathon 2**
- **Objectives:**
  - Expand the communities' knowledge of and capabilities in digital engineering for Systems Under Test (SUT) and Test & Evaluation (T&E)
  - Inform and advance Measure & Share (Me&S) ontologies and tools.
- **Goals:**
  - Enrich System Under Test (SUT) representative tools for SUT brought forward by the community.
  - Enrich test tools brought forward introduced by the community.
  - Enrich test processes.
  - Enrich Expand SUTs' project knowledge related to SUTs.
- **Dates: 17-19 March**
- **Location: McLean, VA**
- **Registration Link: https://na.eventscloud.com/832061**

Upcoming Events

- Call for recommended briefings at future meetings
  - Please send to Cory
- Secure Software and Supply Chain Forum, 13-14 May, Mclean, VA
  - Registration opens in March. https://csrc.nist.gov/projects/cyber-supply-chain-risk-management/ssca
- NDIA Cross-Division DMM Integration and Facilitation Working Group, 2 April, Lockheed Martin, Crystal City
- CRWS/SwA CoP Event, June 2025
- NDIA Systems and Mission Engineering Conference – 27-30 October
  - Theme: DoD Mission-Ready: Digital Transformation Across the Systems' Lifecycle
  - Grand Hyatt, Tampa, FL

Updates

2023-002	1, 39, 52	Supply Chain Software Security No Update	Implements section 4(n) of Executive Order 14028, which requires suppliers of software available for purchase by agencies to comply with, and attest to complying with, applicable secure software development requirements.	05/30/2024 OMB identified draft proposed FAR rule issues. OFPP, FAR and DAR staff resolving issues.
2021-017	12, 2, 39, 4, 52	Cyber Threat and Incident Reporting and Information Sharing 3-month delay	Implements sections 2(b)-(c), 2(g)(i), 8(b) of Executive Order 14028, Improving the Nation's Cybersecurity, relating to sharing of information about cyber threats and incident information and reporting cyber incidents	02/28/2024 DARC Director tasked FAR Acquisition Technology Team to review public comments, draft final FAR rule. Report due 04/17/2024. Report due date extended to 04/02/2025.
2019-014	12, 2, 39, 52	(EO) Strengthening America's Cybersecurity Workforce Proposed Rule Published	Implements Executive Order 13870 of May 2, 2019, America's Cybersecurity Workforce, which directs agencies to incorporate the NICE Framework lexicon, taxonomy and reporting requirements into contracts for information technology and cybersecurity services.	01/03/2025 Published proposed FAR rule in Federal Register (90 FR 297). Public comment period ends 03/04/2025.
2017-016	11, 12, 2.1, 27, 35, 4, 52, 7	Controlled Unclassified Information Proposed Rule Published	Implements the National Archives and Records Administration (NARA) Controlled Unclassified information (CUI) program of E.O. 13556, which provides implementing regulations to address agency policies for designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI.	01/15/2025 Published proposed FAR rule in Federal Register (90 FR 4278). Public comment period ends 03/17/2025.

4/15: Cross NDIA Division Collaboration

- **Purpose:**
  - Facilitate an open, collaborative discussion, extending across the NDIA divisions, to discuss and advance the Digital Materiel Management (DMM)-like objective for industry and our government customers.
  - Discuss with DMM-leadership from the USAF Digital Transformation Office (DTO) and the other Services to learn more about the Digital Transformation (DTr) efforts and to share our activities that align with their initiatives
- **Objective:**
  - NDIA divisions using our already established division conferences, workshops, and publications may provide insight to the DoD on how impactful our support/development of DMM-like concept of operations can be to their activities.
  - Bring NDIA divisions into a space where we can actively discuss and align with the DMM/DTr efforts, in a collaborative, and possibly integrated fashion.
  - Share division objectives/initiatives with traceability to stakeholders' objectives
  - Government stakeholders to share their primary needs and provide feedback
- **Estimated number of attendees:** up to 80
- **When:** April 15, 2025
- **Location:** Lockheed Martin, Crystal City
- **Cost:** TBD

4/15: Agenda (proposed)

- Opening
- Stakeholders share priorities on Digital Transformation (proposed)
  - General Richardson (USAF, Materiel Command) – opening (will look into)
  - Panel: Kristen Baldwin (USAF), Jennifer Swanson (Army), Brett Seidle (Navy), Space Force (NAME), Chris Collins, Elmer Roman
- Break
- Division Introduction for our Stakeholders
  - Intro slide on how the divisions aligns with Digital Transformation efforts
  - Potential connections between the divisions' initiatives
- Lunch
- Breakout Sessions: Shared Digital Challenges
  - Topics: Infrastructure and Environment, Standards/Ontologies/Style Guides, Policy and Enforcement, Integration of Acquisition Functions, Technical Enablers
  - Current NDIA Division efforts in play, What does industry need from government (such RFP concerns), What does government need from industry, Recommended Next Step following this workshop
  - Scribe/facilitator per table
  - Results will be documented and shared with the community
- Break
- Breakout session read out
- Feedback from Around the Room

Systems Security Engineering Committee

Mission / Purpose

- **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.
- **Leadership**:
  - Cory Ocker, RTX Corporation
  - Bradley Lanford, OSD(R&E), STPP

Stakeholders / Sponsors / Collaborators

- **Sponsor**: OUSD R&E Science & Technology Program Protection, AF CROWS
- **Stakeholders**: Systems Security Engineers
- **Collaborators**: NIST, CITAG
- **Membership**: 300+ members receiving information. Meetings typically include 40-60 participants depending on the speaker. Core of 10 that volunteer to lead / support projects.
- **Business Rhythm**: Bi-monthly meetings, events as required. Participation in various SSE related association activities throughout the year (e.g. Software & Supply Chain Assurance (SSCA) Forum, OSD System Security Engineering Forum (previously Cyber Resilient Weapon System (CRWS Workshop))

2024 Accomplishments

- Met 6 times in 2024 with 6 different USG briefers
- Feedback provided on several proposed regulations
- Feedback provided on SSE Work Role Definition
- 9 joint sessions during SME Conference
- 8 dedicated sessions during SME Conference

2025 Plans / Events / Milestones

- **OSD Systems Security Engineering Forum:** Provide industry perspective on secure cyber resilient engineering initiatives and software assurance community of practice activities
- **Publish CUI Sanitization Guidance:** Aligns with deployment of CMMC and CUI FAR Clause implementation to limit industry impact, increase suppliers, and ensure resources are focused on correct data to protect
- **DMEA Trusted Supplier Steering Group:** Collaborate with TSSG to identify opportunities to apply lessons learned to microelectronics assurance policies and procedures
- **Hardware Assurance RFP Strategy Definition Workshop:** concept that sprung from SME conference to leverage RFI/RFP process to determine hardware protection needs and ensure consistency across bidders
- **SSE Workforce Development:** continue shaping NICE Framework and SSE Competency; ensure proper alignment of regulations to SSE acquisition workforce

Backup

NDIA Cross Division DMM Meeting

- **Meeting Objective:** To facilitate an open, collaborative initiative, extending across the NDIA divisions, to advance the USAF Digital Materiel Management (DMM) objectives and build an NDIA cross division roadmap
- **When**: April 2, 2025
- **Location**: TBD. NoVA/DC
- **Who**: US Citizens only
  - NDIA Division leads, Committee leads
  - Stakeholders
  - Specific government participants
- **Agenda**:
  - TBC
- **Homework**: Complete the stakeholder traceability matrix.

How do we operate?

Annual NDIA Systems Engineering Division Planning meeting(s) lays out plans and priorities for the 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.

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.**

Email cory.l.ocker@rtx.com to be added to the committee email list.

Mission / Purpose

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.

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.***

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.***

Reasons to Join

Reasons to join the SSE Committee

- Shape Policy – committee reviews policies/standards that have major impacts on acquisition and provides both detailed comments as well as high level report; allows industry nonrepudiation for candid feedback
- Be the first to know – many documents that eventually become policy/guidance start in the committee; receive draft documents to provide early feedback
- Networking - Committee includes experts from across industry, government, FFRDCs, and Academia
- Continuous Learning Credits – many certifications require CLEs that can be satisfied by committee engagement