USD(R&E)

ANSI / DoD Microelectronics Standards Workshop

Group Exercise

Christine Rink
OUSD(R&E) / CT , Microelectronics

Stephanie Lin
Defense Microelectronics Cross Functional Team

ANSI Workshop
26 Oct 2022

Introduction

SUPPLY CHAIN TRACEABILITY

- Practices focus on the ability to identify and authenticate the provenance of devices, source materials, and/or microelectronics services. May include secure design and/or procurement management methods to improve microelectronics supply chain illumination and advance non-repudiation in the microelectronics supply chain.

Breakout Staff

- Facilitator: Kirsten M. Koepsel JD LLM, Project Engineer, Aerocyonics, Inc.
- Scribe: Jim McCabe, Senior Director, Standards Facilitation, ANSI
- Remote Participant Interface: Elizabeth Gonzalez, Standards Manager, ANSI

Supply Chain Practice Area

Breakout Staff

- Thank you to our volunteers!

Overview

OVERVIEW

Overview

- FY20 NDAA Section 224 requires that standards evaluate the reliability of the supply chain.
- FY20 NDAA Section 224 requires that "other matters germane to supply chain and operational security" be considered in the evaluation of suppliers for DoD microelectronics.

Candidate Risks

- Incomplete knowledge base of suppliers compromises optimized management of supply chain planning, which may have high-level program plans
- If procured devices are not authentic, or otherwise include vulnerabilities, then system performance or integrity may be adversely impacted.
  - Risks to authentic custody and modifications

Workshop Objectives

OBJECTIVE #1

Identify the appropriate set of considerations for each supply chain practice area

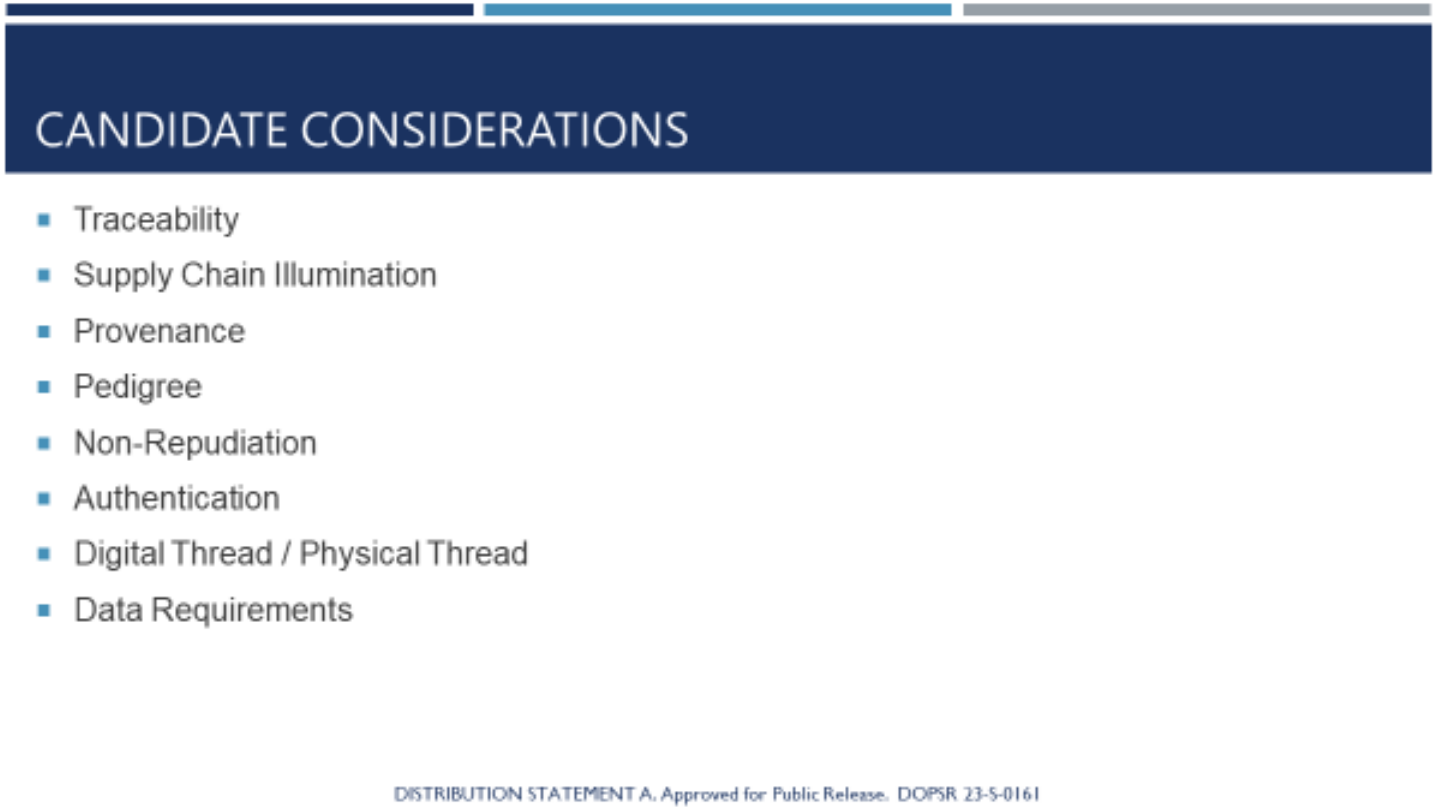
OBJECTIVE #2

Develop baseline criteria for secure microelectronics to be used in DoD systems and national critical infrastructure

OBJECTIVE #3

Identify appropriate references

Candidate Considerations



8 candidate considerations pre-identified for discussion

- Is the list complete?
- Are all items appropriate?

OBJECTIVE #1: Identify Considerations

Each supply chain area (breakout) will receive candidate considerations

- Considerations were informed by ANSI Workshop #1 proceedings
- Definitions language leverages publicly available standards (e.g., NIST) when possible, or is identified as a strawman
- Should be broadly applicable, and not specific to DoD

Baseline Assumption – Do Not Reinvent the Wheel

- Some supply chain practice areas have significant overlap with existing standards (e.g., Procurement Management, Information & IP Protection)
- Sec 224 activities should seek to leverage existing efforts and add value by
  - Specifically addressing considerations that address Sec 224 and/or assured microelectronics and/or
  - Informing DoD's response to Congress (e.g., what is untenable, missing, etc.?)

Workshop only: assume application of NIST SP 800-161r1 as notional baseline

- NIST publications are available free of charge and can be accessed by all workshop participants
- NIST SP 800-161 has already been evaluated and mapped by other USG entities
- Relevant links
  - NIST SP 800-161 Rev. 1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
  - NASA SEWP Standards Crosswalk: ISO 20243 & NIST 800-161
  - DHS CISA ICT SCRM Task Force: CISA Vendor SCRM template
  - DHS CISA ICT SCRM Task Force: ICT SCRM TF Report on Mitigating ICT Supply Chain Risks with Qualified Bidder and Manufacturer Lists

Non-Repudiation
Example Consideration

- Non-Repudiation: Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information. (NIST SP 800-60)

- What about NIST SP 800-161r1 (or NASA SEWP, DHS CISA)?
  - Non-Repudiation Controls: AU-10 (non-repudiation, level 3), IA-4 (Identifier management, levels 2,3), IA-5 (authentication management, level 3)
  - Authentication Controls: Family: Identification and Authentication, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9
  - Does it meet the needs of Sec 224 in this area?
  - If not, what needs to happen to leverage it? Or, are there viable alternatives?

Workshop Objectives

OBJECTIVE #1

Identify the appropriate set of considerations for each supply chain practice area

OBJECTIVE #2

Develop baseline criteria for secure microelectronics to be used in DoD systems and national critical infrastructure

OBJECTIVE #3

Identify appropriate references

OBJECTIVE #2: Develop Criteria

Candidate LoA descriptions for use in this workshop focus on:

- Is the resultant device considered secure microelectronics or not?
- Is additional risk management needed for use in DoD or national critical infrastructure? (no need to define what those mitigations are yet)

Leverage existing value judgements when practicable

Preferred outcome: LoA B criteria defined

LoA: A	Devices that meet or exceed these criteria are considered secure microelectronics and are appropriate for use in DoD or national critical infrastructure systems. Criteria represent a preferred or best-in-class microelectronics security solution. (e.g., highest level of assurance)
LoA: B	Devices that meet these criteria are considered secure microelectronics and may be appropriate for use in DoD or national critical infrastructure systems. Additional risk management may be necessary if used for critical functions. (e.g., baseline level of assurance for national critical infrastructure)
LoA: C	Devices in this category are not considered secure microelectronics. Programs should actively manage the risk associated with these devices if they are used in national critical infrastructure.
LoA: D	Devices in this category are not considered secure microelectronics, and represent a risk to DoD systems. Devices should not be used in DoD systems or national critical infrastructure in the absence of a technically rigorous waiver process that includes decision making at a higher level than the program.

Non-Repudiation
Example

LoA: A	· Authentication, non-repudiation integrated throughout the supply chain (future state)
LoA: B	· Traceability: · Supply Chain Illumination: · Provenance: · Pedigree: · Non-Repudiation: · Authentication: · Digital / Physical Threads: · Data Requirements:
LoA: C	
LoA: D	

Can we identify what is acceptable for baseline secure microelectronics with respect to non-repudiation?

- Is the list complete?
- Are all items appropriate?

If not, can we write what

- our most-preferred, most-secure solution looks like?
- Is unacceptably risky?

Workshop Objectives

OBJECTIVE #1

Identify the appropriate set of considerations for each supply chain practice area

OBJECTIVE #2

Develop baseline criteria for secure microelectronics to be used in DoD systems and national critical infrastructure

OBJECTIVE #3

Identify appropriate references

Documentation
Example

OBJECTIVE #3

REGULATION, POLICY, OTHER
REFERENCES

Regulation

-

Policy

- DoDD O-5240.24, *Acquisition (RDA)*

Other

-

STANDARDS & BEST PRACTICES
REFERENCES

- NIST SP 800-160 v1: Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
- IPC-1782A, Standard for Manufacturing and Supply Chain Traceability of Electronic Products
- IPC-1782, Standard for Manufacturing and Supply Chain Traceability of Electronic Products
- IPC 1791A, Trusted Electronic Designer, Fabricator and Assembler Requirements
- ISO/IEC 20243-1:2018: Information technology — Open Trusted Technology Provider Standard (O-TTPS) — Mitigating maliciously tainted and counterfeit products — Part 1: Requirements and recommendations
- ISO/IEC 20243-2:2018: Information technology — Open Trusted Technology Provider Standard (O-TTPS) — Mitigating maliciously tainted and counterfeit products — Part 2: Assessment procedures for O-TTPS and ISO/IEC 20243-1:218
- SAE AS 5553A Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation and Disposition
- SAE AS 6081Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation and Disposition - Distributors

DISTRIBUTION STATEMENT A. Approved for Public Release. DOPSR 23-S-0161

List reflect Workshop #1, industry identification

- Is the list complete?
- Are all items appropriate?

BACKUP

Slides from ANSI Workshop #1

Approach: Risks, Vulnerabilities, Threats

The microelectronics standards approach utilizes CIA triad

- Commonly used in networking / information security

Confidentiality (C)
Preserving authorized restrictions on information and/or intellectual property access and disclosure

1) **Theft of Design**
2) **Theft of Device**
3) **Theft of Runtime Data**

Loss of confidentiality results in the unauthorized disclosure of information and/or intellectual property, to include the physical element

Integrity (I)
Guarding against malicious information/intellectual property addition, modification, and/or deletion and ensures authenticity

1) **Modification of Design**
2) **Modification of Device**
3) **Modification of Runtime Data**

Loss of integrity results in the unauthorized addition, modification, or removal of information, IP, or physical element

Availability (A)
Ensuring timely and reliable access to and use of suppliers and sources

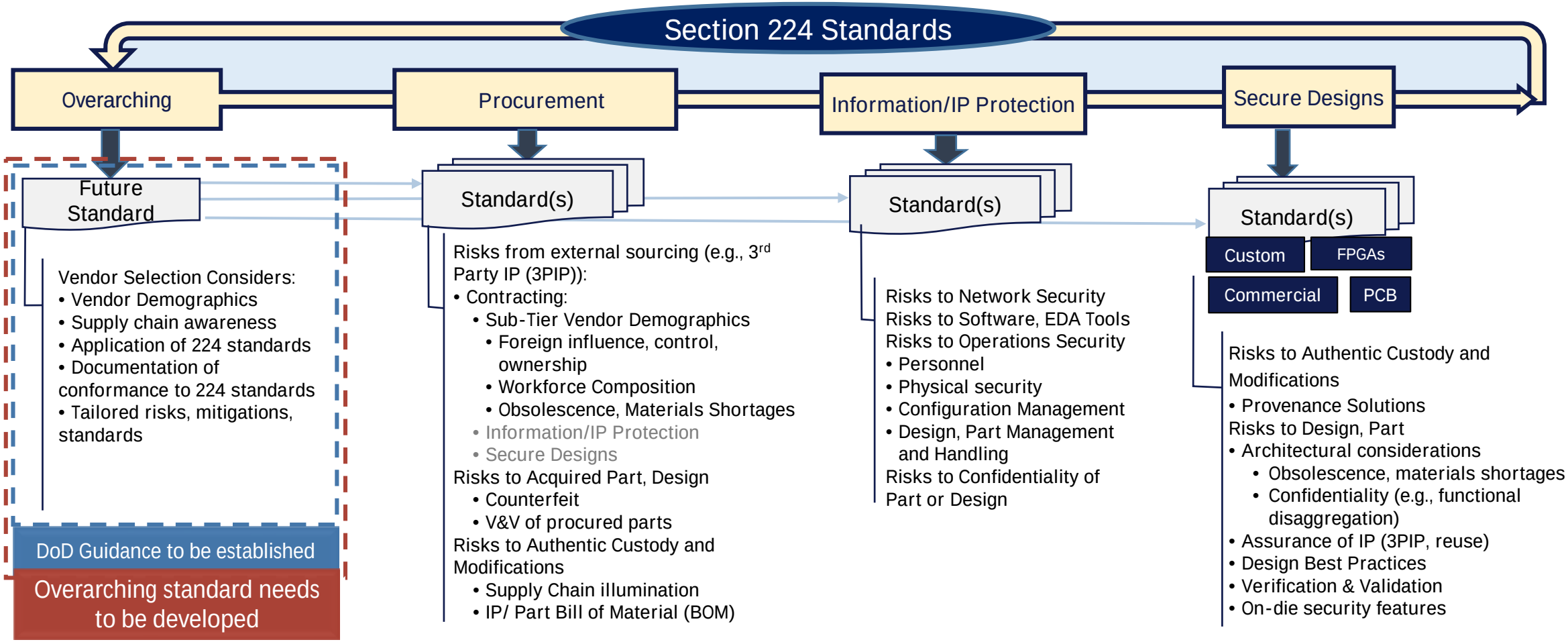
1) **Accessibility of Sources**

Loss of availability results in the disruption of access to or use of products or services necessary to the supply chain

Workshop Objective – Evaluate and Improve Standards Approach

Approach: Adopting and Establishing Standards

3PIP: Third Party Intellectual Property EDA: Electronic Design Automation V&V: Verification and Validation PCB: Printed Circuit Board



Workshop Objective – Recommend and organize standards