INFORMATION & IP PROTECTION

FACILITATOR: ROGER SMITH

DISTRIBUTION STATEMENT A. Approved for Public Release. DOPSR 23-S-0159

INFORMATION & IP PROTECTION

- Risks attributed to the confidentiality of intellectual property and information not intended for public dissemination. May overlap with other supply chain practice areas. Processes are focused on mitigations associated with networks and personnel.

Breakout Staff

- Facilitator: Roger R. Smith, Defense Microelectronics Cross Functional Team – Navy Lead, Printed Circuit Board Executive Agent, U.S. Department of Defense
- Scribe: Anne Caldas, Senior Director, Procedures and Standards Administration, ANSI
- Remote Participant Interface: Stephanie Carroll, Sr. Meetings and Events Manager

OVERVIEW

Overview

- 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 “to protect the United States from intellectual property theft”.

Candidate Risks

- If procured devices are not authentic or otherwise include vulnerabilities, then system performance or integrity may be adversely impacted.
  - Risks to Network Security
  - Risks to Software, EDA tools
  - Risks to Confidentiality of Part or Design
- If confidentiality is not maintained in procurement, then DoD systems may be more vulnerable to supply chain and other types of attacks.

CANDIDATE CONSIDERATIONS

- Information Protection / Confidentiality of Data
  - Device, Design Data
  - Acquirer Data
- Design for Data Security
- Data Requirements
- Chain of Custody

INFORMATION PROTECTION / CONFIDENTIALITY OF DATA

CANDIDATE CONSIDERATION

Confidentiality of device, design data

- ***DoD*** programs should not presume confidentiality of commercial device capabilities or design

Confidentiality of Acquirer Data

- What are appropriate protections for acquirer data?
  - Network & IT
  - Vendor demographics
- What should acquirers consider when sharing data with suppliers?

Criteria

- What should be the minimal criteria for secure microelectronics used in DoD/NCI systems?

DESIGN FOR DATA SECURITY

CANDIDATE CONSIDERATION

Consideration

- What does the acquirer need to know about on-die data protection to assess the security risk of the microelectronics device in the context of their system?
- Should there be baseline requirements for protection / handling of on-die data? Which classes of devices? How to evaluate existing secure processing capabilities? Etc.

Criteria

- What should be the minimal criteria for secure microelectronics used in DoD/NCI systems?

DATA REQUIREMENTS

CANDIDATE CONSIDERATION

Consideration

- What data is required?
- Is the data available?
  - Data exists and can be delivered
  - Data does not exist but can be generated
  - Data cannot be made available
- When is the data available?
- Can the data delivery be standardized?

Criteria

- What should be the minimal criteria for secure microelectronics used in DoD/NCI systems?

CHAIN OF CUSTODY

CANDIDATE CONSIDERATION

Consideration

- Are the considerations in Supply Chain Traceability adequate?
  - Traceability
  - Supply Chain Illumination
  - Provenance, Pedigree
  - Non-Repudiation
  - Authentication
  - Digital Thread / Physical Thread
- If not, what needs to be added as a consideration for information & IP protection?
  - Is it applicable to COTS for DoD? Or does it need to be considered for DoD custom developments only?

Criteria

- What should be the minimal criteria for secure microelectronics used in DoD/NCI systems?

INFORMATION & IP PROTECTION

CANDIDATE CRITERIA

Leverage existing value judgements when practicable (don't reinvent the wheel)

LoA: A	• Information Protection: Acquirer data is protected in accordance with NIST SP 800-172 or DCSA certification • Design for Data Security: • Data Availability: • Chain of Custody:
LoA: B	• Information Protection: • Design for Data Security: • Data Availability: • Chain of Custody:
LoA: C	
LoA: D	

REGULATION, POLICY, OTHER

REFERENCES

Regulation

-

Policy

-

Other

- Accellera Systems Initiative: IP Security Assurance Standard Whitepaper

STANDARDS & BEST PRACTICES

REFERENCES

- 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
- NIST SP 800-160 v1: Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
- NIST SP 800-161 Rev. 1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
- IEEE 1735-2014: Recommended Practice for Encryption and Management of Electronic Design Intellectual Property (IP)

Design for Data Security

- ISO 26262-1:2011: Road vehicles — Functional safety — Part 1: Vocabulary
- NIST FIPS 140-3: Security Requirements for Cryptographic Modules
- NIST FIPS 200: Minimum Security Requirements for Federal Information and Information Systems
- RTCA DO-254 Design Assurance Guidance for Airborne Electronic Hardware