PROCUREMENT MANAGEMENT

FACILITATOR: LORI GORDON

DISTRIBUTION STATEMENT A. Approved for Public Release. DOPSR: 23-S-0163

PROCUREMENT MANAGEMENT

- The process and contractual considerations required for evaluating and defining engagements with external entities for procurements, including the risks/mitigations identified from the other supply chain practice areas. Procurement processes are focused on mitigating risks associated with sourcing IP and parts (e.g., counterfeit, DMSMS), and should include considerations for vendor demographics as identified in FY20 NDAA Section 224 (e.g., company ownership, location, workforce composition).

Breakout Staff

- Facilitator: Lori Gordon, Space Enterprise Integration Initiatives Leader, Office of the Corporate Chief Engineer, The Aerospace Corporation
- Scribe: Will Helfrich, Senior Consultant, Booz Allen Hamilton
- Remote Participant Interface: Sarah Katz, Standards Facilitation Support, ANSI

OVERVIEW

Overview

- FY20 NDAA Section 224 requires that standards evaluate the reliability of the supply chain

Candidate Risks

- Sourcing management in supplier planning and appropriate contractual extension of supply chain security measures
- If procured devices are not authentic, or otherwise include vulnerabilities, then system performance or integrity may be adversely impacted.
  - Risks to Acquired Device, Design (e.g., counterfeit)

COUNTERFEIT PREVENTION

CANDIDATE CONSIDERATION

Consideration

- Counterfeit: An unauthorized copy or substitute that has been identified, marked, and/or altered by a source other than the item's legally authorized source and has been misrepresented to be an authorized item of the legally authorized source. (NIST SP 800-53)
- Principle: Do not acquire counterfeit devices or designs
- ***DoD*** leverages regulations (e.g., 48 CFR § 252.246-7007) and policy (e.g., DoDI 4140.67)
- What about NIST SP 800-161r1 (or NASAQ SEWP, DHS CISA)?
  - 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?

Criteria

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

OBSOLESCENCE & MATERIALS SHORTAGE

CANDIDATE CONSIDERATION

Consideration

- Obsolescence: manufacturer’s declaration of part obsolescence and no valid stock available *(strawman)*
- ***DoD*** leverages policy (e.g., DoDI 4245.15)
- What about NIST SP 800-161r1 (or NASAQ SEWP, DHS CISA)?
  - 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?

Criteria

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

CONTRACTING CONSIDERATIONS

CANDIDATE CONSIDERATION

Consideration

- Definition: Flow down of requirements for secure microelectronics, including other supply chain practices *(strawman)*
- What challenges are anticipated in requirements flow down?
  - How would industry prefer to address the issue

Criteria

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

DATA REQUIREMENTS
CANDIDATE CONSIDERATION

Consideration

- Identification of data to be included in the digital thread is covered in the Supply Chain Traceability Section
- Identification of design data should be covered in the Secure Design Section
- Identification of data in support of Information & IP Protection
- 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?

RELIABILITY OF THE SUPPLY CHAIN

CANDIDATE CONSIDERATION

Consideration

- Definition: the degree to which a supply chain yields consistent performance *(strawman)*
- What about NIST SP 800-161r1 (or NASAQ SEWP, DHS CISA)?
  - 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?

Criteria

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

VENDOR DEMOGRAPHICS

CANDIDATE CRITERIA

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

LoA: A	
LoA: B	• Counterfeit Prevention: • Obsolescence and Material Shortages: • Contracting Considerations: • Access During Manufacturing: • Reliability of the Supply Chain:
LoA: C	
LoA: D	

REGULATION, POLICY, OTHER

REFERENCES

Regulation

- 48 CFR § 252.239-7018 (DFARS/ Supply Chain Risk)
- 48 CFR § 252.246-7007,8 (DFARS / Counterfeit, Sources of Electronics Parts)
- FAR Case 2019-009 (FY19 NDAA Section 889), Prohibition on Contracting With Entities Using Certain Telecommunications and Video Surveillance Services or Equipment
- FOCI mitigation authorities for exclusion (3252, 10 USC) (DoD)

Policy

- DoDI 4140.01, *DoD Supply Chain Materiel Management Policy*
- DoDI 4140.67, *Counterfeit Prevention Policy*
- DoDI 4245.15, *Diminishing Manufacturing Sources and Material Shortages Management*

Other

- ***DoD*** COTS Assembly Checklist
- National Counterintelligence and Security Center – Supply Chain Risk to Semiconductors

DISTRIBUTION STATEMENT A. Approved for Public Release. DOPSR: 23-S-0163

STANDARDS & BEST PRACTICES

REFERENCES

- NIST SP 800-161 Rev. 1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
- IEC 62402, *Obsolescence Management* (adopted by DoD)
- JESD243 Fraudulent / Counterfeit Electronic Parts: Non-Proliferation for Manufacturers / JEDEC JC-13
- AS7171, AS6171A (with 11 published tear sheets and 11 in development) / SAE G-19A
- AS6496 Authorized Distributor Counterfeit Mitigation / SAE G-19D
- AS6081 Counterfeit Electronic Parts Avoidance / SAE G-19D
  - AS6301 Compliance Standard or Guide / SAE G-19C
- AS5553C Counterfeit Electronic Parts; Avoidance, Mitigation and Disposition / SAE G-19CI
- AS6462C AS55553B Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition Verification Criteria Includes Audit Checklist / SAE G-19C
- ARP6328, Guideline for Development of Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition Systems / SAE G-19CI
- AS6174A, Counterfeit Materiel; Assuring Acquisition of Authentic and Conforming Materiel / SAE G-21
  - AS6174/1, Compliance Standard or Guide (Includes Audit Checklist) / SAE G-21
- *In Development: AIR6860, Use of SAE AS5553 for Implementation of U.S. DFARS 252.246-7007 & 252.246-7008 / SAE G-19CI*

STANDARDS & BEST PRACTICES

REFERENCES

- 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
- NASA MSFC STD-3619, MSFC Counterfeit Electrical, Electronic, and Electromechanical Parts Avoidance, Detection, Mitigation, and Disposition Requirements for Space Flight and Critical Ground Support Hardware
- NASA STD-8739.10, Electrical, Electronic, and Electromechanical (EEE) Parts Assurance Standard
- SEMI T20.1-1109, Specification for Authentication of Semiconductors and Related Products
- SEMI T21-0314, Specification for Organization Identification by Digital Certificate Issued from Certificate Service Body (CSB) for Anti-Counterfeiting Traceability in Components Supply Chain
- SEMI T22-0212, Specification for Traceability by Self Authentication Service Body and Authentication Service Body
- SAE STD0016, Standard for Preparing a DMSMS Management Plan
- SAE ARP6178, Fraudulent/Counterfeit Electronic Parts; Tool for Risk Assessment of Distributors
- JEDEC JESD31F, General Requirements For Distributors Of Commercial And Military Semiconductor Devices
- JEDEC JESD243A, Counterfeit Electronic Parts: Non-proliferation For Manufacturers

DISTRIBUTION STATEMENT A. Approved for Public Release. DOPSR: 23-S-0163