SUPPLY CHAIN TRACEABILITY

FACILITATOR: KIRSTEN KOEPSEL

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

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

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

CANDIDATE CONSIDERATIONS

- Traceability
- Supply Chain Illumination
- Provenance
- Pedigree
- Non-Repudiation
- Authentication
- Digital Thread / Physical Thread
- Data Requirements

TRACEABILITY
CANDIDATE CONSIDERATION

Considerations

- Definition: the ability to verify a relationship between two of more procurement points in the supply chain *(strawman)*
- Definition (traceability analysis): The analysis of the relationships between two or more products of the development process conducted to determine that objectives have been met or that the effort represented by the products is completed. Note: A requirements traceability analysis demonstrates that all system security requirements have been traced to and are justified by at least one stakeholder security requirement, and that each stakeholder security requirement is satisfied by at least one system security requirement. (NIST SP 800-160 Vol 1)
- What about NIST SP 800-161r1 (or NASA 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?

SUPPLY CHAIN ILLUMINATION

CANDIDATE CONSIDERATION

Considerations

- Definition: Continual visibility throughout the supply chain that provides an understanding of the tiers of a supply chain, a supply chain map, and vetting of suppliers against a defined set of supply chain criteria to identify and defend against threats *(strawman)*
- What about NIST SP 800-161r1 (or NASA 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?

PROVENANCE, PEDIGREE

CANDIDATE CONSIDERATION

Considerations

- Provenance: the chronology of the origin, development, ownership, location, and changes to a system or system component and associated data. It may also include personnel and processes used to interact with or make modifications to the system, component, or associated data. (NIST SP 800-161r1)
- Pedigree: The validation of the composition and provenance of technologies, products, and services is referred to as the pedigree. For microelectronics, this includes material composition of components. For software, this includes the composition of open source and proprietary code, including the version of the component at a given point in time. Pedigrees increase the assurance that the claims suppliers assert about the internal composition and provenance of the products, services, and technologies they provide are valid. (NIST SP 800-161r1)
- What about NIST SP 800-161r1 (or NASA SEWP, DHS CISA)?
  - Provenance Controls: SR-4 (provenance, levels 2,3) (needs tailoring to ME)
  - 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?

NON-REPUDIATION, AUTHENTICATION

CANDIDATE CONSIDERATION

Considerations

- 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)
- Authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system. (NIST SP 800-171)
- 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?

Criteria

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

DIGITAL THREAD / PHYSICAL THREAD

CANDIDATE CONSIDERATION

Considerations

- Identified as a clear gap at ANSI Workshop #1
- Definition: a communication framework that connects traditionally siloed elements in manufacturing processes and provides an integrated view of an asset throughout the manufacturing lifecycle. *(strawman, techtarget.com)*
  - What should be included in the digital thread of assurance data?

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?

SUPPLY CHAIN TRACEABILITY

CANDIDATE CRITERIA

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

LoA: A	• Authentication, non-repudiation integrated throughout the supply chain (future state) • Full visibility into supply chain or established pedigree for xxxx
LoA: B	• Traceability: • Supply Chain Illumination: • Provenance: • Pedigree: • Non-Repudiation: • Authentication: • Digital / Physical Threads: • Data Requirements:
LoA: C	• No visibility into supply chain (distributor only)
LoA: D	

REGULATION, POLICY, OTHER

REFERENCES

Regulation

-

Policy

- DoDD O-5240.24, *Counterintelligence (CI) Activities Supporting Research, Development, and 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