Global Supply Chain Security for Microelectronics

Recap of 27-29 July workshop

Jim McCabe, Senior Director, Standards Facilitation, ANSI

26 – 28 October 2022 workshop

NDAA FY20 Section 224 Background

- Section 224 of the FY20 National Defense Authorization Act (NDAA) requires U.S. Department of Defense (DoD) to:
  - establish trusted supply chain and operational security standards for the purchase of microelectronics (ME) products and services
  - ensure that procurements made after January 1, 2023 meet these standards
- The standards shall not be military standards or specifications
- The standards shall systematize best practices relevant to:
  - manufacturing location
  - company ownership
  - workforce composition
  - access to manufacturing data
  - reliability of the supply chain
  - and related matters

Section 224 Background (contd.)

- The standards shall be:
  - generally applicable to the trusted supply chain and operational security needs and use cases of the United States Government (USG) and commercial industry, such that the standards could be widely adopted by government agencies, commercial industry, and U.S. allies and partners as the basis for procuring ME
- The law:
  - enables DoD to establish tiers and levels of trust and security
  - aspires to ensure that suppliers are able and incentivized to sell products commercially and to governments of allies and partners of the U.S. that are produced on the same production lines as the ME products supplied to DoD
  - speaks to the need for DoD's requirements and acquisition of ME to enable the success of a dual-use ME industry
  - specifies that the actions taken by DoD should maintain competition, innovation, and the health of the defense industrial base
  - requires broad consultation among industry and government stakeholders

July 27-29 Workshop Goals

- DoD invited ANSI, as national coordinator for the U.S. private-sector system of voluntary standardization, to convene the workshop
- DoD recognized that existing industry consensus standards can play a vital role in addressing the objectives of the section 224 requirements
- The July workshop sought to help DoD identify such standards as well as provide feedback to DoD on a proposed framework approach for how to implement the section 224 requirements
- Some 140 subject matter experts from academia, industry, various parts of the USG, standards development organizations (SDOs), and trade associations participated in the hybrid workshop
- The workshop was scoped to commercial off-the-shelf (COTS) devices, not custom devices

DoD Framework Approach

- During the workshop, DoD presented a framework which could leverage the standards identified through the RFI, and others
- A modular approach to implementation was envisioned by DoD against a high-level COTS ME lifecycle and requirements flow down concept
- DoD emphasized that the framework will include both commercial standards and best practices, as well as DoD specific requirements
- A primary workshop objective was for DoD to receive input from industry on which commercial standards are strong candidates for consideration, as well as those which are not suitable

DoD Framework Approach (contd.)

- DoD presented its strategy for protection against risks, vulnerabilities, threats, and for determining mitigations
- This was referred to as the “CIA” Triad based on three core components: confidentiality (C), integrity (I), and availability (A)
- Nonrepudiation (N) was also called out by the standards community as an important consideration, due to the distributed nature of the ME lifecycle
- These four components became a common thread throughout the workshop discussions

Panel Discussions

- 2 panels discussed the role, status, utilization, and importance of standards and conformance programs for this sector
- Panel 1 covered SDO capabilities to address ME supply chain and operational security issues with focus on work of: IPC, the Telecommunications Industry Association, the IEEE Standards Association, JEDEC, the International Electrotechnical Commission, and SAE International
- The panel noted standards activities related to components, systems, and the broader supply chain, and conformity assessment challenges and opportunities
- General consensus that existing standards can be leveraged, though no single standard meets all the needs, and conformity assessment to standards is a necessary component
- Panel 2 covered federal agency (NASA, NIST) and industry (Intel, GlobalFoundries, Raytheon Technologies) perspectives
- Topics included supply chain considerations, why standards are important, the need for a USG presence in standards development committees, and the DoD's approach to standards development and implementation

Breakout Groups

- Workshop attendees were separated into 3 groups to:
  - discuss existing standards being leveraged by the commercial sector today
  - make recommendations for candidate standards that the DoD should consider when developing their requirements for COTS ME products and services
- The breakouts focused on three supply chain practice areas:
  - procurement management
  - information and intellectual property (IP) protection
  - secure design

Procurement Management Group

- *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).*
- Group spent considerable time discussing considerations related to the vendor demographics outlined in section 224
- Group identified a number of existing standards and government resources that could be looked to for guidance on vetting vendors
- As was the case with the other groups, it was acknowledged that there is no general standard that governs all of the supply chain; rather, there are many standards and other guidance materials across SDOs and the USG that can be leveraged
- Appropriate messaging by DoD in communicating its requirements will improve the chances for broad adoption

Information and IP Protection Group

- *Risks attributed to the confidentiality of IP and information not intended for public dissemination. Processes are focused on mitigations associated with networks and personnel.*
- Over 20 standards were identified as candidate standards, each with its own scope and applicability
- Attendees agreed that a modular approach made sense
- The issues cannot be resolved by one all-encompassing standard
- A map of standards to address the various issues across the supply chain is needed
- The group cautioned that the imposition of overly prescriptive requirements relative to COTS ME will not be well received
- Further, even as DoD strives to meet Congress's mandate and timeline, it must be acknowledged that DoD does not control the timelines for the development of commercial standards
- Standards development takes time, and achieving consensus is not a short-term effort

Secure Design Group

- *Design practices to improve assurance (e.g., verification and validation), manage risk when the part is outside vendor or user control, and address supply chain volatility (e.g., open architecture or modularity).*
- Group discussed various models to evaluate existing and needed commercial standards to support secure design
- The development of a matrix, or map, of standards related to threats and mitigations, so that gaps could be identified, was seen as beneficial
- Discussion included:
  - definitions around design levels (traceability, provenance, risks, quality, validation)
  - data (what is collected, how it is used, what artifacts are appropriate)
  - near-term rather than long-term goals
- A DoD pilot program could support incremental solutions development

Common Themes

Set Realistic Timelines

- Standards development for even a single sector takes a significant amount of time and resources
- COTS ME products impact many sectors
- Developing a solution that meets the needs of broader industry and the DoD today will take years
- A solution that will meet the evolving needs of both the private and public sectors over time, will require ongoing maintenance and continued investments

Common Themes (contd.)

- **Multiple Standards Will Apply**
  - No single standard will meet the needs of the industry and government alike
  - Not only are there company specific processes and products, there are also sector specific applications and compliance requirements
  - Organizations today, across all sectors, rely on portions of various industry standards, then build off those requirements to meet their internal and external customers' needs
  - USG should try implementing what seems to work right now
  - We should not reinvent the wheel

Common Themes (contd.)

- **Set Baseline Requirements to Drive Conformity with the Standards**
  - In order to establish and maintain a trusted supply chain and operational security, conformity assessment to industry standards must be a component
  - Whether this is a 3rd party validation and verification program, or done through contractual obligation (vendor-customer), or self-attestation, it is important that compliance be quantifiable
  - Significant resources and infrastructure have been invested to establish and maintain the standards and conformance programs in place today
  - To get industry buy-in, any new programs should set baseline requirements and not unnecessarily increase the conformity assessment burden for the manufacturing sector

ANSI Staff Contacts

Jim McCabe
Senior Director, Standards Facilitation
1-212-642-8921; jmccabe@ansi.org

www.ansi.org

Christine D. Bernat
Associate Director, Standards Facilitation
1-212-642-8919 cbernat@ansi.org

www.ansi.org

ANSI
American National Standards Institute