Standards Briefings & Standardization Activity Request for Information (RFI) Update

Christine Bernat, Associate Director, Standards Facilitation, ANSI

DoD Microelectronics Workshop

26 October 2022

Sept. 30th & Oct. 6 Standards Briefings

Name	Organization	Topic
Michael Durkan**	Siemens Digital Industries Software	JEDEC: JEP30 PartModel Standard Presentation.
Andras Szakal* John Linford**	The Open Group	Open Trusted Technology Provider™ Standard (O-TTPS) / ISO 20243
Brian Knight	Microsoft	IETF Supply Chain Integrity, Transparency, and Trust (SCITT)
Michael Azarian**	Univ of Maryland / Center for Advanced Life Cycle Engineering (CALCE)	SAE International: AS6171 family of standards on requirements for testing for counterfeit EEE parts.
Ravi Subramaniam	IEEE	IEEE Standards
Dan DiMase**	Aerocyonics, Inc.	SAE: JA7496 Cyber-Physical Systems Security Engineering Plan (CPSSEP)
Andreas Schweiger Aharon David	Airbus Defence and Space Afuzion Inc.	SAE: JA6678 Cyber Physical Systems Security Software Assurance
Dan DiMase**	Aerocyonics, Inc.	SAE: JA6801 Cyber Physical Systems Security Hardware Assurance
Jon Boyens**	National Institute of Standards and Technology	NIST: SP 800-161rev1, C-SCRM for Systems and Organizations; 800-128, Secure Software Development Framework
Sanjay Rekhi Michael Bartock	National Institute of Standards and Technology	Hardware Security; NIST IR 8320
Mike Regan*	Telecommunication Industry Association / QuEST Forum	TIA: SCS 9001 Supply Chain Security standard

JEP30 PartModel Standard

- **Scope**
  - Data exchange requirements for all electronic parts
  - Physical, Electrical, Thermal, assembly process classification
- **Objectives**
  - Increase traceability, reliability, & quality
  - Reduce human errors of manual entries from datasheets
  - Streamline design-to-manufacturing

- Developed in coordination with Component Manufacturers, OEM's, & EDA Industry
- Used/Referenced by IPC Traceability Standards & GSA TIES
- Expanding to include:
  - Product Change Notices
  - Product Discontinuance
  - Digital Signatures

O-TTPS Standard / ISO/IEC 20243

Scope:

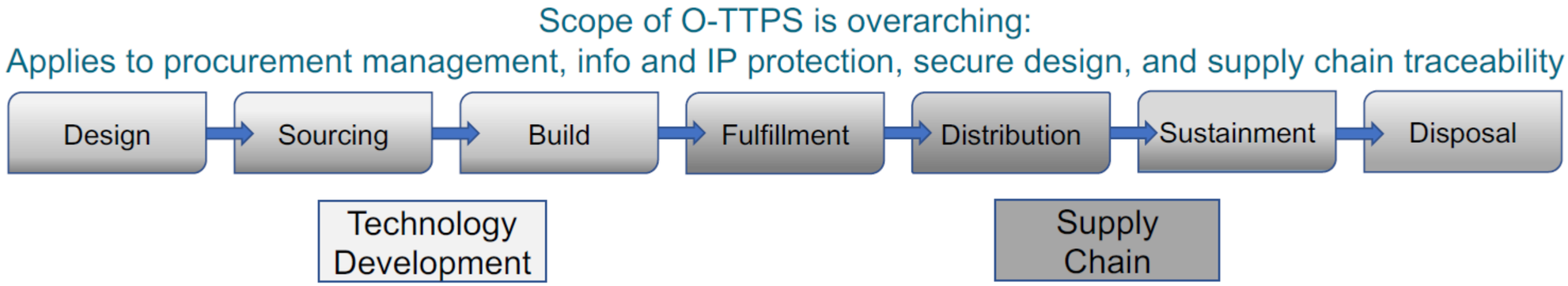
- Mitigates Threats across Product Life Cycle
- Technology Development & Supply Chain
- Process focused: Product -> Organization
- Part 1: Guidelines, requirements, & recommendations to assure against maliciously tainted & counterfeit products throughout COTS ICT product life cycle
- Part 2: Assessment procedures

O-TTPS Certification Program :

- Process based
- Applicants choose between self-assessed or 3rd party assessed tiers.
- Demonstrate conformance to the standard
- OEM's, hardware/software component suppliers; resellers, integrators and distributors

Future Plans

- Other government / market needs
- Workforce skills / experience
- Address critical infrastructure



Supply Chain Integrity, Transparency, and Trust (SCITT)

SCITT Kicked off in 2021:

Promote interoperability, simplify and automate workflow for managing compliance of goods and services across end-to-end supply chains

An Architecture for Trustworthy & Transparent Digital Supply Chains (*in development*)

- Defines scalable & flexible decentralized architecture to enable auditability & accountability of supply chains
- Outlines Security Guarantees
- Minimum adoption barriers for producers
- Ability for consumers to verify
- Flexible implementations for auditing/compliance

Countersigning COSE Envelopes in Transparency Services (*in development*)

- Concise Signing and Encryption (COSE)
- Defining a method for issuing and verifying the counter-signatures on COSE messages
- Based on an authenticated data structure

Supply Chai
Transparenc

SCITT Kicked off in 2021:

Promote interoperability, simplify and automate worl nd services across end-to-end supply chains

An Architecture for Trustworthy & Transparent Digital Supply Chains (*in development*)

- Defines scalable & flexible decentralized architecture to enable auditability & accountability of supply chains
- Outlines Security Guarantees
- Minimum adoption barriers for producers
- Ability for consumers to verify
- Flexible implementations for auditing/compliance

-
-
- er-
-

Table of Contents

y Chain Integrity, parency, and Trust (SCITT)

Table of Contents

utomate workflow for managing compliance of goods and

nsparent
ent)

hitecture

pply

bliance

Countersigning COSE Envelopes in Transparency Services (*in development*)

- Concise Signing and Encryption (COSE)
- Defining a method for issuing and verifying the counter-signatures on COSE messages
- Based on an authenticated data structure

G-19a / AS6171 Test Methods Standards

AS6171 General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts

- Risk-Based Selection of a sequence of counterfeit detection tests
- Metrics to quantify effectiveness of a test set
- Flexibility to select combinations of tests
- Allow optimization based on
  - equipment availability,
  - part construction
  - Expected use
  - likely failure modes & mechanisms.

Test Methods Covered in the Slash Sheet

- AS6171/2: External Visual Inspection (EVI)
- AS6171/3: X-Ray Fluorescence (XRF)
- AS6171/4: Delid/Decapsulation Physical Analysis (DDPA)
- AS6171/5: Radiological Inspection (RI)
- AS6171/6: Acoustic Microscopy (AM)
- AS6171/7: Electrical Test
- AS6171/8: Raman Spectroscopy
- AS6171/9: Fourier Transform Infrared Spectroscopy (FTIR)
- AS6171/10: Thermogravimetric Analysis (TGA)
- AS6171/11: Design Recovery (DR)

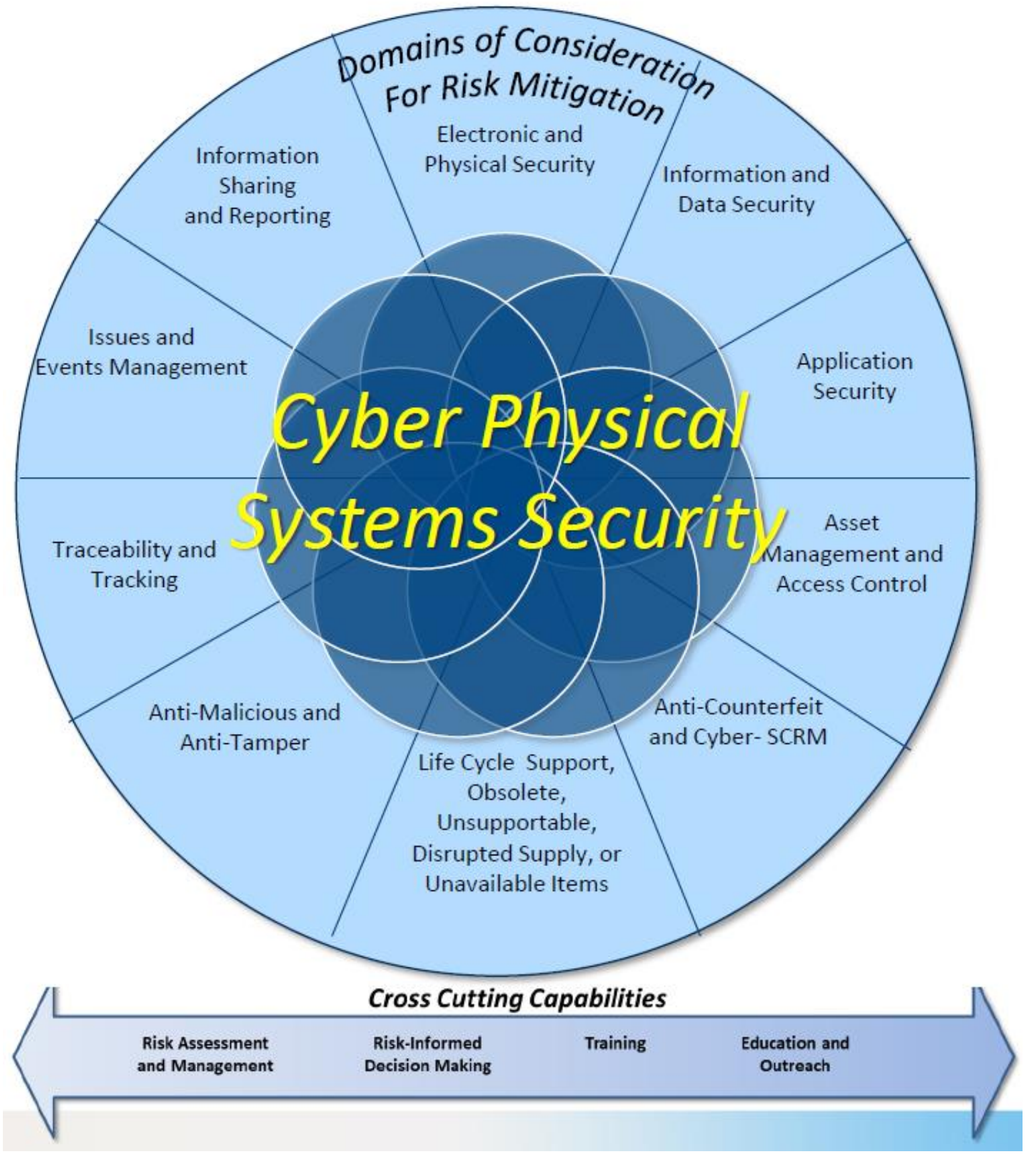
Other Highlights:

- 7 New Test Method Under Development
- Tampered Parts & Defects Taxonomy
- Hardware Trojans
- Netlist Assurance

G-32 Cyber Physical Systems (CPSS)

G-32 Objectives:

1. **Characterize and address the risk to CPSS, assess vulnerabilities, and recommend System Engineering focused mitigation actions.**
2. Share the knowledge of **how vulnerabilities are introduced and exploited** in cyber physical systems.
3. **Document best practices** for addressing areas of concern utilizing existing processes, procedures, and standards.
4. Develop a **taxonomy** for CPSS.
5. Establish standard methods for **identifying vulnerabilities** in cyber physical systems introduced at any point in the CPSS **life cycle & mitigating impacts**.
6. Develop **validation and verification methods** to ensure requirements are addressed.



G-32 Cyber Physical Systems

JA7496 - Cyber Physical Systems Security Engineering Plan (CPSSEP)

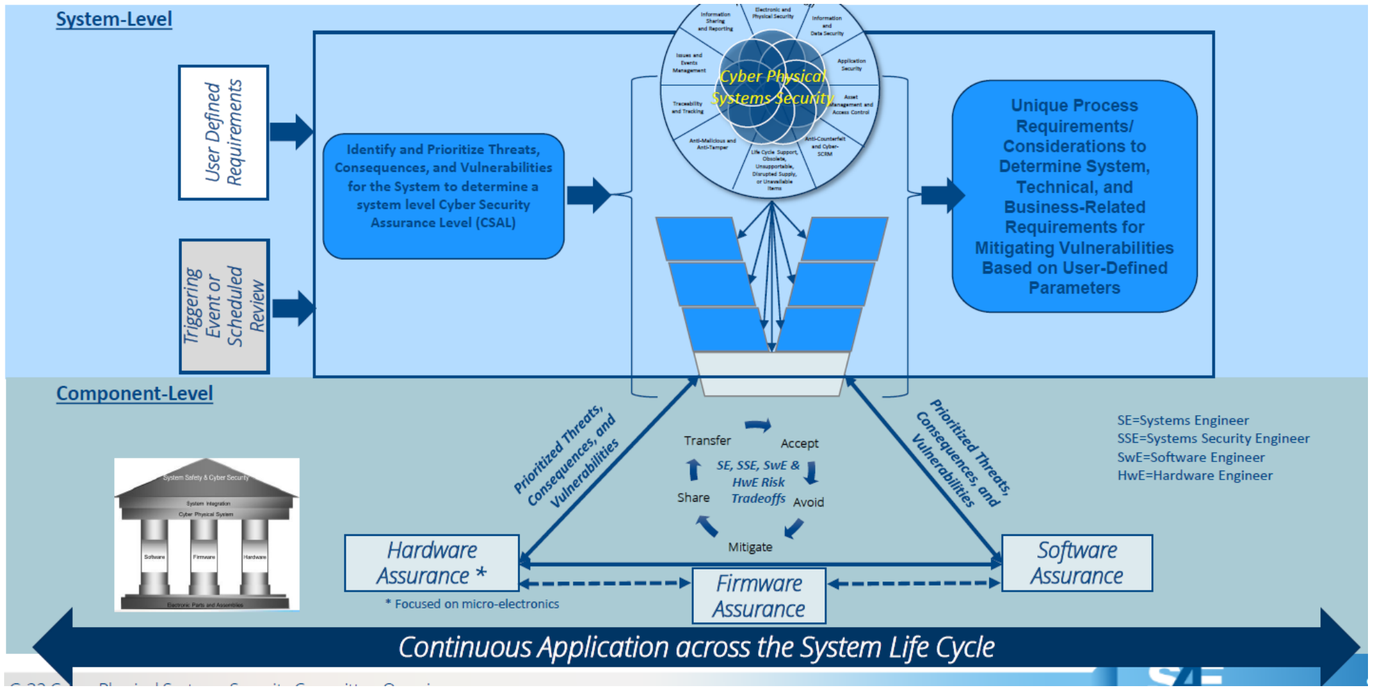
Supports developing a systems engineering approach to standardization of cyber physical systems security.

JA6678 – Cyber Physical Systems Security Software Assurance (SwA):

(a) Framing, Assurance, Realization and Utilization
(b) Structure follows NIST SP 800-39 (Managing Information Security Risk) and Common Criteria Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)
(c) Developed as blueprint for multi-sector application
(d) Designed to be used by specific sectors adaptations of SAE JA7496 for implementing CPS cybersecurity

A6801 - Cyber Physical Systems Security Hardware Assurance (HwA):

(a) Clarify HwA requirements with CPS system engineering activities
(b) ID & analyze risks associated with hardware components
(a) Develop countermeasure implementation plan
(b) Standardize practices for implementing HwA countermeasures
(a) and more…



IEEE Standards Association & Microelectronics

IEEE SA Overview :

- Standards Development
- Programs & Services
- IEEE SA Open Source
- Government Engagement Programs on Standards (GEPS)
- Conformity Assessment Program (ICAP)
- IEEE SA Centers of Competence

Standards Development Organization (SDO)	Developer / Committee	Designation / Title of Standard, Specification, Other Publication, or Program	Description
IEEE - Institute of Electrical and Electronics Engineers	Design Automation Standards Committee (DASC)	IEEE 1481-2019 - Standard for Integrated Circuit (IC) Library Architecture (OLA)	Addresses ways for integrated circuit designers to analyze chip timing and power consistently across a broad set of electri design automation (EDA) applications. Methods by which integrated circuit vendors can express timing and power information once per given technology are also covered.
IEEE - Institute of Electrical and Electronics Engineers	Design Automation Standards Committee (DASC)	IEC 61523-4 Edition 1.0 2015-03 (IEEE 1801-2013), IEEE/IEC International Standard - Design and Verification of Low-Power Integrated Circuits	Establishes a format used to define the low- power design intent for electronic systems and electronic intellectual property (IP). The format provides the ability to specify the supply network, switches, isolation, retention, and other aspects relevant to power management of an electronic system.
IEEE - Institute of Electrical and Electronics Engineers	Design Automation Standards Committee (DASC)	IEEE P1666 - Standard for Standard SystemC Language Reference Manual	Defines SystemC(R) with Transaction Level Modeling (TLM) as an ISO standard C++ class library for system and hardware design.
IEEE - Institute of Electrical and Electronics Engineers	Design Automation Standards Committee (DASC)	IEEE P1735 - Recommended Practice for Encryption and Management of Electronic Design Intellectual Property (IP)	Specifies embeddable and encapsulating markup syntaxes for design intellectual property encryption and rights management, together with recommendations for integration with design specification formats described in IEEE 1800 (SystemVerilog) and IEEE 1076 (VHDL).
IEEE - Institute of Electrical and Electronics Engineers	Design Automation Standards Committee (DASC)	IEEE P2416 - Standard for Power Modeling to Enable System-Level Analysis	Describes a parameterized and abstracted power model enabling system, software, and hardware intellectual property (IP) centric power analysis and optimization. It defines concepts for the development of parameterized, accurate, efficient, and complete power models for systems and hardware IP blocks usable for system power analysis and optimization.
IEEE - Institute of Electrical and Electronics Engineers	C/FSSC - Functional Safety Standards Committee	IEEE P2851 - Standard for Functional Safety Data Format for Interoperability within the Dependability Lifecycle	Defines a data format with which results of functional safety analyses (such as FMEA (Failure Mode and Effects Analysis), FMEDA (Failure Modes, Effects and Diagnostic Analysis), FMECA (Failure Mode, Effects and Criticality analysis), FTA (Fault Tree analysis) and related functional safety verification activities.
IEEE - Institute of Electrical and Electronics Engineers	Microprocessor Standards Committee (MSC)	IEEE 1722.1-2021 - Standard for Device Discovery, Connection Management, and Control Protocol for Time-Sensitive Networking System	Specifies the protocol, device discovery, connection management, and device control procedures used to facilitate interoperability between systems that use IEEE 802 time sensitive networking standards.
IEEE - Institute of Electrical and Electronics Engineers	Smart Manufacturing Standards Committee (SM)	IEEE 2671-2022 - Draft Standard for General Requirements of Online Detection Based on Machine Vision in Intelligent Manufacturing	Specifies through the general requirements of online detection based on machine vision, including requirements for data format, data transmission processes, definition of application scenarios and performance metrics for evaluating the effect of online detection deployment.
IEEE - Institute of Electrical and Electronics Engineers	C/SAB - Standards Activities Board	IEEE P2672 - Guide for General Requirements of Mass Customization	Provides the definitions, terminologies, operation procedures, system architectures, key technological requirements, data requirements and applications of and related to user- oriented mass customization. This guide provides reference information to be used by manufacturing enterprises for designing and implementing business models of mass customization.
IEEE - Institute of Electrical and Electronics Engineers	C/SAB - Standards Activities Board	IEEE P2806 - System Architecture of Digital Representation for Physical Objects in Factory Environments	Defines the system architecture of digital representation for physical objects in factory environments. The system architecture describes the objective, important components, required data resources and basic establishing procedure of digital representation in factory environments.
IEEE - Institute of Electrical and Electronics Engineers	Smart Manufacturing Standards Committee (SM)	IEEE P2879 - General Principles for Assessment of a Smart Factory	Defines basic terminologies, assessment process requirements, indicator metrics, assessment methods and assessment criteria of smart factories
IEEE - Institute of Electrical and	Software and Systems Engineering	IEEE 2675-2021 - Standard for DevOps:Building Reliable and	Specifies practices for groups including development, operations and other key stakeholders to collaborate and

National Institute of Standards & Technology

SP 800-161r1 C-SCRM for Systems and Organizations Revisions

- Integrates broader ERM C-SCRM & NextGen C-SCRM controls
- Templates to enable C-SCRM
- Risk Appetite & Tolerance guidance
- Guidance on C-SCRM program management function development
- Address Critical Success Factors
- Appendix E on FASCSA
- Appendix F on EO 14028 Section 4(d),Software Supply Chain Security

National Institute of Standards & Technology

SP 800-218 Secure Software Development Framework (SSDF)

- A core set of high-level secure software development practices
- Help software producers:
  - reduce the number of vulnerabilities in released software,
  - reduce the potential impact of the exploitation of undetected or unaddressed vulnerabilities, and
  - address the root causes of vulnerabilities to prevent recurrences.
- Organized into 4 Groups
  - Prepare the Organization (PO)
  - Protect the Software (PS)
  - Produce Well-Secured Software (PW)
  - Respond to Vulnerabilities (RV)
- Software producers & acquirers can use it to foster communications for procurement processes and other management activities.

Hardware Security Program – NIST IR 8320

- Identify threats, develop mitigations and manage vulnerabilities
- Develop standards, guidelines for IP/data protection/sharing, security risk management and establish provenance
- Integrate point tools for an automated cybersecurity tools and techniques
- Develop cybersecurity measurements and metrics
- Leverage and extend existing NIST cybersecurity principles and practices

Telecommunications Industry Association

SCS 9001

[TIA QuEST Forum's Supply Chain Security Working Group]

[SCS 9001: Global Supply Chain Security Standard]

SCS 9001 is a certifiable, process-based standard for the ICT industry. Aligned with EO14028, BEAD NOFO and NIST Publications and provides guidance for:

(1) Secure software development;
(2) Validation methods for ensuring software ID and source traceability;
(3) Product security;
(4) Governmental requirements on source of origin and transparency of internal controls.

Updates Anticipated by EOY 2022:

- General improvements from lessons learned from the Pilot Program and initial engagements
- Changes on Hardware provenance and development requirements
- Increased coverage of procurement, shipping and logistics requirements
- More support for government requirements such as BEAD NOFO UK Telecommunications Security Act
- Decoupling from the ISO 9001 standard:
- More flexibility in selecting facilities needing a QMS or just a security standard
- Maintains the ISO Annex SL format for ease of integration with existing Quality Management Systems as required

Microelectronics Standards and Guidance Landscape

American National Standards Institute

Department of Defense RFI 2020

Objectives

- Identify Standards Development Organizations (SDOs) activities;
- Gain understanding about procedures, policies, participation, and fees;
- Learn history and engagement with federal & other government agencies;
- Determine interest for supporting future ME standards development.

Outreach

ASTM INTERNATIONAL

Electronic Components Industry Association

Respondents

ANSI RFI 2022

Outreach

- 2020 RFI Respondents – updates incorporated
- ANSI's networks of standards development organizations, technical experts and members

Respondent Organizations

IEEE

IPC

JEDEC

SAE INTERNATIONAL

TIA Telecommunications Industry Association

THE Open GROUP


ANSI
American National Standards Institute

Website: www.ansi.org

Contacts: James McCabe
Senior Director, Standards Facilitation
jmmcabe@ansi.org

Christine Bernat
Associate Director, Standards Facilitation
cbernat@ansi.org

Respondents should send RFI submittals and inquiries to Christine Bernat and Jim McCabe.

Global Supply Chain Security for Microelectronics Standardization

Standards Roadmap and Gap Analysis

Standards tables last edited October 24, 2022

Description:

The tables found in the "ANSI Microelectronics Standards Landscape" include standards previously identified for the U.S. Department of Defense (DoD) in response to both 2020 and 2022 Requests for Information, discussions from the July 2022 ANSI workshop, and other relevant activity captured by ANSI staff. On behalf of the DoD, ANSI is seeking information about published standards, standards activities underway from standards development organizations (SDOs), or other guidance documents that will help to assure supply chain and operational security standards for the procurement of microelectronics products and services.

The objective(s) of the standard(s) are to create a system of best practices for procuring and assuring microelectronics products and services. For this activity, procurements are primarily scoped to microelectronic integrated circuits, the components that comprise them, and the services supporting the full procurement lifecycle. These standards will establish a risk-based approach that considers technology alternatives, supplier demographics (e.g., manufacturing location, company ownership, workforce composition), processes (e.g., access during manufacturing suppliers' design, sourcing, manufacturing packaging, and distribution processes), supply chain reliability, and other matters germane to supply chain and operational security. Standards or mitigations should provide risk mitigation techniques through best practices in engineering design and evaluation, product verification, technology and intellectual property controls, and other mechanisms for implementation in the design, manufacture and use of microelectronics products and services.

Request for Information:

Instructions

Respondents should add their directly related standards into the tables on the next worksheet following the format provided. The Lanscape tables contain two sections:

(1) Microelectronics Supply Chain Standards Technical Pillars
(2) Standards Development Organizations and other Standards Activities Listing

It is requested that respondents add their standards in Section 2 and then note which of the pillars the individual standards address in Section 1 using an 'X'. Additional context around the pillars can be found in the "Pillars Context" worksheet of this excel. Upon completion, please send the spreadsheet back to Christine Bernat and Jim McCabe. Respondents interested in entering information through OneDrive should provide 1 primary point of contact for entry to ANSI.

July Workshop Results

- 45 standards, related guidance and policies identified & incorporated into ME landscape
- In addition to SDOs, other resources from:
  - DHS – U.S. Department of Homeland Security
  - DoD – U.S. Department of Defense
  - EASA – European Union Aviation Safety Agency
  - NASA – U.S. National Aeronautics and Space Administration
  - NIST – National Institute of Standards & Technology
  - NSA – National Security Agency
  - Whitehouse EO's

RFI Technical Pillars

Evaluating Standards Content

- Respondents were asked to identify which supply chain practice and risk management areas that their documents addressed.

- Standards may address more than one of the pillars.

- Breakout groups organized by these pillars.

Supply Chain Practice Areas:	
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)
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.
Secure Design	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). May overlap with other supply chain practice areas.
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.

Activity Listing & Pillar Affiliation

Contents:

Pillars Affiliation Notation: Individual standards are evaluated and note for their applicability to the pillars. This will assist to filter and identify existing and needed standards.

Standards Listing: Provides direct links to the committees, individual standards as well as brief context and status of documents to give users access to and a better understanding of what is available today.

MICROELECTRONICS SUPPLY CHAIN SECURITY TECHNICAL PILLARS					STANDARDS AND GUIDANCE LISTING								
Supply Chain Practice	Procurement Management	Supply Chain Traceability	Information / IP Protection	Secure Design	Organization / Standards Development Organization (SDO)	Developer / Committee	Designation / Title of Standard, Specification, Other Publication, or Program	Description	Publication / Target Date	Publication Status	Inactivated / Withdrawn Date	Notes
	X	X	X	X	Accellera	IP Security Assurance WG	Security Annotation for Electronic Design Integration Standard 1.0	SA-EDI Standard defines a specification that documents security concerns for hardware IP and its associated components when integrated into an IC. With the new standard, IP providers can either identify security concerns to mitigate within their IP or disclose the concerns to their integrator. Users of the SA-EDI standard can provide consistent security collateral in a uniform format.		Published		Donated to IEEE as P3164
	X	X	X	X	Accellera	Functional Safety WG	Data for Interoperability & Traceability in the Functional Safety Lifecycle	The standard is to capture and propagate the functional safety intent. This helps to better integrate analysis methods such as FMEDA, DFA and FTA and to enable a functional safety-aware design and verification flow for electronic circuits and systems. Enabling functional safety is a multi-disciplinary challenge which significantly benefits from alignment and standardization across the supply chain involving different industries and domains.		WIP		Whitepaper published with standard development in progress
	X	X	X	X	Accellera	Portable Stimulus WG	Portable Test and Stimulus Standard 2.0	The Portable Test and Stimulus Standard (PSS) defines a specification to create a single representation of stimulus and test scenarios, usable by a variety of users across many levels of integration under different configurations. This representation facilitates the generation of diverse implementations of scenarios that run on a variety of execution platforms, including, but not necessarily limited to, simulation, emulation, FPGA prototyping, and post-silicon. With this standard, users can specify intent once and observe consistent behavior across multiple implementations.		Published		
			X		Alliance for Telecommunications Industry Solutions (ATIS)	5G Supply Chain	ATIS Standard: 5G Network Assured Supply Chain (ATIS-I-0000080)	Among other things, the 5G Supply Chain Working Group works to establish a common assurance framework for trusted 5G networks; develop or identify standards to be applied to 5G systems; and evaluate audit/certification options for ICT solution providers, infrastructure and endpoint device original equipment manufacturers. These objectives are intended to address end-to-end ICT supply chain visibility, coordination of existing supply chain management best practices, industry alignment with federal guidelines, improved threat monitoring tools and a method to influence national/international standards development.	6/1/2022	Active Standard		
			X		Department of Defense	Committee on National Security Systems (CNSS)	CNSSI No. 1253: Security Categorization and Control Selection for National Security Systems	CNSSI No. 1253 is a companion document to the NIST publications relevant to categorization and selection (i.e., NIST SP 800-53; NIST SP 800-37; NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories; and Federal Information Processing Standards [FIPS] 199, Standards for Security Categorization of Federal Information and Information Systems) and applies to all NSS. This Instruction also provides NSS-specific information on developing and applying overlays for the national security community and parameter values for NIST SP 800-53 security controls that are applicable to all NSS.	3/37/2014	Published		Identified in the July 2022 ANSI workshop Information and IP protection WG
			X	X	Department of Defense (DoD)	Office of the Under Secretary of Defense for Research and Engineering (OUSD R&E)	DoDI 5000.83 Technology and Program Protection to Maintain Technological Advantage	Establishes policy, assigns responsibilities, and provides procedures for science and technology (S&T) managers and engineers to manage system security and cybersecurity technical risks from foreign intelligence collection; hardware, software, cyber, and cyberspace vulnerabilities; supply chain exploitation; and reverse engineering to: o DoD-sponsored research and technology that is in the interest of national security. o DoD warfighting capabilities. • Assigns responsibilities and provides procedures for S&T managers and lead systems engineers for technology area protection plans (TAPPs), S&T protection, program protection plans (PPPs), and engineering cybersecurity activities.	5/21/2021	Published		Identified in the July 2022 ANSI workshop Information and IP protection WG
			X	X	Department of Defense (DoD)	Office of the Under Secretary of Defense for Research and Engineering (OUSD R&E)	DoDI 5200.44 Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)	This Instruction, in accordance with the authorities in DoD Directive (DoDD) 5134.01 (Reference (a)) and DoDD 5144.02 (Reference (b)): a. Establishes policy and assigns responsibilities to minimize the risk that DoD's warfighting mission capability will be impaired due to vulnerabilities in system design or sabotage or subversion of a system's mission critical functions or critical components, as defined in this Instruction, by foreign intelligence, terrorists, or other hostile elements.	10/15/2018	Published		Identified in the July 2022 ANSI workshop Information and IP protection WG
					Department of Defense (DoD)	Office of the Under Secretary of Defense for Research and Engineering (OUSD R&E)	DoD Cybersecurity Maturity Model Certification (CMMC)	To safeguard sensitive national security information, the Department of Defense (DoD) launched CMMC 2.0, a comprehensive framework to protect the defense industrial base from increasingly frequent and complex cyberattacks. With its streamlined requirements, CMMC 2.0: Cuts red tape for small and medium sized businesses Sets priorities for protecting DoD information Reinforces cooperation between the DoD and industry in addressing evolving cyber threats	11/4/2021			

**Image not intended to be a full representation of all listing content*

Overall Statistics

- 23 Organizations
  - Some published as joint documents
  - 6 Government Agencies
- 71 Committees/Groups
- 167 Standards
  - 21 Regulatory Policies / Guidance

Organizations Represented

Accellera	National Institute of Standards and Technology (NIST)
Alliance for Telecommunications Industry Solutions (ATIS)	National Security Agency (NSA)
Department of Defense (DoD)	Open Compute Project (OCP)
Department of Homeland Security (DHS)	RISC-V International
European Aviation Safety Agency (EASA)	RTCA Inc.
Institute of Electrical and Electronics Engineers (IEEE)	SAE International
International Standards Organization (ISO)	Silicon Integration Initiative (Si2)
Internet Engineering Task Force (IETF)	Telecommunications Industry Association (TIA)
IPC	The Open Group
International Electrotechnical Commission (IEC)	Transported Asset Protection Association (TAPA)
JEDEC	Unified Extensible Firmware Interface Forum (UEFI)
National Aeronautics and Space Administration (NASA)	

Takeaways

- Several standards organizations are developing related standards.
- Collectively, there is a toolbox industry and government can leverage.
- No commonly agreed singular high-level specification/practice providing how to leverage the collection of existing resources.
- Several forums are well-positioned to fill gaps and support future standards development needs.
- Other organizations wishing to submit their documents should utilize the excel and submit to cbernat@ansi.org and jmccabe@ansi.org

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