Request for Information (RFI) Summary: *SDO Responses & Analysis*

Christine Bernat, Associate Director, Standards Facilitation, ANSI

DoD microelectronics kick-off

27 July 2022

©2022

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 · ecia Electronic Components Industry Association · IEEE · IPC · ISO · JEDEC · SAE INTERNATIONAL · semi · UL

Respondents

IEEE · IPC · JEDEC · SAE INTERNATIONAL

2020 RFI Respondents

IEEE

- 8 Committees
- 55 Standards
- Focus on microprocessors, design/verification, software, testing, smart manufacturing

JEDEC

- 1 Committee
- 3 Standards
- Focus on procurements, counterfeit parts, semiconductor devices

IPC BUILD ELECTRONICS BETTER

- 4 Committees
- 10 Standards
- Focus on electronic packages, plastic chip carriers, supply chain traceability.

SAE INTERNATIONAL

- 6 Committees
- 28 Standards
- Focus on cyber, counterfeit, best manufacturing processes, and solid state devices

ANSI RFI 2022

Outreach

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

Respondent Organizations

IEEE

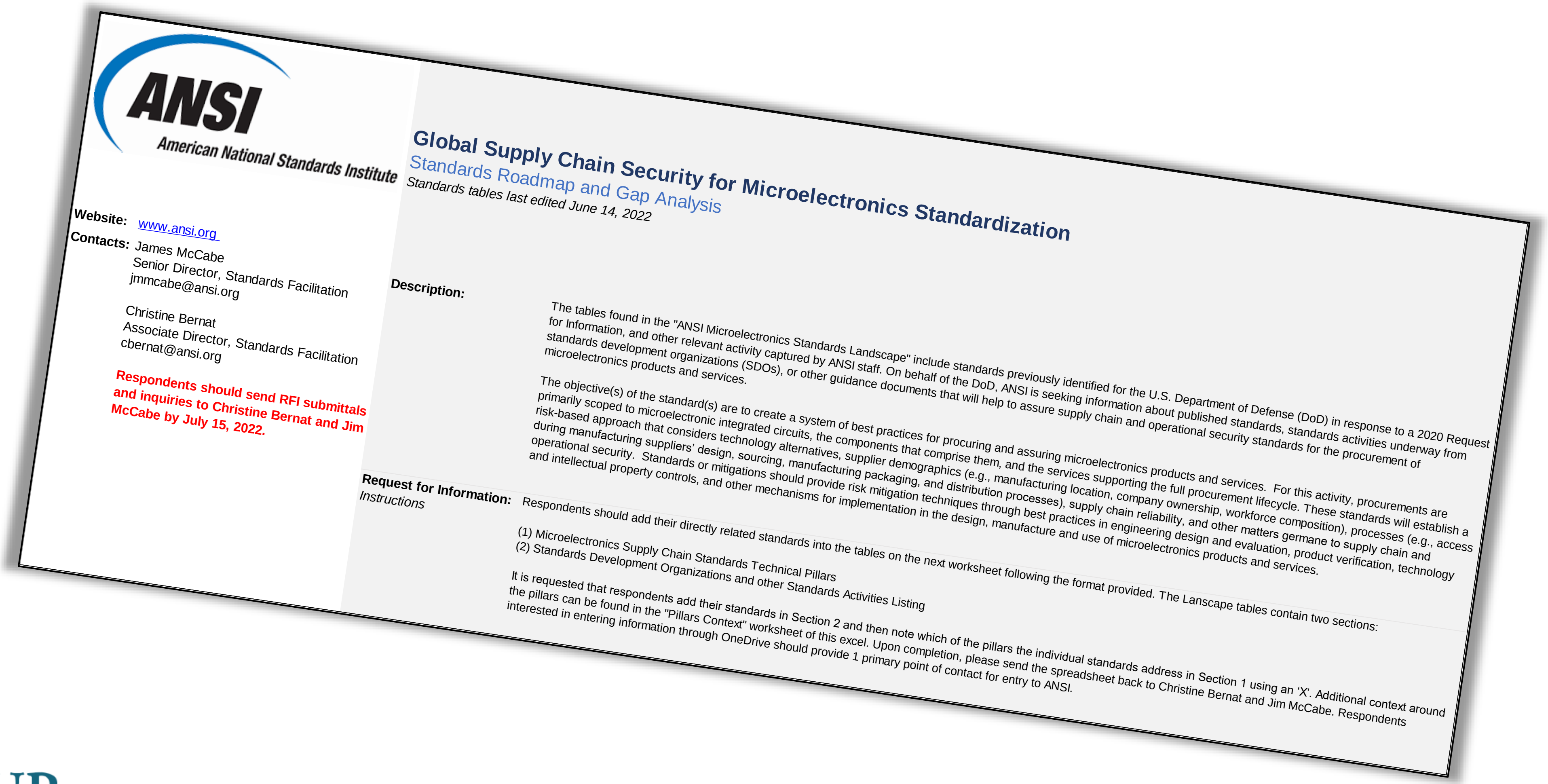
IPC®

JEDEC®

SAE INTERNATIONAL®

TIA® Telecommunications Industry Association

THE Open® GROUP



ANSI American National Standards Institute

Global Supply Chain Security for Microelectronics Standardization

Standards Roadmap and Gap Analysis

Standards tables last edited June 14, 2022

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 by July 15, 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 a 2020 Request for Information, 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:

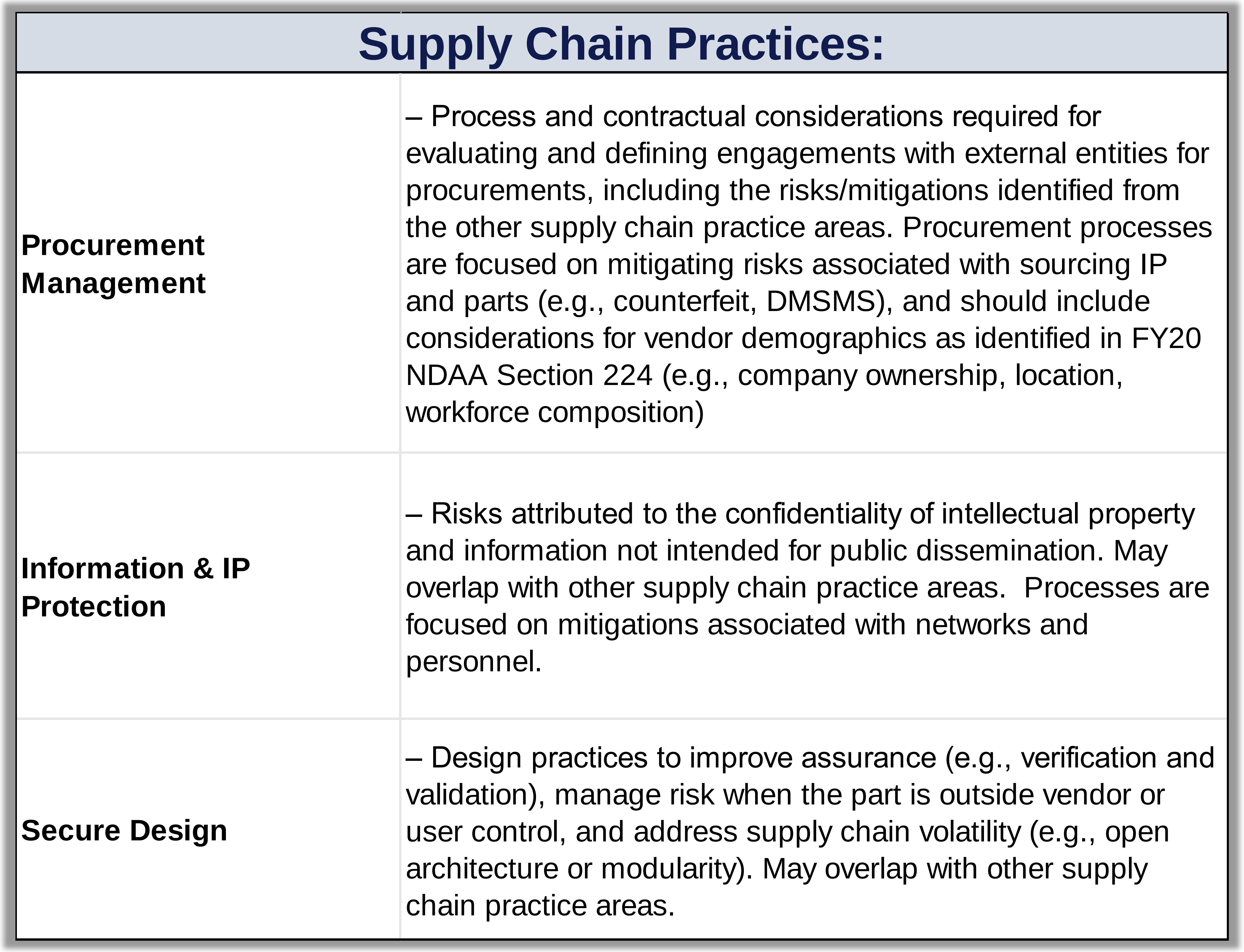
(1) Microelectronics Supply Chain Standards Technical Pillars
(2) Standards Development Organizations and other Standards Activities Listing

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.

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.
- Discussions tomorrow are also organized by these pillars.



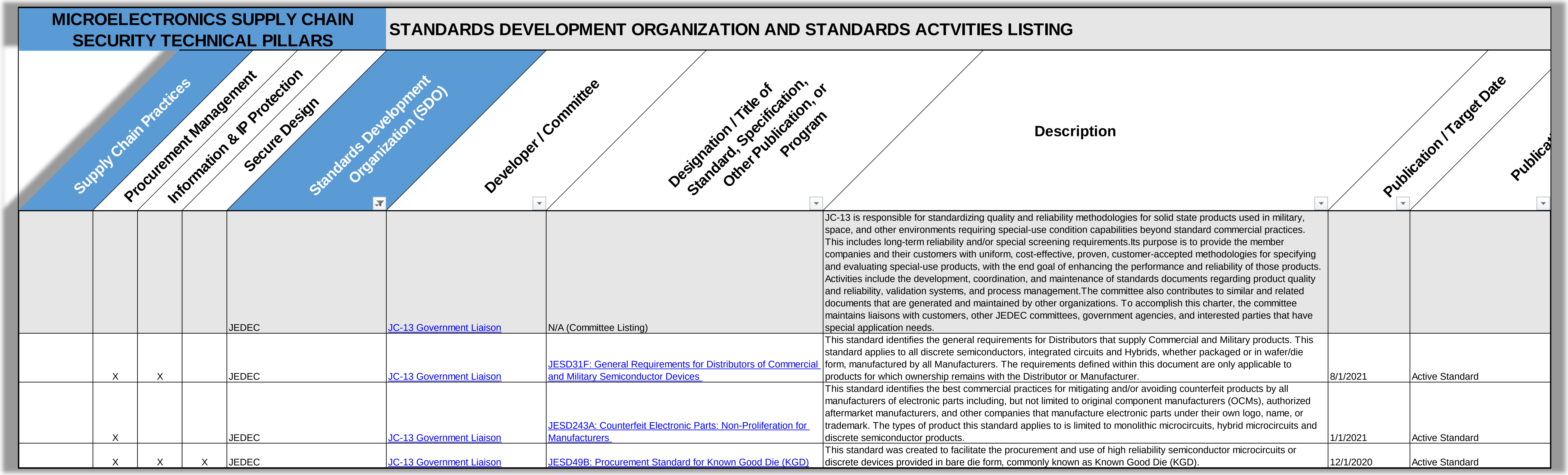
Supply Chain Practices:	
Procurement Management	– Process and contractual considerations required for evaluating and defining engagements with external entities for procurements, including the risks/mitigations identified from the other supply chain practice areas. Procurement processes are focused on 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.

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 DEVELOPMENT ORGANIZATION AND STANDARDS ACTVITIES LISTING					
Supply Chain Practices	Procurement Management	Information & IP Protection	Secure Design	Standards Development Organization (SDO)	Developer / Committee	Designation / Title of Standard, Specification, Other Publication, or Program	Description	Publication / Target Date	Publica
				JEDEC	JC-13 Government Liaison	N/A (Committee Listing)	JC-13 is responsible for standardizing quality and reliability methodologies for solid state products used in military, space, and other environments requiring special-use condition capabilities beyond standard commercial practices. This includes long-term reliability and/or special screening requirements.Its purpose is to provide the member companies and their customers with uniform, cost-effective, proven, customer-accepted methodologies for specifying and evaluating special-use products, with the end goal of enhancing the performance and reliability of those products. Activities include the development, coordination, and maintenance of standards documents regarding product quality and reliability, validation systems, and process management.The committee also contributes to similar and related documents that are generated and maintained by other organizations. To accomplish this charter, the committee maintains liaisons with customers, other JEDEC committees, government agencies, and interested parties that have special application needs.		
	X	X		JEDEC	JC-13 Government Liaison	JESD31F: General Requirements for Distributors of Commercial and Military Semiconductor Devices	This standard identifies the general requirements for Distributors that supply Commercial and Military products. This standard applies to all discrete semiconductors, integrated circuits and Hybrids, whether packaged or in wafer/die form, manufactured by all Manufacturers. The requirements defined within this document are only applicable to products for which ownership remains with the Distributor or Manufacturer.	8/1/2021	Active Standard
	X			JEDEC	JC-13 Government Liaison	JESD243A: Counterfeit Electronic Parts: Non-Proliferation for Manufacturers	This standard identifies the best commercial practices for mitigating and/or avoiding counterfeit products by all manufacturers of electronic parts including, but not limited to original component manufacturers (OCMs), authorized aftermarket manufacturers, and other companies that manufacture electronic parts under their own logo, name, or trademark. The types of product this standard applies to is limited to monolithic microcircuits, hybrid microcircuits and discrete semiconductor products.	1/1/2021	Active Standard
	X	X	X	JEDEC	JC-13 Government Liaison	JESD49B: Procurement Standard for Known Good Die (KGD)	This standard was created to facilitate the procurement and use of high reliability semiconductor microcircuits or discrete devices provided in bare die form, commonly known as Known Good Die (KGD).	12/1/2020	Active Standard

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

Overall Results

- 16 Organizations
  - Joint IEEE/ISO/IEC
  - Joint SAE/ISO
- 31 Committees
- 113 Standards

IEEE Committees

1. Design Automation Standards Committee (DASC)
2. Microprocessor Standards Committee (MSC)
3. Simulation Interoperability Standards Organization Standards Activity Committee (SISO SAC) Committee
4. Smart Manufacturing Standards Committee (SM)
5. Software and Systems Engineering Standards Committee (S2ESC)
6. Test Technology Standards Committee (TT)
7. IM/WM&A - TC10 - Waveform Generation Measurement and Analysis
8. PES Substations Committee

Design Automation Standards Committee (DASC)

IEEE 2401-2019™, IEEE Standard Format for LSI-Package-Board Interoperable Design	Provides a method for specifying a common interoperable format for electronic systems design. The format provides a common way to specify information/data about the project management, netlists, components, design rules, and geometries used in the large-scale integration-package- board designs.
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 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 P1800 - Standard for SystemVerilog--Unified Hardware Design, Specification, and Verification Language	Provides the definition of the language syntax and semantics for the IEEE 1800-2017 Standard for SystemVerilog--Unified Hardware Design, Specification, and Verification Language, which is a unified hardware design, specification, and verification language.
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 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.

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 695-1990™, IEEE Standard for Microprocessor Universal Format for Object Modules:
Specifies the format of linkable, relocatable, and absolute object modules. MUFOM, the Microprocessor Universal Format for Object Modules, is designed to apply to a variety of target machines.

Smart Manufacturing Standards Committee (SM)

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 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 P2671 - 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.

Software and Systems Engineering Standards Committee (S2ESC)

IEEE P1012 - Standard for System, Software, and Hardware Verification and Validation:
Addresses all system, software, and hardware life cycle processes including the Agreement, Organizational Project- Enabling, Project, Technical, Software Implementation, Software Support, and Software Reuse process groups.

IEEE P1228 - Standard for Software Safety:
Applies to software safety during the development, procurement, maintenance, and retirement of safety- critical software. Requires that software safety be considered within the context of the system safety program throughout the software lifecycle.

IEEE 7002-2022 - Standard for Data Privacy Process:
Defines requirements for a systems/software engineering process for privacy-oriented considerations regarding products, services, and systems utilizing employee, customer or other external user's personal data. Extends across the life cycle from policy through development, quality assurance, and value realization.

IEEE/ISO/IEC P41062 - Software Engineering - Life cycle processes - Software Acquisition:
Describes set of useful activities, tasks and methods that can be selected and applied during the acquisition of software or software services. Supply chain may include integration of commercial-off-the-shelf (COTS), custom, or open source software.

Test Technology Standards Committee (TT)

IEEE 1687-2014™, IEEE Standard for Access and Control of Instrumentation Embedded within a Semiconductor Device:
Describes a methodology for accessing instrumentation embedded within a semiconductor device, without defining the instruments or their features themselves, via the IEEE 1149.1™ test access port (TAP) and/or other signals. The elements of the methodology include a hardware architecture for the on-chip network connecting the instruments to the chip pins, a hardware description language to describe this network, and a software language and protocol for communicating with the instruments via this network.

IEEE 1450-1999™, International Standard Test Interface Language (STIL) for Digital Test Vector Data:
Provides an interface between digital test generation tools and test equipment. A test description language is defined that: (a) facilitates the transfer of digital test vector data from CAE to ATE environments; (b) specifies pattern, format, and timing information sufficient to define the application of digital test vectors to a DUT; and (c) supports the volume of test vector data generated from structured tests.

IPC Committees & Standards

2-19b Trusted Suppliers TG *(2-19 Supply Chain Traceability & Trust Subcommittee)*	IPC-1791 B - Trusted Electronic Designer, Manufacturer, and Assembler Requirements	Provides minimum requirements, policies and procedures for printed board design, fabrication, and assembly organizations and/or companies to become trusted sources for markets requiring high levels of confidence in the integrity of delivered products. IPC-1791B expands the standard's requirements to account for trusted sources of cable and wire harness assemblies.
B-10a Plastic Chip Carrier Cracking TG	IPC/JEDEC-J-STD-033 D - Packaging and Handling of Moisture Sensitive Non-Hermetic Solid State Surface Mount Devices	Provides surface mount device manufacturers and users with standardized methods for handling, packing, shipping and use of moisture/reflow sensitive components. These methods help avoid damage from moisture absorption and exposure to solder reflow temperatures that can result in yield and reliability degradation and damaged components. Procedures provide a minimum shelf life of 12 months from the seal date when properly implemented. Developed by IPC and JEDEC.
B-11a 3D Electronic Packages Guideline TG	IPC-7091 - Design and Assembly Process Implementation of 3D Components	Information to those who are designing, developing or using 3D-packaged semiconductor components or those who are considering 3D package implementation. The 3D semiconductor package may include multiple die elements—some homogeneous and some heterogeneous. The package may also include several discrete passive SMT devices, some of which are surface mounted and some of which are integrated (embedded) within the components' substrate structure.
B-10a Plastic Chip Carrier Cracking TG	IPC/JEDEC-J-STD-020 E - Moisture/Reflow Sensitivity Classification of Plastic Surface Mount Devices	Used to determine what moisture-sensitivity-level (MSL) classification level should be used so that surface mount devices (SMDs) can be properly packaged, stored and handled to avoid subsequent thermal and mechanical damage during the assembly solder reflow attachment and/or repair operation. J-STD-020 covers components to be processed at higher temperatures for lead-free and lower temperature Sn-Pb assemblies.
6-10d SMT Attachment Reliability Test Methods TG	IPC/JEDEC-9301 - Numerical Analysis Guidelines for Microelectronics Packaging Design and Reliability	Basic tenets of a typical Finite Element Analysis (FEA) model, as well as, to educate new designers (and in some cases even experienced designers) on the basic information and best practices that should be captured and provided to technical reviewers of the results of FEA data.
6-10d SMT Attachment Reliability Test Methods TG	IPC-1782 A - Standard for Manufacturing and Supply Chain Traceability of Electronic Products	Minimum requirements for manufacturing and supply chain traceability based on perceived risk. IPC-1782A applies to all products, processes, assemblies, parts, components, equipment and other items used in the manufacture of printed board assemblies and in mechanical assembly

JEDEC Committees

JC-13 Government Liaison	JESD31F: General Requirements for Distributors of Commercial and Military Semiconductor Devices	Identifies the general requirements for Distributors that supply Commercial and Military products. This standard applies to all discrete semiconductors, integrated circuits and Hybrids, whether packaged or in wafer/die form, manufactured by all Manufacturers. The requirements defined within this document are only applicable to products for which ownership remains with the Distributor or Manufacturer.
JC-13 Government Liaison	JESD243A: Counterfeit Electronic Parts: Non-Proliferation for Manufacturers	Identifies the best commercial practices for mitigating and/or avoiding counterfeit products by all manufacturers of electronic parts including, but not limited to original component manufacturers (OCMs), authorized aftermarket manufacturers, and other companies that manufacture electronic parts under their own logo, name, or trademark. The types of product this standard applies to is limited to monolithic microcircuits, hybrid microcircuits and discrete semiconductor products.
JC-13 Government Liaison	JESD49B: Procurement Standard for Known Good Die (KGD)	Facilitates the procurement and use of high reliability semiconductor microcircuits or discrete devices provided in bare die form, commonly known as Known Good Die (KGD).

JC-13 is responsible for standardizing quality and reliability methodologies for solid state products used in military, space, and other environments requiring special-use condition capabilities beyond standard commercial practices. This includes long-term reliability and/or special screening requirements. Its purpose is to provide the member companies and their customers with uniform, cost-effective, proven, customer-accepted methodologies for specifying and evaluating special-use products, with the end goal of enhancing the performance and reliability of those products.

SAE International Committees

1. CE-12 Solid State Devices
2. G-14 Americas Aerospace Quality
3. G-19 Counterfeit Electronics Avoidance and Detection
4. G-23 Manufacturing Management
5. G-32 Cyber Physical Systems
6. Avionics Process Management Committee (APMC)
7. TEVEES18A - Vehicle Cybersecurity Systems Engineering Committee
8. Vehicle Cybersecurity Systems Engineering Committee

G-19A Test Laboratory Standards Development Committee

AS6171A - Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts.

AS6171/1 - Suspect/Counterfeit Test Evaluation Method

AS6171/2A - Techniques for Suspect/Counterfeit EEE Parts Detection by External Visual Inspection, Remarking and Resurfacing, and Surface Texture Analysis Using SEM Test Methods

AS6171/3 - Techniques for Suspect/Counterfeit EEE Parts Detection by X-ray Fluorescence Test Methods

AS6171/4 - Techniques for Suspect/Counterfeit EEE Parts Detection by Delid/Decapsulation Physical Analysis Test Methods

AS6171/5 - Techniques for Suspect/Counterfeit EEE Parts Detection by Radiological Test Methods

AS6171/6 - Techniques for Suspect/Counterfeit EEE Parts Detection by Acoustic Microscopy (AM) Test Methods

AS6171/7 - Techniques for Suspect/Counterfeit EEE Parts Detection by Electrical Test Methods

AS6171/8 - Techniques for Suspect/Counterfeit EEE Parts Detection by Raman Spectroscopy Test Methods

AS6171/9 - Techniques for Suspect/Counterfeit EEE Parts Detection by Fourier Transform Infrared Spectroscopy (FTIR) Test Methods

AS6171/10 - Techniques for Suspect/Counterfeit EEE Parts Detection by Thermogravimetric Analysis (TGA) Test Methods

AS6171/11 - Techniques for Suspect/Counterfeit EEE Parts Detection by Design Recovery Test Methods

AS6810 - Requirements for Accreditation Bodies when Accrediting Test Laboratories Performing Detection of Suspect/Counterfeit in Accordance with AS6171 General Requirements and the Associated Test Methods

SAE Counterfeit Defect Coverage Tool

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.

JA6801 - Cyber Physical Systems Security Hardware Assurance:

(a) assess and address weaknesses and vulnerabilities of cyber physical system hardware utilizing systems engineering principles to ensure security and resilience throughout the lifecycle of the system,
(b) conduct EEE component level assurance and analysis, considering impact on the hardware, software, and firmware, in the product or system,
(c) Address concerns including interfaces and network of the system and command and control that could be manipulated through a physical process and/or physical input of the data.

JA6678 – Cyber Physical Systems Security Software Assurance:

(a) assess and address vulnerabilities of cyber physical system software utilizing systems engineering principles to ensure security and resilience throughout the lifecycle of the system,
(b) conduct software assurance and analysis, considering impact on the product's software, hardware, and firmware,
(c) Address concerns including consideration of the interfaces and network of the system and command and control that could be manipulated through a physical process and/or physical input of the data flow and computation,
(d) perform design validation and verification to assess security and resiliency of software impacting the cyber physical system safety, security and integrity across the complete lifecycle.

Avionics Process Management Committee (APMC)

EIA933C - Requirements for a COTS Assembly Management Plan:
This document applies to the development of Plans for integrating and managing COTS assemblies in electronic equipment and Systems for the commercial, military, and space markets; as well as other ADHP markets that wish to use this document.

STD0016A Standard for Preparing a DMSMS Management Plan:
Requirements for developing a DMSMS Management Plan to assure customers that the Plan owner is using a proactive DMSMS process for minimizing the cost and impact that part and material obsolescence will have on equipment delivered by the Plan owner. Owners of DMSMS Management Plans include System Integrators, Original Equipment Manufacturers (OEM), and logistics support providers. Technical requirements ensure that the Plan owner can meet the requirement of having a process to address obsolescence as required by DoD Programs as required by MIL-STD-3018 "Parts Management".

EIASTD4899C - Requirements for an Electronic Components Management Plan:
Development of Plans for integrating and managing electronic components in equipment for the military and commercial aerospace markets. Examples of electronic components, as described in this document, include resistors, capacitors, diodes, integrated circuits, hybrids, application specific integrated circuits, wound components, and relays.

SAE International Key Standards

G-14 Americas Aerospace Quality	AS9100D - Quality Management Systems - Requirements for Aviation, Space, and Defense Organizations	Includes ISO 9001:2015 quality management system requirements and specifies additional aviation, space, and defense industry requirements, definitions, and notes.
CE-12 Solid State Devices	AS6294/2 Requirements for Plastic Encapsulated Microcircuits in Military and Avionics Applications.	Establishes common industry practices, and screening and qualification testing, of Plastic Encapsulated Microcircuits (PEMs) for use in military and avionics application environments. This document addresses many of the concerns associated with PEM construction and manufacturing, primarily the non-hermetic packaging and the supply chain situation of multiple material sets and assembly sites.
CE-12 Solid State Devices	AS6294/4 Requirements for Plastic Encapsulated Semiconductor Devices in Military and Avionics Applications.	Establishes common industry practices, and screening and qualification testing, of plastic encapsulated discrete semiconductors (PEDs) for use in military and avionics application environments. Addresses many of the concerns associated with PED construction and manufacturing, primarily the non-hermetic packaging and the supply chain situation of multiple material sets and assembly sites.
G-19 Counterfeit Electronics Avoidance and Detection	AS5553D - Counterfeit Electrical, Electronic, and Electromechanical (EEE) Parts; Avoidance, Detection, Mitigation, and Disposition.	For use by organizations that procure and/or integrate and/or repair EEE parts and/or assemblies containing such items, including maintenance, repair, and overhaul (MRO) organizations and can be flowed down supply chains through contract to ensure reliability and robustness. It was revised to take into account DFARS 252.246-7008 – Sources of Electronic Parts, to deal with traceability and control throughout the supply chain.

The Open Group

Open Trusted Technology Forum	Open Trusted Technology Provider™ Standard (O-TTPS); Technically equivalent to ISO/IEC 20243	• Set of guidelines, recommendations and requirements that help assure against maliciously tainted and counterfeit products throughout commercial off-the-shelf (COTS) information and communication technology (ICT) product lifecycles. • All phases of a product's life cycle: design, sourcing, build, fulfillment, distribution, sustainment, and disposal • Focuses on verification of the procedures used within the organization to maintain security and integrity of the supply chain,

The Open Trusted Technology Forum provides a collaborative environment to facilitate creating international standards focused on supply chain security to establish a unified view of practicing supply chain risk management (SCRM) for information and communication technology (ICT) products.

OTTF has developed two preeminent international certification programs:

- The Open Trusted Technology Provider ™ Standard (O-TTPS) Certification Program
- Certified Trusted Technology Practitioner (Open CTTP) Professional Certification.

Telecommunications Industry Association (TIA)

TIA QuEST Forum's Supply Chain Security Working Group	SCS 9001: Global Supply Chain Security Standard (Handbook)	SCS 9001 addresses the urgent need for an information and communications technology (ICT) specific standard for global supply chain security. The standard provides guidance for key components of supply chain security: (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.

TIA QuEST Forum Working Groups collaboratively identify best practices and execute key projects and initiatives to address a range of global ICT issues. The Supply Chain Security working group:

- Worked over 24 months to get the document prepared
- SCS 9001 is a process-based standard, built on top of a quality management system (QMS)
- The internal SCS 9001 comment review has been completed with the Integrated Global Quality (IGQ) Working Group
- The document was out for comment review to other specific industry subject matter exerts
- The deadline for all comment inputs was: 26 October 2021
- Comment reviews took place in November
- SCS 9001 Pilot Auditor Training has been conducted with 25 global AB and CB auditors participating
- SCS 9001 pilots are taking place in November and December 2021. Let us know if you're interested in participating.
- SCS 9001 R1.0 is expected to be sent for a full TIQ QuEST Forum vote in December 2021

Other Activities Identified

- Accellera
- Alliance for Telecommunications Industry Solutions (ATIS)
- National Institute of Standards and Technology (NIST)
- Open Compute Project (OCP)
- RISC-V International
- Silicon Integration Initiative (Si2)
- Transported Asset Protection Association (TAPA)
- Unified Extensible Firmware Interface Forum (UEFI)

**Require SME evaluation for applicability*

Takeaways

- Several standards organizations are developing related standards.
- Collectively, there is a toolbox industry and government can leverage.
- No commonly agreed upon 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.
- Workshop discussions will likely identify other useful documents.
- 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