NDIA

Electronics Division

2101 Wilson Boulevard, Suite 700, Arlington, VA 22201-3060 • (703) 522-1820 • NDIA.org

Clear Demand Signal Needed for CHIPS Success

White Paper

July 2025

Authors

Mike Fritze
Dan DiMase
Jim Will

Members of the Electronics Division reviewed this paper prior to its publication. For more information about the Electronics Division, including a list of upcoming events, please visit **NDIA.org/Divisions/Electronics**

The Creating Helpful Incentives to Produce Semiconductors (CHIPS) and Science Act[1] funding was a critical first step in providing incentives to advance secure domestic and allied microelectronics supply capabilities. CHIPS represents the single largest USG investment in semiconductors since the Sematech consortium in the 90s. $52B is being committed over five years to both stimulate domestic production facilities ($39B) and create a robust and sustainable R&D effort ($11B). With all the new infrastructure and capability coming online ***it will be important that they are commercially sustainable for the program to succeed***.

However, CHIPS only addresses the supply side of the ecosystem. It does not create demand. In order to drive new demand into more secure domestic fabrication facilities, clear market preferences must be established. This can take the form of mandating an assured supply chain for defense and all types of critical infrastructure applications, such as power grids, water, banking, healthcare, automotive, transportation, etc. To enable such a mandate, a practical set of multi-tiered assurance standards for microelectronics must first be established. The most effective approach is a collaborative engagement where the Government enables and provides advice to an Industry-led coalition. This is a key step to enable companies as stakeholders to monetize enhanced assurance practice (at a higher cost) which is becoming more important today.

At the same time, Congressional requirements have been mandated for assured microelectronics including Fiscal Year 2020 National Defense Authorization Act section 224 "Requiring Defense microelectronics products and services meet trusted supply chain and operational security standards"[2] and Fiscal Year 2023 National Defense Authorization Act section 5949 "Prohibition on certain semiconductor products and services"[3] (including supply chain traceability and assurance aspects***). To successfully achieve the NDAA mandates, it is imperative that participants in the global microelectronics supply chain establish an infrastructure for measuring assurance, tracking provenance, enabling supply chain traceability, and establishing a strategy for market preference for assured supply, market access, and end-market use.***

Domestic sources are more costly compared to less secure equivalents so compelling business reasons to utilize them are critical to counter our adversary's objective to dominate the microelectronics market by undercutting costs for assured supply. Thus, clear demand signals to drive utilization of new domestic capabilities are critical for economic security and to establish a business model on which domestic suppliers can succeed.

How Microelectronics Assurance Standards Can Help Establish a Clear Demand Signal

As discussed above, mandating increased supply chain assurance is best accomplished via the use of a set of multi-tiered assurance standards. Lower tiers would be less complex and expensive to implement, while higher tiers would be more complex and expensive, as expected. The applicable tier will depend on the specific application of the component or system. Although there have been efforts in this direction, such as Microelectronics Quantifiable Assurance, no such standards currently exist[4]. It is important that the USG does not act unilaterally but collaborates very closely with industry to develop such a set of practically implementable assurance standards. The government's most effective role is to convene and advise commercial stakeholders, while enabling an industry coalition to lead this effort.

Once such a set of assurance standards is developed, the USG could mandate increased assurance for microelectronics supply to critical infrastructure. Critical infrastructure represents a much larger assurance-conscious market compared to only the DoD, which is only 1% of the commercial market.[5] Not only is this an important way to help drive demand for more secure (and expensive) domestic microelectronic sources being developed by CHIPS, the assurance standards can address demand to critical microelectronic and electronic packaging infrastructure as result of investments by DoD's Manufacturing Capability Expansion and Investment Prioritization (MCEIP) office in on-shore PCB, substrates, and uHDI technology.

1 https://www.congress.gov/bill/117th-congress/house-bill/4346

2 https://www.congress.gov/116/plaws/publ92/PLAW-116publ92.pdf

3 https://www.congress.gov/bill/117th-congress/house-bill/7776/text

4 https://apps.dtic.mil/sti/trecms/pdf/AD1208000.pdf

5 https://www.businessdefense.gov/docs/resources/FY2021-Industrial-Capabilities-Report-to-Congress.pdf

Development of Industry-Based Microelectronics Assurance Standards is Foundational to Business Success and Customer Value

Standards are an important basis on which many successful businesses that provide products and services operate. They specify fundamental requirements that are woven into the operation model in order to ensure value to the customer base and mitigate business risks, including an assured supply chain. There are competitive advantages and strategic benefits for suppliers and manufacturers to participate in the standards development to advocate for their organization and their customers' best interests, including the feasibility of requirements aligning with the organization's goals and initiatives. At the end of the day, such standards must have broad industry acceptance and be straightforward to implement to succeed in adoption by industry. Given the current focus on microelectronics supply chain assurance, along with geopolitical concerns, the development of such standards is a high priority.

Industry has Adopted Assurance Standards We Need to Build on for Microelectronics

The standards foundation exists, but the need now is to formalize a coalition of government and industry stakeholders to collaborate in establishing a common, tiered set of assurance standards. There are several industry organizations that have been, or are in the process of, developing standards to address topics like cyber-physical systems security, hardware and software assurance, provenance, traceability, and supply chain risk management. Government organizations, such as NIST, are actively engaging industry to understand assured supply chain needs, while DoD has long established the Trusted Foundry program for secure microelectronics access. Additional details can be found in Appendix 1.

For instance, IPC -1791 Qualified Manufacturers Listing (QML),[6] released in August 2018 as the result of an industry lead effort, outlines the minimum requirements, policies, and procedures for printed circuit board design, fabrication, assembly, and cable and wire harness assembly as part of method to provide secure products and services for DoD and other markets. Management and Mitigation of Cybersecurity Incidents in the Manufacturing Industry Supply Chain requirements are specified in IPC-1792.[7] IPC-1782 Standard for Manufacturing and Supply Chain Traceability of Electronic Products[8] establishes the minimum requirements for manufacturing and supply chain traceability and IPC-1783 International Standard for Component-Level Authentication,[9] which is under development, establishes methodology for absolute material authentication and manufacturing process provenance.

The SAE G-32 Cyber Physical Systems Security team published a joint aerospace and automotive standard, JA7496, Cyber Physical Security Engineering Plan.[10] This standard establishes practices for managing risk and ensuring the security of a cyber-physical system and addresses broad industry use, for both commercial and defense applications, along with other high-reliability/critical systems.

And NIST published IR 8419,[11] in April 2022, to catalyze the understanding of traceability in manufacturing supply chains as an ecosystem-wide concern, and to recommend directions of future research in manufacturing supply chain traceability, enabled by blockchain and related technologies. NIST also released an initial public draft in September 2024, NIST IR 8536, "Supply Chain Traceability: Manufacturing Meta-Framework," that presents a comprehensive framework designed to enhance traceability across manufacturing supply chains.

DoD's Trusted Foundry Program[12] was established to provide a means to assure integrity and confidentiality for integrated circuits, from design to packaging and test. Trusted sources provide an assured chain of custody, prevent access to mitigate modification/tampering, and protect from attempts to reverse engineer or analyze for vulnerabilities.

6 https://www.ipc.org/TOC/IPC-1791D-TOC.pdf

7 https://www.ipc.org/TOC/IPC-1792_TOC.pdf

8 https://www.ipc.org/TOC/IPC-1782B_TOC.pdf

9 https://www.ipc.org/solutions/ipc-factory-future

10 https://www.sae.org/standards/content/ja7496_202206/

11 https://csrc.nist.gov/pubs/ir/8419/final

12 https://www.acq.osd.mil/asds/dmea/tapo/trusted-supplier-programs.html

The Cost of not Taking Action

The cost for not taking action, simply put, promotes the status quo, including the supply of very low-priced, less assured parts from adversarial sources, undercutting domestic suppliers. This worsens the current situation where such components are supplied to systems that protect our national security and ensure the operation of critical infrastructure.[13] **This is an untenable outcome for which the major CHIPS Program was designed to address.**

Domestic sources capable of supplying assured components will fail in competition with low-priced alternatives, diminishing the return on CHIPS and other investments. We need clear demand drivers.

Proposed Plan of Action

We anticipate that a multi-step approach will be required to accomplish the following:

1. Form a coalition of Industry, Industry Association, and USG stakeholders, led by a council comprised of Industry Association leads
2. Develop a tiered set of assurance standards vetted by Industry and Government
3. Promulgate with USG Policy stakeholders (i.e. DOC, DoD, DOE, DHS, etc.)
4. Formalize assurance standards within a clearly responsible and defined group of organizations, including the process to certify
5. Revise policy guidance and acquisition requirements to mandate assurance standards by USG Organizations

The objective is to mandate the use of newly developed assurance standards for critical infrastructure and national security. In this way, a new market driver is created for the more expensive domestic microelectronics capabilities CHIPS is developing.

This is an urgent call to action that begins with assembling a coalition of key stakeholders from Industry and Government to address assurance standards. Such standards will then be used to mandate improved assurance for DoD and Critical Infrastructure applications.

13 https://www.forbes.com/sites/erictegler/2024/01/09/americas-carriers-rely-on-chinese-chips-our-depleted-munitions-too/

Clear Demand Signal Needed for CHIPS Success

Appendix 1 - Assurance Standards Reference

Industry Standards Addressing Microelectronics Assurance and Traceability

Published | In Development | Gap (Proposed)

	PPP/CPI	Design	Verify	Mask	Fabrication	Packaging & Test	V&V	Config & SW	Distribution	Integrate & Test	Operations & Maintenance
Cyber Physical Systems Security	JA7496 - Cyber-Physical Systems Security Engineering Plan[1] Note - Rev. A in progress [1]References 100's of cross-sector standards not uniformly adopted and used										
	JA7496 Compliance Standard or Guide (includes Audit Checklist)										
	NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations										
	NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations										
	ISO/IEC 27001 Information security, cybersecurity and privacy protection — Information security management systems — Requirements										
	NIST Cybersecurity Framework (CSF)										
SwA	JA6678 - Cyber Physical Systems Security Software Assurance										
	JA6678 Compliance Standard or Guide (includes Audit Checklist)										
								JA6678/1 Config & SW/Integration SwA Standard			
								JA6678/1 Compliance Standard or Guide (includes Audit Checklist)			
HwA	JA6801 - Cyber Physical Systems Security Hardware Assurance										
	JA6801 Compliance Standard or Guide (includes Audit Checklist)										
	JA6801/1 Design & Verify HwA Standard			JA6801/2 Mask & Fab HwA Standard		JA6801/3 Packaging & Test/V&V HwA Standard				IPC-1791 Trusted Electronic Designer, Fabricator, and Assembler Requirements	
	JA6801/1 Compliance Standard or Guide (includes Audit Checklist)			JA6801/2 Compliance Standard or Guide (includes Audit Checklist)		JA6801/3 Compliance Standard or Guide (includes Audit Checklist)				IPC-1791 Certification Scheme offered by IPC	
	JA7151 Netlist Analysis Techniques for HwA										
Traceability					IPC-1782 - Standard for Manufacturing / Supply Chain Traceability of Electronic Products						
					SEMI E142 Specification for Substrate Mapping						
	SEMI 6504 - Specification for Electronic Supply Chain Traceability Using Distributed Ledger Technology										
	IPC-1783 - International Standard for Component-Level Authentication										
					SAE J3327 Surface Vehicle EV Battery Global Traceability						
					SEMI T17 Specification of Substrate Traceability						
					SEMI T18 Specification for Traceability of Materials to the Source Used in Semiconductor Manufacturing						
					SEMI T21 Specification for Organization Identification by Digital Certificate Issued from Certificate Service Body (CSB) for Anti-Counterfeiting Traceability in Components Supply Chain						
					SEMI T22 Specification for Traceability by Self Authentication Service Body and Authentication Service Body						
	SEMI T23 Specification for Single Device Traceability for the Supply Chain										
					SEMI T25 Specification for Blockchain for Semiconductor Supply Chain Traceability						
	NIST IR 8536 Supply Chain Traceability: Manufacturing Meta-Framework										
Counterfeit Avoidance & Detection	Anti-Counterfeit (preemptive controls) for Design & Verify			JESD243 - Counterfeit Electronic Parts: Non-Proliferation For Manufacturers		Anti-Counterfeit Mechanisms for Packaging		AS6171 - Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts and specific test method slash sheets	AS6496 Fraudulent/ Counterfeit Electronic Parts... Authorized/ Franchised Distribution AS6081 Fraudulent/ Counterfeit Electronic Parts... Distributors	AS5553 - Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition AS6174 - Counterfeit Materiel; Assuring Acquisition of Authentic and Conforming Materiel	
					SEMI T20 Specification for Authentication of Semiconductors and Related Products						

Industry Standard Activity by Organization

Organization Name	Focus, Purpose	Connection, Strategy, Communications, Outreach
SAE G-32 Committees	SAE G-32 CPSS Committee and all subcommittees will develop and maintain technical documents (Standards, Handbooks, Recommended Practices, and Information Reports) to further CPSS including analyses of the systems operating. Though the G-32 committee is chartered under the SAE Aerospace Council's authority, its documents are intended for broad industry use (commercial, defense, and other high-reliability and/or critical systems in aerospace, transportation, medical, etc.). Stds for CPSSEP, SwA, and HwA from all areas of the supply chain and a broad range of industries for electronic components and systems.	SAE G-32 utilizes and coordinates the knowledge, experience, and skills of technical experts in the field of CPSS to: 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 and mitigating impacts. 6. Develop validation and verification methods to ensure requirements are addressed
NDIA (Trust and Assurance Committee)	The National Defense Industrial Association drives strategic dialogue in national security by identifying key issues and leveraging the knowledge and experience of its military, government, industry, and academic members to address them. The mission of the Electronics Division is to lead the evaluation of current and future challenges and to develop proposed solutions to address them, enabling the U.S. government and industry to access and provide trusted and assured electronics.	Focus on trust and assurance within the Electronics Division, in national defense issues. Engagement includes whitepaper support & subcommittee support, such as with the Zero Trust and Provenance & Traceability for Assured and Preferred Supply white papers.
MITRE (the HW SIG)	Works in the public interest across federal, state, and local governments, as well as industry and academia. MITRE brings innovative ideas into existence in areas as varied as artificial intelligence, intuitive data science, quantum information science, health informatics, space security, policy and economic expertise, trustworthy autonomy, cyber threat sharing, and cyber resilience.	Maintains CWE/CVE data, etc. To incorporate data into std work and tools
IPC (committee 2-19A and 2-19C)	A new work in process, IPC-1782 and IPC-1783 establish the methodology for the absolute authentication and provenance of all materials, ranging from singular components, bulk materials, and composite products, using immutable unique identification. IPC-1782 establishes the minimum requirements for manufacturing and supply chain traceability based on risk, IPC-1783 mandates requirements for the associated secure information technology infrastructure, ensuring privacy, while enabling interoperability between process provenance cluster data for immutable supply chain traceability. IPC-1792 is the standard for the management and mitigation of cybersecurity incidents in the manufacturing industry supply chain.	Stds related to integrators/assemblers. Current focus on traceability and component authentication. Promoting a "public domain" blockchain for interoperability across the supply chain.

Organization Name	Focus, Purpose	Connection, Strategy, Communications, Outreach
Other SAE Committees (CE-12, G-31, G-19, TEVEES18A "Vehicle Cybersecurity Systems Engineering Committee", etc.)	Solutions to technical problems in the application, standardization, and reliability of solid-state devices, counterfeit prevention, blockchain solutions, cybersecurity assurance from the perspective of the automotive industry, and others. This is intended to find synergistic opportunities to align with other industry standards that are already working on different aspects of the overall problem.	Stds for parts management, counterfeit prevention, blockchain use for traceability, pedigree, provenance tracking, engineering requirements for cybersecurity risk management of electrical and electronic (E/E) systems in road vehicles, etc.
JEDEC JC-14	Stds for the microelectronics industry, manufacturers, and suppliers together to create standards to ensure product quality, reliability, and interoperability. Particularly work in component traceability documentation through distribution channels. Largest Stds organization for semiconductor manufacturers/designers.	Standardizing quality and reliability methodologies for solid-state products used in commercial applications such as computers, automobiles, telecommunications equipment, etc. It also includes developing standards for board-level reliability of solid-state products used in commercial equipment.
SEMI	Stds related to fab operations, traceability, etc. Need for collaboration with other groups on traceability (such as E142, 6504, and 6506). Topics include traceability for fab and packaging products (wafers, frames, strips, and trays), external traceability, and a specification for cybersecurity of fab equipment. Global industry association representing the electronics manufacturing and design supply chain, connecting over 2,400 member companies and 1.3 million professionals worldwide.	Programs, communities, initiatives, market research, and advocacy, SEMI informs and coordinates its members and the industry, cultivates collaboration, drives action, and synchronizes innovation.
NIST	NIST NCCoE Blockchain Community of Interest (COI). Technology, measurement, and standards through labs and other work to provide for a measurement infrastructure supporting all industries.	Provides various projects and resources used extensively by various standards organizations. Technology, measurement, and standards provided by the National Institute of Standards and Technology that empower and facilitate many industries from electric power grid and electronic health records to atomic clocks, advanced nanomaterials, and computer chips, with innumerable products and services. The NIST glossary by itself has greatly streamlined the standards work.
IEEE	Stds for various technical areas with very broad industry use. Cyber privacy and stds committee (IEEE 1619.1-2018). Essential to the global technical community and to technical professionals everywhere and universally recognized for the contributions of technology and of technical professionals in improving global conditions. Trusted source of technical knowledge-sharing and educational resources, many related directly to the cyber physical security topics.	Probably the world's largest forum for publications, papers, and communications on related technical issues. Forum for broad communication of issues, positions, and approaches.
The Open Group	A global consortium that enables the achievement of business objectives through technology standards. Our diverse membership of more than 900 organizations includes customers, systems and solutions suppliers, tool vendors, integrators, academics, and consultants across multiple industries. Created the Open Trusted Technology Provider Standard (O-TTPS) cybersecurity and supply chain integrity standard.	Mitigation of maliciously tainted and counterfeit products, and assessment procedures for this scope.

The National Defense Industrial Association is the trusted leader in defense and national security associations. As a 501(c)(3) corporate and individual membership association, NDIA engages thoughtful and innovative leaders to exchange ideas, information, and capabilities that lead to the development of the best policies, practices, products, and technologies to ensure the safety and security of our nation. NDIA's membership embodies the full spectrum of corporate, government, academic, and individual stakeholders who form a vigorous, responsive, and collaborative community in support of defense and national security. For more than 100 years, NDIA and its predecessor organizations have been at the heart of the mission by dedicating their time, expertise, and energy to ensuring our warfighters have the best training, equipment, and support. For more information, visit **NDIA.org**