Comments of the
Semiconductor Industry Association

On

NIST Internal Report NIST IR 8536 2pd
Supply Chain Traceability: Manufacturing Meta-Framework

October 3, 2025

The Semiconductor Industry Association (SIA) appreciates the opportunity to comment on the draft NIST IR 8536 2pd, Supply Chain Traceability: Manufacturing Meta-Framework Second Public Draft (the "Framework" or "NIST IR 8536").

I. INTRODUCTION & BACKGROUND

SIA has been the voice of the U.S. semiconductor industry for nearly half a century. Our member companies, representing more than 99 percent of the U.S. semiconductor industry by revenue, as well as major non-U.S. chip firms, are engaged in the full range of research, design, manufacture, and back-end assembly, test, and packaging of semiconductors. SIA's members design and produce all major advanced and mature-node semiconductor types, including logic, memory, analog, microprocessors, and optoelectronics. More information about SIA and the semiconductor industry is available at www.semiconductors.org.

SIA shares the Trump Administration's goal of manufacturing critical technologies in the United States. SIA member companies have announced more than $600 billion (and counting) in private investments to manufacture and develop semiconductors in the U.S., with over 130 projects across 28 states. These projects will create and support over 500,000 American jobs.

Strengthening and securing U.S. semiconductor supply chains is a top priority for SIA and our member companies in our efforts to support U.S. economic and national security, and to maintain global technological leadership. We have been pleased to partner with NIST and other U.S. government agencies on various efforts to advance American semiconductor supply chain security and competitiveness over the years.

SIA is encouraged by Executive Order 14267[1] and the Trump Administration's efforts to avoid onerous and unnecessary regulations in favor of smart regulation as a means of unleashing American innovation and manufacturing. In an increasingly competitive global marketplace – where SIA member companies face non-market competition and price undercutting from foreign players that receive significant supply-side and demand-side support from their government – we

[1] White House, "Reducing Anti-Competitive Regulatory Barriers," Executive Order 14267, April 9, 2025. https://www.federalregister.gov/documents/2025/04/15/2025-06463/reducing-anti-competitive-regulatory-barriers

encourage NIST to avoid advancing even well-meaning efforts that could increase requirements and related compliance costs for SIA member companies and undercut their ability to compete and win globally.

II. THE SEMICONDUCTOR SUPPLY CHAIN

The global semiconductor supply chain is highly specialized, dispersed, and complex – from semiconductor design and manufacturing (both front-end wafer fabrication and back-end assembly, test, packaging) to semiconductor manufacturing equipment and upstream materials necessary for chip production.[2] Specialization across the supply chain allows for the deep focus required to innovate the next chip that will power the technology of tomorrow. There are more than 30 types of semiconductor product categories, each optimized for a particular function in an electronic subsystem.

Creating a single wafer spans continents with thousands of individual suppliers. Chip fabrication requires as many as 300 different inputs, including raw wafers, commodity chemicals, specialty chemicals, and bulk gases. These inputs are processed by more than 50 classes of highly engineered precision equipment. Most of this equipment, such as lithography and metrology tools, incorporates hundreds of technology subsystems such as modules, lasers, mechatronics, control ships, and optics. The highly specialized supplies involved in semiconductor design and fabrication are often based in different countries and a chip itself can cross up to seven international borders in the manufacturing process.

Not only is the semiconductor supply chain complex, but semiconductor content in everyday electronic products, home appliances, and industrial machinery continues to grow significantly, driven by increasing electrification and digitization across end markets. According to one research consultancy, semiconductor content in electronic systems reached 33.2% in 2021.[3] Nearly 50% of all medical devices now contain semiconductor content, spanning insulin pumps to pacemakers to MRI machines. In the automotive industry, S&P AutoTechInsight projected that the average semiconductor content per vehicle will increase 80% over the next seven years from $854 in 2022 to $1,542 in 2029.[4] Electric vehicles demand far more semiconductors, with some models containing up to 8,000.[5] The aerospace and defense industries are also highly dependent

---

[2] For a more fulsome explanation of the semiconductor supply chain and production ecosystem, see SIA and Boston Consulting Group, "Strengthening the Global Semiconductor Supply Chain in an Uncertain Era," April 2021. https://www.semiconductors.org/wp-content/uploads/2021/05/BCG-x-SIA-Strengthening-the-Global-Semiconductor-Value-Chain-April-2021_1.pdf;
SIA and Boston Consulting Group, "Emerging Resilience in the Semiconductor Supply Chain," May 2024. https://www.semiconductors.org/wp-content/uploads/2024/05/Report_Emerging-Resilience-in-the-Semiconductor-Supply-Chain.pdf

[3] Jessie Shen, "Semi content in electronic systems reaches record high in 2021, says IC Insights," DIGITIMES, January 17, 2022. https://www.digitimes.com/news/a20220114VL201.html.

[4] S&P Global, "Automotive Semiconductor Market Tracker – January 2023," AutoTechInsight, March 2, 2023. https://autotechinsight.spglobal.com/shop/product/5003356/automotive-semiconductor-market-tracker-january-2023; "Automotive lone bright spot," Semiconductor Intelligence, March 28, 2023. https://www.semiconductorintelligence.com/automotive-lone-bright-spot/.

[5] Audi MediaCenter, "Semiconductors are Becoming the Neurons of Our Cars," June 14, 2024. https://www.audi-mediacenter.com/en/press-releases/semiconductors-are-becoming-the-neurons-of-our-cars-16053.

on semiconductors, from so-called "legacy" or mature-node chips to the most advanced AI processors.

With this significant growth in semiconductor content across many end markets, the total number of stock keeping units, or SKUs, active across the industry today continues to grow, involving an immense volume of data that would need to be tracked and stored securely for provenance verification and reporting. The logistical challenges of collecting and tracking this data should be a key consideration informing any traceability and provenance framework put forward, as should the competitive impacts of sharing such information with customers and competitors.

III. GENERAL COMMENTS

We have carefully reviewed NIST's Supply Chain Traceability: Manufacturing Meta-Framework draft and offer the following comments on behalf of the semiconductor industry in the U.S.

As a general matter, while NIST IR 8536 is presented as an industry and technology agnostic approach to traceability, we note the document features the microelectronics industry as the primary use case for the traceability framework outlined in the document. In fact, the initial draft proposed framework was presented at a NIST workshop entitled "Trust and Provenance in the Semiconductor Supply Chain Workshop" in April 2025, leading us to conclude that NIST intends for the framework to be adopted by the semiconductor industry in the U.S., as well as by downstream semiconductor-consuming industries. [6]

NIST IR8536 also attempts to address traceability and data management challenges internal to a company. Companies should be free to structure their internal traceability systems and operations tailored to their specific business model and needs. A more practical framework would focus on a voluntary and adaptable external traceability model that does not collect and store sensitive data in a central repository.

Finally, we note that SIA has previously raised concerns with respect to many of the proposed approaches outlined in NIST IR 8536 that were similarly proposed in other regulatory contexts, namely Federal Acquisition Regulation ("FAR") Case 2023-008 titled *Prohibition on Certain Semiconductor Products and Services,* 89 Fed. Reg. 36738 (May 3, 2024)[7] and *Securing the Information and Communications Technology and Services supply Chain: Connected Vehicles*[8] rule (i.e., proposed ICTS Rule).

---

[6] National Institute of Standards and Technology, *Trust and Provenance in the Semiconductor Supply Chain Workshop* (Rockville, MD), April 15, 2025. https://csrc.nist.gov/Events/2025/trusted-semiconductor-supply-chain-workshop.

[7] U.S. Department of Defense, General Services Administration, and National Aeronautics and Space Administration, "Federal Acquisition Regulation: Prohibition on Certain Semiconductor Products and Services," *Federal Register*, May 3, 2024. https://www.federalregister.gov/documents/2024/05/03/2024-08735/federal-acquisition-regulation-prohibition-on-certain-semiconductor-products-and-services

[8] U.S. Department of Commerce Bureau of Industry and Security, "Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles," *Federal Register*, January 16, 2025. https://www.federalregister.gov/documents/2025/01/16/2025-00592/securing-the-information-and-communications-technology-and-services-supply-chain-connected-vehicles

Comment III.A: The Framework laid out in NIST IR 8536 does not account for the complexity of semiconductor supply chains.

The Framework provides a very generalized overview of critical infrastructure supply chains, using microelectronics (semiconductors) as a use case for the initial upstream input. It assumes that all of a company's suppliers are seamlessly integrated within the company's control and ecosystem and can track records in real time for each supplier. NIST IR 8536 assumes there is already an established alignment across the customer/supplier ecosystems, when in reality suppliers work independently with their customers. As outlined in section II, the semiconductor production process is complex, as are the sales and distribution channels.

We question whether the draft sufficiently takes into account the semiconductor industry's complexity, as the Framework omits key stakeholders in the supply chain. Specifically, NIST IR 8536 omits the fabless business model —companies that design but do not manufacture chips— and does not account for the role of contract manufacturing or sales distribution channels in the chip supply chain and sales market. It is not always the case that finished chips are sold directly to an original equipment/device manufacturer (OEM/ODM). The general process laid out in Figure 1 of the Framework assumes a chip manufacturer is the ultimate seller of a chip to an ODM or OEM; this is not the case for fabless companies that rely on foundries and OSATs to manufacture the chips they design, or for manufacturers that sell chips through a distribution channel.

COMMENT III.B: The proposed collection and sharing of provenance data is burdensome and creates risks to proprietary and business confidential information, including the risk of malicious modification.

The government previously proposed a requirement for semiconductor companies to share supply chain or "provenance" data with certain customers —in this case government contractors— to allow the government to validate those customers' compliance with requirements outlined in Section 5949(h) of the FY2023 National Defense Authorization Act (NDAA). In SIA's comments in response to the advanced notice of proposed rulemaking to implement Section 5949 via Federal Acquisition Regulation (FAR) Case 2023-008, we conveyed that such data collection and sharing requirements would be overly burdensome and could create a precedent for future rulemakings.[9] Similarly, in response to the Commerce Department's proposed ICTS rule for connected vehicles, SIA underscored that proposed requirements for companies to share a hardware bill of materials in order to comply with that rule would have posed risks to proprietary and business confidential information.[10] We have the same concerns with respect to NIST IR 8536. It should be noted that the Commerce Department dropped the proposed provenance data reporting requirements (i.e., hardware bill of materials) from the final

[9] Comments of the Semiconductor Industry Association (SIA) on "Prohibition on Certain Semiconductor Products and Services," August 2024. https://www.semiconductors.org/wp-content/uploads/2024/08/SIA-Comments-on-ANPRM-Sec.-5949-FINAL.pdf

[10] Comments of the Semiconductor Industry Association (SIA) on "Securing the Information and Communications Technology and Services supply Chain: Connected Vehicles," October 2024. https://www.semiconductors.org/wp-content/uploads/2024/10/SIA-Comments-Proposed-CV-Rule-FINAL.pdf

ICTS rule on connected vehicles based on industry feedback and instead requires a Declaration of Conformity.[11]

As we outlined in our responses to the rulemakings referenced above, required sharing of traceability and provenance data with other companies throughout the supply chain (e.g., suppliers, customers, distributors) creates risks to proprietary and business confidential information. Semiconductor companies consider information about their supply chain as sensitive information and IP, including materials suppliers and other vendors. Companies have serious concerns about providing such proprietary information, either to their customers, who may also be their competitors, or to their distributors, who may also work on behalf of their direct competitors. For example, requiring the identification of external vendors and facilities responsible for the design of a semiconductor to a contractor could result in sharing enough information to allow a customer-competitor to "poach" engineers from the semiconductor supplier, with the aim of creating an in-house replacement chip to the one supplied.

In addition, the aggregation of proprietary provenance information introduces considerable information safeguarding issues. Secure IP protection is crucial for U.S. innovators facing trade secret thefts from cross-border misappropriation, corporate espionage, and cyber intrusions. We are concerned the Framework outlined in NIST IR 8536 does not adequately account for how customers might store and safeguard the proprietary and confidential provenance-related information the Framework recommends companies collect throughout the supply chain.

Lastly, while the Framework is intended to serve as a tool for counterfeit prevention, it does not adequately account for risks of malicious modification. Because semiconductor supply chains span multiple companies and jurisdictions, chip-level traceability alone cannot reliably prevent or detect tampering, especially by well-resourced, technically skilled adversaries. Such modifications may degrade or disable intended functionality, introduce data exfiltration features, or trigger unsafe, uncontrolled behavior. Mitigation may include component-level fingerprinting and advanced physical and electrical inspection to verify products against a trusted golden reference. However, these measures are resource-, time-, and cost-intensive and are not practical for broad deployment.

IV. SPECIFIC COMMENTS AND RECOMMENDATIONS

In our general comments above, we note that a more practical framework would focus on a voluntary and adaptable external traceability model that does not collect and store business sensitive data in a central repository. Should NIST proceed with the Framework, we offer the following detailed comments on IR8536.

Comment IV.A. Line 307-308 - The Meta-Framework....enables traceability across diverse manufacturing environments

- Each manufacturing sector across any given supply chain even within the semiconductor ecosystem has its own standards bodies that create sector-specific requirements. Fragmentation in requirements across jurisdictions and industries could hamstring the efficacy of any microelectronic traceability system.

- Recommendation: Ensure any standards remain voluntary, extensible, adaptable; in short, any framework should be flexible enough to accommodate different situations, requirements, and approaches. The system will be more successful if people choose to use it and if they see other people/companies/industries using it.

Comment IV.B. Line 309 - The Meta-Framework....allow[s] authorized stakeholders to discover, retrieve, and interpret supply chain event data.

- Data ownership and asset ownership are two different things. The point of a traceability system is to link an asset to information about that asset. The data owner owns the data and sets the terms under which the data is provided to the asset owner. Whoever wants data from the data owner must be legitimized/authorized to access data from the data owner. The only function of a traceability system should be creating and storing links between the asset and the information repository. Data should not be stored in a traceability system. Rather, a traceability system should provide links between the asset and the data controlled by the data owner. There is a risk that actors could seek to "mine" the traceability system to do market analysis or gain intelligence on competitors or adversaries.

- Recommendation: We agree "authorized stakeholders" are key, and finding ways to limit access is important. The type of query that can be made to a traceability system should be limited. For example, bulk queries of X company parts to build a map of X company's sales volume, suppliers, and customers should be treated with care.

Comment IV.C. Lines 310-316 - The Meta-Framework provides a structured approach to supply chain traceability, enabling interoperable and secure data exchange between organizations.

Line 338-352 – A major barrier…

- The traceability system should not try to solve internal traceability or data management within any single company. Every organization/company has their own unique blend of systems, databases, software, practices, specs, and procedures tailored to their needs and business.

- Companies need to be able to effectively link to the external traceability system for incoming goods, create a bridge from incoming materials to outgoing materials, and to link to the external traceability system for outgoing materials.

- Recommendation: NIST should facilitate secure data exchange between organizations but not mandate internal data exchange patterns. It is important to provide good external traceability with a well-defined interface such that companies can link their internal traceability to the external traceability system.

Comment IV.E. Line 592 - Table 1, Tracked Entity Data & Supplemental Data

- Trying to store sensitive, potentially proprietary data about a company's assets in this system will be a non-starter for companies. Storing all this data would also make the system unwieldy and non-functional for many or all use cases.

- Recommendation: This should not be included in a traceability system. Rather than storing data in this system, the system should retain links to data sources.

Comment IV.F. Line 599 - Table 2 - Make and Assemble records

- This is not a record of the manufacturing process; the record of manufacturing would be dealt with in internal traceability systems. This should focus on tracking assets through the supply chain as an external traceability record.

Comment IV.G. Line 684-693 "Controlled Access and Authentication"

- Recommendation: Create limitations on the number of queries, who can make queries, and what items may be queried.

Comment IV. H. Lines 1252-55 – D.2. Additional Supply Chain Traceability Record Subclasses

- Recommendation: The processes described in the table for "Process / Convert", "Split", and "Modify" should be left to each manufacturer and to the realm of internal traceability. This section and embedded table ("Candidate New Supply Chain Traceability Record Subclasses") should be deleted.

IV CONCLUSION

While we appreciate NIST's well-intended efforts to develop the proposed supply chain traceability Framework for manufacturing outlined in NIST IR 8536, we are concerned that this effort will lead to additional burdensome data-collection requirements and resource drain on semiconductor companies in the U.S. We encourage NIST to approach this and its other semiconductor-focused workstreams within the spirit of the President's deregulation agenda, embodied in Executive Order 14267 on Reducing Anti-Competitive Regulatory Barriers.[12]

SIA appreciates the opportunity to provide these comments and is available to provide additional information or assistance as NIST may require. If you have any additional questions or would like to discuss these comments further, please contact SIA via jkellon@semiconductors.org.

[12] NIST, "Cybersecurity Framework Profile for Semiconductor Manufacturing," https://www.nccoe.nist.gov/projects/cybersecurity-framework-profile-semiconductor-manufacturing; SIA comments, https://www.semiconductors.org/wp-content/uploads/2025/09/SIA-Comments-on-NIST-IR-8546.pdf