SEMICONDUCTOR INDUSTRY ASSOCIATION

Via Regulatory Portal

Re: Federal Acquisition Regulation (FAR) Case 2023-008: Comments on Advanced Notice of Proposed Rulemaking, *Prohibition on Certain Semiconductor Products and Services*

Dear Mr. Clark:

The Semiconductor Industry Association ("SIA") welcomes the opportunity to provide written comments to the U.S. Department of Defense ("DOD"), the U.S. General Services Administration, and the National Aeronautics and Space Administration (collectively, the "FAR Council") on the Advanced Notice of Proposed Rulemaking ("ANPRM") titled *Prohibition on Certain Semiconductor Products and Services*, 89 Fed. Reg. 36738 (May 3, 2024) (the "ANPRM" or "Proposed Rule"). SIA shares the U.S. Government's goals of bolstering the U.S. semiconductor ecosystem, promoting resilient and reliable supply chains, and creating new opportunities for U.S. companies, products, and workers.

The semiconductor industry is critical to U.S. economic competitiveness and national security in an era of digital transformation, artificial intelligence, Industry 4.0, connected vehicles, and 5G/6G communications. Against the backdrop of global technology competition and complex geopolitical dynamics, strengthening American and global semiconductor supply chains is a top priority for SIA and its members. Our association and its member companies have been supporting and working closely with government for more than three decades to help improve the government's understanding of our sector and the issues that drive its success. Collaboration and two-way information sharing between government and industry will be critical in successfully achieving shared supply chain objectives related to the semiconductor industry, and we look forward to a robust public-private partnership on these issues going forward.

I. INTRODUCTION AND BACKGROUND

SIA has been the voice of the U.S. semiconductor industry for over 45 years. SIA member companies represent more than 99% of the U.S. semiconductor industry by revenue and are engaged in the cutting-edge research, design, and manufacture of semiconductors. The U.S. is a global leader in the semiconductor industry. We strongly believe continued U.S. leadership in semiconductor technology will drive economic strength, national security, and global competitiveness. More information about SIA and the semiconductor industry is available at www.semiconductors.org.

Semiconductors are the bedrock of today's global economy, powering virtually everything digital – from cellphones and cars to supercomputers and medical equipment. They are also critical

components in a host of American technologies and industrial products, including cars, household and kitchen appliances, clean energy, and medical devices. Few industries, if any, have a supply chain and development ecosystem as complex, geographically widespread, and interdependent as the semiconductor industry. A joint report by the Boston Consulting Group and SIA found that more than 120 countries are involved in the semiconductor production supply chain. As these comments will discuss in more detail, the globalized and complex nature of semiconductor supply chains underscores the complexity of the provenance requirements suggested in the ANPRM.

II. THE GLOBAL 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. Different regions of the world have particular strengths at different stages of the value chain, and as underscored by Secretary of State, Antony Blinken, "No one country, including the United States, can produce or onshore everything it needs."

Developing semiconductor designs is similarly complex and global. Chip design is a key activity behind the function and value of a semiconductor device. The design process consists of defining the product requirements for the chip's architecture and system, as well as the physical layout of the chip's individual circuits, which ultimately enable semiconductors to receive, transmit, process, and store ever-increasing amounts of data for today's digital world.

Semiconductor design involves two types of activities: hardware design and software development work. Hardware design is a multistep process encompassing product definition and specification, system design, integrated circuit design, and post-silicon validation. Software development entails the creation of firmware – a type of lower-level software that bypasses (for example) the operating system of an end device, like a laptop, to provide instructions directly to a chip. As chip design grows more complex, it becomes an increasingly iterative process – especially for leading players – with hardware design and software development occurring in parallel in order to identify issues earlier, optimize overall system-level performance, and decrease time to market.

Chip design engineers – most of whom have either a PhD or other advanced degree in engineering – use both new and established techniques in the design process. When driving innovations, designers generate new, highly specialized plans that enable specific applications to leverage the latest advances. These teams working together on the most advanced chip architectures often include many hundreds of engineers working together across the globe, in real time. Designers will often use existing, reusable architectural building blocks (core IP) to simplify and accelerate creation of the overall design. In all cases, designers use electronic design automation ("EDA") software to automate the design process and ensure that chip designs can be manufactured on distinct and often proprietary fabrication processes. Close collaboration with the designer's manufacturing partner reduces delays and prevents errors from becoming embedded in designs that could compromise the performance of the device.

The semiconductor hardware design process consists of four major stages:

- *Product definition and specification:* Product management, system architects, and customer define initial product requirements.
- *Architecture/system design:* System architects define block-level architecture for an integrated circuit design and may leverage previous intellectual property ("IP"). Re-using IP or IP cores can allow for faster design.
- *Integrated circuit design:* Multidisciplinary effort involving logic (initial analog and digital design), circuit (digital synthesis and design for test), and layout (routing and mask generation). This step also includes verification, where engineers verify design functionality and timing through simulation using a "test bench." Verification can generate significant amounts of test data and is time intensive, accounting for as much as half of the time to design a chip.
- *Post-silicon validation:* Engineers validate physical device functionality across extreme working conditions.

Chip design is a highly complex, interdisciplinary process that involves years of research and development ("R&D"), hundreds of millions of dollars of investment, and thousands of engineers often spanning multiple countries.

With respect to semiconductor manufacturing, the process consists of hundreds of steps to produce a single wafer (i.e., a thin, round slice of a semiconductor material varying in size between 6 and 12 inches in diameter). Patterned layers are added on and into the wafer creating interconnected electrically active regions on the surface, ultimately forming the complete semiconductor. An abridged overview of the semiconductor manufacturing supply chain, from mine to fabricator, is as follows:

- *Mining and Refinement of Metallurgical Grade Silicon:* Silicon dioxide, also known as silica (which is found in sand), is mined and refined into metallurgical grade silicon.
- *Polysilicon:* Metallurgical grade silicon is further refined into polysilicon.
- *Ingot Production:* Polysilicon is heated into a molten liquid. In a process similar to repeatedly dipping a wick in wax to make a candle, a small piece of solid silicon (i.e., the "seed") is dipped in molten liquid. As the seed is slowly withdrawn by mechanical means from the melt, the liquid quickly cools to form a single crystal ingot.
- *Blank Wafer Production:* This cylindrical crystal ingot is then ground to a uniform diameter. A diamond saw blade slices the ingot into thin wafers. The cut wafers are then processed through a series of machines where they are ground (optically) smooth and chemically polished.
- *Front-End Wafer Fabrication*: The heart of any semiconductor manufacturing business is the fabrication, where the integrated circuit is formed on the wafer. The fabrication process, which takes place in an environmentally controlled clean room, involves a series of principle repetitive steps.

- *Back-End Wafer Fabrication*: Electrical tests then check the functionality of each chip on the completed wafer, which is then sliced into single chips that are assembled and packaged for delivery to customers.

Creating a single wafer spans continents and requires the participation (directly and indirectly) of thousands of workers. There are thousands of individual suppliers responsible for the complex materials and tools referenced above. Ensuring that such a complex supply chain remains resilient and secure in the face of global challenges requires a multi-pronged effort on the part of the United States.

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.[1] 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.[2] For example, electric vehicles ("EV") and self-driving cars require more semiconductors than conventional automobiles. EVs are generally loaded with about 1,300 semiconductors while Level 4 autonomous cars (i.e., highly autonomous) have more than 3,000 semiconductors. The aerospace and defense industries are also highly dependent 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 reporting. The logistical challenges of tracking this data should be a key consideration informing implementation of requirements.

III. COMMENTS AND RECOMMENDATIONS

SIA commends the FAR Council for the significant work completed to date to implement the Section 5949 requirements. We have carefully reviewed the ANPRM and are pleased to provide these comments to inform how the Government's national security objectives can be accomplished more effectively and without unnecessarily harming the U.S. semiconductor industry.

---

[1] Jessie Shen, "Semi content in electronic systems reaches record high in 2021, says IC Insights," DIGITIMES (Jan. 17, 2022), *available at* https://www.digitimes.com/news/a20220114VL201.html.

[2] Automotive Semiconductor Market Tracker – January 2023 (Mar. 2, 2023), *available at* https://autotechinsight.ihsmarkit.com/shop/product/5003356/automotive-semiconductor-market-tracker-january-2023; *see also* "Automotive lone bright spot," Semiconductor Intelligence (Mar. 28, 2023), *available at* https://www.semiconductorintelligence.com/automotive-lone-bright-spot/.

Section A contains general comments on the ANPRM, with a particular focus on the broad provenance requirements suggested in Section H of the ANPRM. **Section B** contains our responses to the specific questions posed to industry in the ANPRM.

A. General Comments on the ANPRM

Section H of the ANPRM indicates that the FAR Council is "considering requiring offerors to identify the provenance of the supply chain for the semiconductor components for each electronic product provided to the Government." Required provenance information could include the "identification of vendors and facilities responsible for the design, fabrication, assembly, packaging, and test of the product, manufacturer codes used for the product, and distributor codes used for the product," among other things.

As described in Section II above, electronic products typically include numerous semiconductors sourced through an extraordinarily complex and globalized supply chain. This makes tracing the provenance of individual components challenging, time-consuming and resource intensive. Given the FAR Council estimates that 75% of awardees will have electronic products or services impacted by this prohibition as well as the likelihood that many affected products may incorporate hundreds if not thousands of semiconductors depending on the end product, SIA submits that it is critical for the proposed rulemaking to consider and mitigate the immense effort necessary to track the provenance of each semiconductor included in an electronic product. SIA would also like to understand the status and timeline for the development of a Government-wide Traceability and Diversification Initiative described in Section 5949(f).

Below we provide our comments with respect to the proposed provenance requirement:

i. ***The collection of provenance information would not provide the Government with greater assurances of compliance than the certifications that Section 5949 requires.*** Section 5949(h) requires implementing regulations to include a number of methods of ensuring compliance with the prohibitions. Specifically, the regulations must require prime contractors to:

   1. Certify to the non-use of covered semiconductor products or services;
   2. Have a means to detect and avoid the use or inclusion of covered semiconductor products or services;[3] and
   3. Bear responsibility for any rework or corrective action that may be required to remedy the use or inclusion of such covered semiconductor products or services in such parts or products.

[3] The ANPRM aligns this to the reasonable inquiry standard, stating that the rule may "[r]equire contractors to conduct a reasonable inquiry to detect and avoid the use or inclusion of covered semiconductor products or services in electronic products and electronic services."

The regulations further require "covered entities" (as defined in the ANPRM) to disclose the inclusion of a covered semiconductor product or service in electronic parts, products, or services included in electronic parts, products, or services to their direct customers.

Contractor certifications have proven to be highly effective tools for ensuring compliance with important government compliance requirements and are widely used. For example, contractors must certify to their provision and use of covered telecommunications equipment or services in compliance with Section 889 of the FY19 NDAA (FAR 52.204-26), present responsibility (FAR 52.209-5), knowledge of child labor for listed end products (FAR 52.222-18), implementation of a compliance plan to prohibit trafficking in persons (FAR 52.222-56), and domestic sourcing requirements (FAR 52.225-2, FAR 52.225-4, FAR 52.225-6). Contractors will also soon be required to certify to compliance with information security requirements in connection with DOD's Cybersecurity Maturity Program and software developers will need to certify to implementation of secure software development practices through the forthcoming CISA Secure Software Attestation Common Form.

These programs are able to effectively rely on contractor certifications because of the severe penalties – including but not limited to cost of rework, re-procurement, or corrective actions – that contractors and lower tier suppliers can face for making misrepresentations, or causing misrepresentations to be made, to the U.S. Government. Ultimately, the provenance information that the Government is considering collecting for verification purposes would be unlikely to provide the Government with any greater assurances than the certifications that are already mandated by Section 5949 since contractors must rely on the accuracy of information from subcontractors and vendors in the federal supply chain in either case.

ii. ***A provenance requirement goes beyond what is required to validate contractor compliance with the Section 5949 prohibitions and risks establishing an unreasonably expansive and burdensome information-sharing precedent.*** The broad supply chain information that would need to be provided under the proposed provenance requirement exceeds the scope of information necessary to confirm that electronic products or electronic services that are provided to the Government do not include covered semiconductor products or services, or do not use electronic products that include covered semiconductor products or services. The proposed requirements could therefore establish a burdensome precedent regarding the type and level of information, particularly regarding proprietary and confidential information, that companies must provide to the U.S. Government pursuant to future rulemakings. In this regard, there is substantial concern that the U.S. Government may seek to mandate that companies provide provenance information down to the sub-component level, to include, for example, the raw materials used to produce the semiconductor wafer.

Overly expansive information-sharing requests could also create burdensome disclosure requirements for companies, particularly those with limited experience in federal contracting. Indeed, such requirements could translate into higher barriers to entry for and small- and medium-sized companies/non-traditional contractors who are seeking new opportunities to sell to Federal agencies and could further drive innovative companies out of the federal marketplace entirely. This could result in increasing costs for the Federal government and place a further strain on the defense industrial base by shrinking the available pool of subcontractors and suppliers, including for DOD.

Finally, SIA members also often struggle to respond to government procurements due to the level of data disclosure required. Because the pool of subcontractors is relatively small, companies are often simultaneously potential competitors ***and*** partners. This in turn leads to strained data sharing and procedures that are onerous for the Federal agencies, such as having subcontractors submit detailed pricing separately so that the prime contractor does not have visibility – this is administratively challenging for both the agency and the prime and leads to a top-level price constructed on incomplete data.

iii. ***The proposed provenance requirement is duplicative of the "reasonable inquiry" obligations outlined under the ANPRM.*** The proposed provenance requirement is duplicative of the planned requirement for contractors to conduct a reasonable inquiry to detect and avoid the use of covered semiconductor products or services in electronic products and services provided to the Government. A requirement for offerors to provide the provenance for every semiconductor included in electronic products or services provided to the Government duplicates and far exceeds the scope of a reasonable inquiry as that phrase is contemplated being defined in the ANPRM and as it is used in other federal supply chain sourcing regimes, such as the Section 889 ban on covered Chinese telecommunications equipment and services.[4]

Additionally, as noted above, the FAR Council is to consider aligning the provenance requirements with existing alternative frameworks, notably the Uyghur Forced Labor Prevention Act ("UFLPA"). However, as it currently functions, the UFLPA's supply chain due diligence, tracing, and management requirements far exceed the more targeted "reasonable inquiry" promulgated in the ANPRM. The references to both the UFLPA and "reasonable inquiry" requirements are inconsistent and therefore will cause considerable confusion amongst industry as to which requirements apply and when. SIA therefore requests that the forthcoming regulations provide additional clarity on the scope of contractors' compliance requirements and do so with the more targeted scope of the reasonable inquiry in mind.

[4] Describing a "reasonable inquiry" as "an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity. A reasonable inquiry need not include an internal or third-party audit." 85 Fed. Reg. 42665 (Aug. 13, 2020).

iv. ***The UFLPA is not a suitable supply chain provenance model for purposes of validating contractor compliance with Section 5949.*** Section H of the ANPRM indicates that the FAR Council will assess existing supply chain provenance initiatives, such as the UFLPA Operational guidance, to align any provenance requirements with existing industry practices. The UFLPA, however, is unsuitable as a provenance model in the semiconductor context for multiple reasons. Principally, UFLPA certification is based on a rebuttable presumption that goods seized by U.S. Customs and Border Protection ("CBP") that are made with any inputs from the Xinjiang Uyghur Autonomous Region of China are presumed to be made with forced labor. However, it is unclear how a UFLPA model would be intended to apply in the context of Section 5949. Is the reference to the UFLPA certification regime meant to suggest that electronic products procured or obtained by the Government are presumed to include covered semiconductors products or services, and that offerors must therefore provide provenance information for every semiconductor included in electronic products or services provided to the Government to prove otherwise? If so, we reiterate the point above that such a requirement would far exceed the scope of a "reasonable inquiry" and would be more burdensome than is required to validate compliance with Section 5949, especially in light of the growing semiconductor content in electronic systems, as discussed in Section II.

SIA also notes the lack of clarity on whether an offeror will be presumed non-compliant if they are unable to provide to the U.S. Government all required provenance-related information, which is likely to be challenging for the reasons discussed in these comments. SIA disagrees with the adoption of any such presumption.

The global semiconductor industry already maintains strict supply chain controls and closely tracks suppliers of parts, equipment, and materials, including steps to prevent human rights abuses. For example, in 2013 the global industry established a Conflict-Free Supply Chain Policy to ensure the responsible sourcing of minerals and address deep concerns about the sources of minerals, including polysilicon, from "conflict-affected and high-risk areas."[5] In contrast to the UFLPA discussed above, this approach provides a list of sources and suppliers against which companies can check and then certify that it does not source from those suppliers. The risk-based approach is based on objective and verifiable information that the Government can use to determine whether an item complies with prohibitions.

v. ***The proposed provenance requirements create risks to proprietary and business confidential information.*** The protection of IP is essential to U.S. technological advantage and continued semiconductor competitiveness. U.S. semiconductor companies devote approximately one-fifth of sales revenue to R&D, often leading to the creation of trade secrets and other valuable IP. The rapid pace of technological change in semiconductor

[5] *See* 77 Fed. Reg. 56274 (Sept. 12, 2012) (SEC final rule relating to the use and chain of custody of conflict minerals).

technology also requires constant advancement in semiconductor process technology and device capabilities. Semiconductor companies consider information about their supply chain – including materials suppliers and other vendors – as sensitive information and/or IP. The proposed provenance requirement would mandate offerors to provide expansive provenance-related information for themselves and on behalf of their subcontractors and suppliers, much of which constitutes highly safeguarded proprietary and business confidential information. The U.S. Government's aggregation of proprietary provenance information creates considerable information safeguarding issues, as addressed further below in Section(B)(viii).

vi. ***Suppliers unwilling to share sensitive IP may opt to exit the government contracting pipeline.*** Requiring IP sharing may discourage companies from bidding on federal contracts, or semiconductor companies and suppliers from selling chips or electronic products and services directly to the Government. Offerors are likely to struggle to collect provenance information from downstream subcontractors and suppliers and suppliers will, in turn, resist sharing their IP. These pressures could therefore eliminate from the federal contracting pipeline offerors who are unable to obtain provenance information from sub-tier suppliers. For those offerors that remain, the provenance requirement will likely lead to all parties passing compliance costs into the cost of their products, raising the total cost of products and services for the Government and the defense industrial base. This together will undermine U.S. Government efforts to strengthen, maintain, and diversify the U.S. semiconductor supply chain.

vii. ***The provenance requirement may be anti-competitive.*** Semiconductor suppliers/vendors have expressed serious concern about providing provenance-related information – to include sensitive IP – to subcontractors and/or prime contractors, who may also be their competitors, or distributors that also serve their direct competitors. For instance, 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.

viii. ***The ANPRM does not adequately address the protection and storage of provenance-related information.*** Secure IP protection is crucial for U.S. innovators facing trade secret thefts from cross-border misappropriation, corporate espionage, and cyber-intrusions, among other forms. The ANPRM overlooks how the U.S. Government might store and safeguard the proprietary and confidential provenance-related information it seeks to collect from companies throughout the semiconductor supply chain. For example, centralizing this information within the U.S. Government may create unintended vulnerabilities, increasing a company's exposure to trade secret theft. The FAR Council should carefully consider the impact and mitigation of these risks, including whether the U.S. Government has the necessary systems and personnel to safeguard proprietary

information and ensure the rule clearly articulates federal requirements for each agency to protect and limit the dissemination of business confidential information.

We appreciate your consideration of these concerns and recommendations and are available to provide any further information or discussion as needed.

B. SIA Responses to Specific Questions from the ANPRM

The following are our responses to certain specific questions posed in the ANPRM.

(a) ***Do you have any recommendations for how DoD, GSA, and NASA can further clarify the scope of the prohibition?***

Response: The ANPRM references an example relevant to the section 5949(a)(1)(B) prohibition, noting that "section 5949(a)(1)(B) could restrict a Federal agency from acquiring a replacement control panel within a critical system that enables an Internet of Things (IoT) device that includes a covered semiconductor product or service and was purchased prior to the effective date of the prohibition." This particular example appears to be inconsistent with the statute's requirement that federal agencies will not be required to – (1) Remove or replace any products or services resident in equipment, systems, or services, prior to the effective date of the prohibition (i.e., December 23, 2027); or (2) Prohibit or limit the utilization of covered semiconductor products or services throughout the lifecycle of existing equipment. In turn, the section 5949(a)(1)(B) example appears to contemplate a limitation on the utilization of a covered semiconductor product that was purchased prior to the effective date of the prohibition. This might be viewed as contrary to the ANPRM's statement that agencies will not be prohibited from using covered semiconductor products throughout the lifecycle of existing equipment, such as the IoT device referenced in the example. SIA recommends that the FAR Council clarify how the section 5949(a)(1)(B) example would fit within the statement that agencies can use covered semiconductor products or services throughout the lifecycle of existing equipment.

Moreover, the section 5949(a)(1)(B) example cited in the ANPRM introduces potential complexity or impracticality for contractors. Based on the example description, it could be a challenge for the Government (and in turn contractors) to understand the source of every semiconductor included in legacy products, especially if no Bill of Materials or other artifacts were provided, or subsequently archived, when the ultimate product was sold to the Government. The ANPRM does not discuss if there would be an affirmative obligation on the part of the contractor providing the replacement part to determine the source of the semiconductor in a legacy part, or if the Government would expect the contractor to adopt a default position that any semiconductor included in a legacy product is non-compliant.

The ANPRM is also unclear as to whether the Government is expected to take the position that the source of the semiconductor in the legacy part (i.e., control panel) is irrelevant and

instead prompt contractors to ensure that any new replacement part does not include or use a prohibited semiconductor (however, this position would only seem to make sense if the contractor is replacing the entire control panel and not just refurbishing it). The section 5949(a)(1)(B) example also does not account for whether the rest of the device includes covered semiconductor products. These uncertainties could complicate confirming for the Government and contractors alike whether devices "enabled" by the control panel included covered semiconductor products. Overall, the example provided to explain the scope of section 5949(a)(1)(B) has created more questions than answers. SIA recommends that the FAR Council provide more clarity on how the example is expected to impact contractors in practice.

Lastly, SIA asks the Government to clarify and/or confirm several aspects of the "use" prohibition in Section 5949(a)(1)(B). First, SIA asks for clarification that the "use" prohibition will not prohibit a contractor from using covered products for their internal or own manufacturing or production purposes. Second, the Government should clarify whether the use prohibition prohibits an agency from procuring cloud services for a critical system if those services use devices that include covered semiconductor products.

(b) ***Do you have any comments on the proposed definitions being considered for this rule, including the definition for reasonable inquiry?***

Response: The proposed definition of "reasonable inquiry" does not adequately explain the scope of the required reasonable inquiry. While the ANPRM defines what a reasonable inquiry ***does not require*** (e.g., independent third-party audits), it offers little guidance on what actions an offeror must undertake to comply with the requirement. For example, the proposed definition does not clarify what "other mechanisms of diligence review" may be required. The ANPRM also does not elaborate on how, and by whom, results of a reasonable inquiry would be validated and/or to whom the results would be provided. Providing additional information to companies regarding the lowest depth of review (i.e., the finished product or raw materials) to meet the definition of reasonable inquiry would be beneficial as well. As such, SIA recommends that the FAR Council either revise the definition of "reasonable inquiry" to clarify company requirements when performing a reasonable inquiry or promulgate additional guidance to offerors that clarifies this requirement.

It is also unclear how the reasonable inquiry requirement relates to the proposed requirement that contractors make "a ***comprehensive and documentable effort*** to identify and remove the covered semiconductor products or services," as set out under Section D of the ANPRM. The ANPRM neither provides a specific definition for the phrase "comprehensive and documentable effort" nor explains whether this is part of, or a separate requirement to, the reasonable inquiry for offerors. SIA recommends that the proposed rulemaking include definitions of these terms that clearly distinguish the differences between a "reasonable inquiry" and a "comprehensive and documentable effort," including

when each is required. SIA alternatively recommends that the term "reasonable inquiry" be used throughout the rulemaking to avoid confusion.

Finally, the proposed definition for "covered semiconductor product or service" includes semiconductors, semiconductor products, and semiconductor services produced or provided by an entity that the Secretary of Defense or the Secretary of Commerce, in consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation, determines is a covered entity. SIA recommends that the proposed rule establish the process and criteria by which the Secretaries of Defense or Commerce may designate a "covered entity." There should also be some due process mechanism for companies to request removal of the designation of "covered entity." We further recommend that there be a public comment period on the proposed process and criteria, as well as a phase-in period for this authority.

(c) ***Are there any definitions that should be added?***

Response: *See* SIA response to question (b), which proposed including a definition of "comprehensive and documentable effort."

The ANPRM lacks key definitions that must be clarified. For example, Section D makes clear that DOD, GSA, and NASA plan to require a clause in all solicitations and contracts with ten requirements. However, several of the contract clause requirements set forth in Section D of the ANPRM include terms with no definitions, such as "reasonable inquiry" (requirement 3) or "direct customer" (requirement 4). Under requirement 5, the standard for "becoming aware or having reason to suspect" is unclear. As written, this standard appears lower than the credible evidence standard in the mandatory disclosure rule, which could result in a flood of over-reporting to avoid draconian penalties, as happens with the government's significant overpayment rule. (Since the Government has never defined what constitutes a "significant overpayment" which then must be disclosed, there are companies which will report an overpayment of $1.) Instead, it would be helpful for the Government to provide an example of the standard in support of Item 5. The counterfeit parts regulations, which provide a reasonable standard for identifying suspect electronic parts (*see* DFARS 252.246-7007(a) for a definition of "Suspect Counterfeit Electronic Part"), is an example to consider. The definition of "use" for the "use prohibition" in Section 5949(a)(1)(B) is also undefined. Lastly, the terms "control" and "can control" for the term "affiliates" are undefined. The term "control" in the corporate and commercial contexts typically means more than a 50-percent ownership. It is unclear if the same definition of control would apply in the context of the ANPRM's definition of affiliate.

(d) ***Do you have any comments on DoD, GSA, and NASA's plan for requiring a solicitation provision and contract clause?***

Response: Section D(2) of the ANPRM notes that the proposed clause would require contractors to apply the prohibition of Section 5949(a)(1)(B) *unless* the agency identifies

that the product or service would *not* be in a critical system. Instead, SIA recommends that the Government should affirmatively state in the solicitation and contract that the product or service it is purchasing will be used in a critical system. In doing so, the Government will directly reduce the compliance burden on industry since the procuring agency is the only party that knows whether its requisition is for a critical system.

(e) ***Are there any details regarding the waiver authority that would be helpful to clarify?***

Response: The FAR Council should clarify the scope of any waiver authority – e.g., whether waivers may be granted for particular vendors or for product classes or categories (versus individual products).

(f) ***Do you have sufficient visibility into your supply chain to understand whether your supply chain uses any covered semiconductor products or services? What information is normally requested from subcontractors and suppliers about semiconductor provenance?***

Response: *See* SIA's general comment in Section III.A regarding the difficulty of collecting provenance-related proprietary and confidential business information.

(g) ***What procedures do you anticipate using to conduct a reasonable inquiry into your supply chain to understand whether your supply chain uses any covered semiconductor products or services? How do you currently or how do you plan to detect the inclusion of covered semiconductor products and services in your supply chain?***

Response: SIA recommends the U.S. Government create a standard reasonable inquiry form and upload it on a government-hosted web portal that is accessible to **all** suppliers.[6] SIA notes that its recommended standard reasonable inquiry form **is not** the same as a mandatory FAR/DFARS flow-down but instead is advance due diligence that satisfies the "reasonable inquiry" standard in this ANPRM.

U.S. and non-U.S. suppliers would be able to register on the portal and complete the form. SIA does not recommend mandatory registration. Instead, suppliers can choose to visit the portal and complete the standard form. Completion of the form can be done once and then anyone can query a company to confirm if they have completed the form. If a company chooses to complete the online form, a customer **cannot** ask it to complete another form. The form would need to be accepted as sufficient evidence to satisfy the reasonable inquiry standard. In doing so, this helps to standardize the inquiry, so companies required to comply with Section 5949 are on a level playing field. Small and medium-size businesses would particularly benefit from a standardized form as this would help minimize the

[6] SIA notes that SAM.gov – the official website of GSA – is only accessible by U.S. suppliers. Given the global nature of semiconductor supply chains, SIA members naturally have non-U.S. supply chains as well. As a result, SAM.gov would not be an appropriate website/platform through which any standard reasonable inquiry could be accessed by suppliers.

regulatory burden placed on them and alleviate staff requirements necessary to otherwise manage dozens of inquiries on the same issues from all of their customers.

The U.S. Government can set up the system to have routine recertifications that suppliers can complete once on a routine basis (i.e., yearly). If suppliers do not recertify or it lapses, then customers can proceed with their own forms.

Lastly, SIA recommends any online form to be scalable. The form should allow suppliers, for example, to add sections related to other similar government sourcing restrictions such as Section 889, as applicable.

(h) ***If your organization does use covered semiconductor products or services, how much of an impact will this prohibition have on your organization?***

Response: Companies that source or use covered semiconductor products or services will likely incur significant expense and resources to modify their supply chain for compliance with this prohibition.

For those fabless chip companies currently partnering with covered entities, the U.S. Government could establish a porting fund to aid their transition to other, non-covered manufacturing partners. DoD could leverage existing funds from its Industrial Base Analysis and Sustainment ("IBAS") Program to support this effort.

(i) ***Do you have any comments on DoD, GSA, and NASA's estimated impact of a future rule to implement section 5949?***

Response: Compliance with the ANPRM requirements, particularly those obligating offerors to provide provenance-related information, likely will require companies throughout the supply chain to divert time, resources, and personnel away from critical day-to-day business operations. It will also introduce practical difficulties of collecting and identifying information on all vendors in the supply chain, particularly for distributors or re-sellers. The FAR Council therefore should consider the considerable time and resource cost to companies – whether large or small businesses – to comply with the proposed supply chain provenance requirement.

The FAR Council should clarify how it calculated the anticipated $10,000 average cost for each non-compliant semiconductor product or service to come into compliance through an alternative or updated product or service. The complexity and cost, as noted above, associated with confirming semiconductor sourcing and seeking alternatives (which would undoubtedly be more expensive than a covered semiconductor), makes the $10,000 anticipated cost seemingly low. For example, when factoring in probable costs of process changes such as mask changes and requalification, costs for semiconductor companies can range from $100,000 to as high as $10 million.

(j) ***Are there any categories of products or services you currently provide to the Government for which you anticipate needing a waiver when the prohibition is effective in December 2027? If so, which categories of products or services?***

Response: No response.

(k) ***For categories of products or services for which a waiver may be necessary, how long do you anticipate it will take to find alternative semiconductors that are compliant?***

Response: Qualifying and producing alternative sources for some complex products can take up to three-to-four years. Any waiver should reasonably cover this transition period. Further, many semiconductor manufacturers may find the government market is too small to justify the time and expense of designing or developing alternatives.

(l) ***What impact will implementation of section 5949 in the FAR have on small businesses, including small disadvantaged businesses, women-owned small businesses, service-disabled veteran-owned small businesses, and Historically Underutilized Business Zone (HUBZone) small businesses? How should DoD, GSA, and NASA best align this objective with efforts to ensure opportunity for small businesses?***

Response: *See* SIA's general comments in Section III.A regarding the compliance challenges associated with the provenance requirement, as well as SIA's response to question (i) above regarding the significant time and resource cost of compliance generally.

(m) ***What additional information or guidance do you view as necessary to effectively comply with a future rule to implement section 5949?***

Response: SIA is unclear how it can comment on what additional guidance is needed on a *future* rule when the organization, and its members, do not know what a future, final rule will entail. It would be speculative at this point. SIA respectfully requests the FAR Council to carefully consider and incorporate SIA's comments into the *current* ANPRM and will provide additional comments on future rulemaking related to Section 5949 when it occurs.

(n) ***What challenges do you anticipate facing in effectively complying with a future rule to implement section 5949?***

Response: *See* SIA's general comments in Section III.A regarding the compliance challenges associated with the provenance requirement, as well as SIA's response to question (i) above regarding the significant time and resource cost of compliance generally.

(o) ***What would be the best method or process for identifying the provenance of the supply chain for the semiconductor components? Are you aware of existing guidelines or best practices for identifying and documenting the provenance of the supply chain for electronic products and electronic services? Do you have any suggestions for how and***

when the Government should validate supply chain provenance information and documentation?

Response: *See* SIA's comments regarding provenance requirements in Section III.A.

An alternative to provenance requirements could be to develop standards for chips based on specific criteria, which could include trust, operational security, and environmental sustainability, among others. Industry members could then certify their products to such standards to ensure compliance with Section 5949 and the implementing regulations, while simultaneously minimizing the risk of supply shortages and unnecessary disruptions that could, and likely would, impact key economic and defense sectors.

In this regard, we would draw the U.S. Government's attention to relevant provisions in the European Union's "Chips Act" regulations[7], which calls for the development of "common standards for green, sustainably manufactured, trusted and secure chips." The regulation goes on to say that "future smart devices, systems and connectivity platforms will have to rely on ***advanced semiconductor chips*** and they ***will have to meet green, trust and cybersecurity requirements which will largely depend on the features of the underlying technology***." We strongly urge the U.S. Government to coordinate closely with the European Union and its Member States to ensure that any such standards are developed transatlantically, together with other relevant partner countries, and with the involvement and participation of industry stakeholders. Given this rulemaking, and similar efforts within Europe, SIA and its member companies are concerned that uncoordinated, unilateral efforts could lead to divergent or incompatible national approaches, contributing to a balkanization of the semiconductor supply chain, a panoply of differing and onerous requirements in different jurisdictions, and increasing administrative burden and costs across the semiconductor and electronics supply chains. Given that the efforts within the U.S. and EU in this regard are at relatively nascent stages, we again strongly urge the U.S. Government to begin coordinating a multilateral approach on this topic without delay. A second alternative related to the above could be to establish a process along the lines of the third-party assessment organization (3PAO) that companies use to achieve FedRAMP certification. In this scenario, the Government would construct relevant metrics and any company that wants to be measured against these metrics would commission an independent third party to evaluate and certify their supply chain processes to validate compliance with Section 5949. Establishing a 3PAO process could also serve to address anti-competitive concerns discussed above, such that a semiconductor supplier would not need to provide sensitive IP and proprietary information to a contractor, but instead to an independent third party.

[7] Council Regulation 2023/1781, Establishing a Framework of Measures for Strengthening Europe's Semiconductor Ecosystem and Amending Regulation 2021/694, 2023 O.J. (L 229) 1, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1781.

A third idea for the FAR Council's consideration could be to look at the DFARS counterfeit part sourcing clause as a more manageable alternative model to the proposed traceability and provenance models. The cornerstone of counterfeit sourcing in the DFARS (48 CFR 252.246-7008) is that the obligation for traceability ends at the OEM or the OEM's authorized source. SIA notes that parallels exist between the counterfeit DFARS clauses, the ANPRM, and statutory text of section 5949. For example, both the statute and the counterfeit regulations use the same terms such as "detect," "avoid," "rework," and "corrective action." *S*ee DFARS 252.246-7007(b) and 231.205-71(b) and its reference back to the sourcing clause 252.246-7008.

Section H of the ANPRM suggests that the collected provenance-related information could include the "identification of vendors and facilities responsible for the design, fabrication, assembly, packaging, and test of the product." To the extent the proposed rulemaking includes a provenance requirement, SIA urges the FAR Council to limit the scope of any information-sharing to the minimum amount of provenance information needed to identify the use of covered semiconductor products or services, for example by limiting the provenance requirement to front-end wafer fabrication. SIA also questions whether it is necessary to include third-party IP providers in the proposed supply chain validation or provenance requirement. Logic integrated circuits ("ICs"), such as semiconductor microcontrollers, or MCU, often are designed by large teams located in different geographical areas and entities. The design of such logic ICs may also include pre-designed IP from third-party IP providers. There may also be impacts to the Government if the provenance requirement is extended to third-party IP providers. For example, IP providers often negotiate commercial terms with chipmakers, and federal procurement requirements would likely complicate these transactions, and lead to increased costs. Accordingly, we request that the proposed rulemaking clarify that contractors do not need to validate third-party IP providers as part of the proposed provenance requirement. To the extent that the FAR Council does require third-party validation, SIA recommends that the FAR Council establish a materiality threshold or adopt a *de minimis* approach.

(p) ***If the Department of Commerce establishes a public list that identifies electronic products with prohibited semiconductors, would this be helpful for implementing this prohibition?***

Response: SIA cautions against the practicality of the Government compiling and maintaining a list of electronic products with prohibited semiconductors. SIA recommends that the U.S. Government consider the time, resources, and personnel required to establish a list, the frequency it intends to update the list (i.e., monthly, bi-annually, annually), etc. It is also unclear how the Government would develop and vet this list to ensure its reliability. The use of such a list fails to consider the lead time and cost required for companies to identify and qualify new suppliers should an existing one be added to a prohibited list. Any new addition to a prohibited supplier list could result in significant contraction of existing inventory as supply chain requirements evolve, especially should a

new entity be added to the prohibited list without much notice. Alternatively, *see* SIA's comment in Section III.B(o) regarding standards.

(q) ***Do you have any feedback regarding how DoD, GSA, and NASA should incorporate the requirements regarding certification, disclosure, notification safe harbors, and allowable costs in paragraph (h) of section 5949?***

Response: The model clause section suggests that in all cases "rip & replace"-related costs are unallowable in contract costs. This means that a contractor who discovers the inclusion of a prohibited component (through no fault of its own) and acts in good faith to report this non-compliance, could then be liable for any and/or all replacement costs. Moreover, "allowability" also only applies in cost type contracts – the rules do not indicate if there is a presumption that in fixed-price contracts such costs are grounds for an equitable adjustment. Any final rules should clearly allow flexibility and leeway related to any costs associated with good-faith efforts to address non-compliance.

(r) ***What else should DoD, GSA, and NASA consider in drafting a proposed rule to implement the prohibitions outlined in section 5949?***

Response: The FAR Council should also consider the impacts of the ANPRM on U.S. competition, market demand, and supply chains, as well as ensuring that the U.S. Government is coordinating with other governments who are undertaking similar efforts to ensure alignment and interoperability of regulatory approaches. The U.S. Government and its partners are a small consumer of semiconductor products relative to the commercial market, yet require specialization, customization, and now, prohibition as part of its procurement requirements. These requirements are misaligned with commercial demands for semiconductors and can hinder offerors' access to the most innovative technologies from vendors who otherwise may choose not to participate in government contracting for reasons related to provenance, as discussed above in detail. Therefore, the Section 5949 proposed rule should prioritize manageable, appropriately scoped, and purpose-fit compliance requirements.

It is paramount for the U.S. Government and its federal contractors to ensure continued access to technologies developed and commercialized by companies headquartered in close, democratic allied countries. Currently, companies located in allied nations – e.g., in Europe, South Korea, Japan, and Taiwan – manufacture nearly 90% of the leading-edge chips in the world. SIA encourages the U.S. Government to work with international allies to strengthen the semiconductor supply chain and ensure continued access to related semiconductor technologies.

The FAR Council should also consider exempting commercial items that could potentially be used in the course of maintaining critical systems tangentially. For example, including commercial items products used in data centers would likely result in the rule reaching far beyond products used more directly in mission critical settings.

Section 5949(f)(2)(C) requires the "development of a process for provenance and traceability design to disposal of microelectronics components and intellectual property contained therein implementable across the Federal acquisition system to improve reporting, data analysis, and tracking." The ANPRM does not mention the "traceability" program as would be expected under Subsection (f), and therefore it is difficult for SIA to comment on any provenance traceability design and what will be required. SIA recommends that the FAR Council address its recommendations for and the status of the provenance and traceability design so that industry can be better positioned to comment on what specific information the Government may be looking for with respect to chain of custody.

IV. CONCLUSION

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

Uploaded to www.regulations.gov. FAR-2023-0008-0005

Courtesy copy sent to: William.Clark@gsa.gov.