SIA SEMICONDUCTOR INDUSTRY ASSOCIATION

Comments of the Semiconductor Industry Association (SIA)
to the
General Service Administration (GSA) on
"Request for Information From Suppliers Selling on Commercial ECommerce Portals"

83 Fed. Reg. 27989 (June 15, 2018)

Notice-Qp–2018–02;
Docket No. 2018–0002; Sequence No. 11

Submitted July 20, 2018

The Semiconductor Industry Association (SIA) submits these comments to the General Service Administration (GSA) on its "Request for Information From Suppliers Selling on Commercial ECommerce Portals." 83 Fed. Reg. 27989 (June 15, 2018).

SIA is the trade association representing leading U.S. companies engaged in the design and manufacture of semiconductors. Semiconductors are the fundamental enabling technology of modern electronics that has transformed virtually all aspects of our economy, ranging from information technology, telecommunications, health care, transportation, energy, and national defense. The U.S. is the global leader in the semiconductor industry, and continued U.S. leadership in semiconductor technology is essential to America's continued global economic leadership. More information about SIA and the semiconductor industry is available at www.semiconductors.org.

In its Phase II Market Analysis and Consultation, GSA seeks "recommendations for any changes to, or exemptions from, laws necessary for effective implementation" of section 846 of the NDAA of 2018. GSA seeks to evaluate the products or product categories that are suitable for purchase on the commercial e-commerce portals and the precautions necessary to safeguard any information pertaining to the Federal Government, especially precautions necessary to protect against national security or cybersecurity threats. In terms of product categories, GSA requests comments on:

- An "[a]ssessment of supply chain risk, including the extent to which you believe counterfeit products are a significant problem, and mitigation strategies."
- "Identify which categories/ subcategories should be excluded from the scope of this effort and the rationale."

Under program design, GSA seeks information on competition and comparison across various suppliers: "Competition is a core goal of the program. Towards that end, the user needs to be able to see/compare products across multiple portals and/or suppliers. What is the best way to get to a single sign-on across portals?"

SIA's comments seek to address these questions as they pertain to semiconductors. As discussed in more detail below, **SIA believes the federal government and its contractors and subcontractors should only purchase semiconductors through e-commerce portals of a manufacturer's authorized distributor or the manufacturer directly. There is extensive documented evidence of the risk to human health and safety resulting from the purchase of counterfeit semiconductors, and this risk increases significantly when these devices are purchased outside the authorized distribution channels.** Instead of creating risks of purchasing untested, unreliable products through e-commerce portals outside the authorized distribution chain, the federal government should meet its purchasing needs by limiting its purchasing of semiconductors to e-commerce portals of authorized distributors or the manufacturer directly.

1. Product Categories – Assessment of Supply Chain Risk and the Challenge of Counterfeits

Semiconductors[1] are the microelectronics that enable virtually all modern electronics and are used in numerous industry sectors, including the military, aerospace; industrial; critical infrastructure (e.g., utilities and energy), transportation, medical devices, and a range of consumer products. Semiconductors are complex products that are designed, manufactured and distributed under highly controlled conditions to meet exacting quality and reliability standards.

Unfortunately, counterfeiters have sought to infiltrate the global supply chain and profit from the sale of counterfeit semiconductors. Semiconductor counterfeiting is considered the act of fraudulently manufacturing, altering, distributing, or offering a product or package that is represented as genuine. These products are usually used or defective but refurbished to look new. Counterfeit semiconductors are typically salvaged from discarded electronic products ("e-waste") in a dirty, uncontrolled process that results in products that cannot be expected to operate reliably. The counterfeit products are typically sold on the open market through brokers, independent distributors, unauthorized aftermarket manufacturers, and e-commerce portals which are not operated by Original Component Manufacturer (OCM) or OCM's authorized distributors.

Semiconductor companies and their Authorized Distributors, Authorized Resellers, and Authorized Aftermarket Distributors/Manufacturers have extensive, proven controls to ensure products are properly manufactured, tested, handled, and stored to prevent failures. Counterfeiters have few if any such controls. The result is that, unlike legitimate semiconductors from authorized sources, counterfeits and other semiconductors available from nonauthorized sources often have low quality and poor reliability.

Improper purchasing practices are the primary reason that counterfeit semiconductor products have proliferated. Counterfeit components reported to SIA member companies and reported through the Government-Industry Data Exchange Program ("GIDEP") invariably involve purchases from sources that are not authorized by the original component manufacturers ("OCMs") to sell their company's semiconductor products. The OCMs sell their products either directly or through their own controlled network of authorized distributors and authorized resellers. The OCMs authorize and manage their networks to meet stringent handling, storage, and transportation requirements to protect the semiconductors from damage; this allows the products to be covered by the OCMs' full warranties. In contrast, the open market includes independent distributors, brokers, and on-line component exchanges that obtain products from a wide range of suppliers. Unfortunately, some suppliers either intentionally or unknowingly introduce counterfeits into the open market supply chain. Even if components purchased from non-authorized sources are authentic, they may not have been properly handled and stored and may therefore risk future performance and reliability problems. Therefore, non-authorized components may not be authentic, may not be reliable, and are not covered by the OCM's warranty.

[1] NAICS Code 334413.

The safest way to ensure that semiconductor components are authentic, and have optimal quality and reliability levels, is to buy them exclusively through authorized sources, including e-commerce portals of a manufacturer's authorized distributor or the manufacturer directly. Products purchased through authorized sources have superior quality and reliability levels and carry full factory warranties.

2. Product Categories – Semiconductors Purchased through E-Commerce Portals of a Manufacturer's Authorized Distributor or the Manufacturer Directly

Federal procurement from e-commerce portals should be limited to the portals of a manufacturer's authorized distributor and/or the manufacturer directly because of (a) the significant risk posed by counterfeit semiconductors offered outside the authorized supply chain, (b) the likelihood of purchasing counterfeit semiconductors through portals outside the authorized supply chain, and (c) the availability of secure purchasing alternatives.

a. Adverse Consequences of Purchasing Counterfeit Semiconductors

Unlike some other counterfeit products, such as counterfeit consumer goods or apparel, counterfeit semiconductors have the potential to result in significant health, safety and security consequences. Because semiconductors are found in a wide range of critical systems, the failure of a key component can result in the risk of injury or property damage. The potential for failure increases dramatically with the purchase of counterfeit semiconductors that are not manufactured, tested, handled, or stored according to the exacting specifications of legitimate semiconductors.

In the civilian sector, semiconductors play a critical role in medical and health equipment, transportation safety systems, and numerous other critical systems. There are numerous documented instances of counterfeit semiconductors resulting in the failure of components in these products.[2]

The risks posed by the infiltration of counterfeit semiconductors into national security systems is even more severe and also well-documented. In 2011, the Senate Armed Services Committee ("SASC") staff initiated an investigation into counterfeit electronic parts in the defense supply chain. The investigation found extensive infiltration of counterfeit semiconductors in critical defense systems. The report's summary clearly outlines the scope of the problem:

> The systems we rely on for national security and the protection of our military men and women depend on the performance and reliability of small, incredibly sophisticated electronic components. Our fighter pilots rely on night vision systems, enabled by transistors the size of paper clips, to identify targets. Our soldiers and Marines depend on radios and GPS devices, and the microelectronics that make them work, to stay in contact with their units and get advance warning of threats that may be around the next corner. The failure of a single electronic part can leave a soldier, sailor, airman, or Marine vulnerable at the worst possible time.

[2] Winning the Battle Against Counterfeit Semiconductor Products: A report of the SIA Anti-Counterfeiting Task Force (available at 5-6 http://www.semiconductors.org/clientuploads/directory/DocumentSIA/Anti%20Counterfeiting%20Task%20Force/SIA%20Anti-Counterfeiting%20Whitepaper.pdf).

> Unfortunately, a flood of counterfeit electronic parts has made it a lot harder to prevent that from happening.[3]

The Senate investigation uncovered suspect counterfeit semiconductor components in a range of military systems. Among others, the report found counterfeits in:

- mission computers for the MDA's THAAD missile,
- military aircraft including SH-60B, AH-64, and CH-46 helicopters, C-17, C-130J, and C-27J military transport planes, and the P-8A Poseidon, a military plane with antisubmarine and anti-surface warfare capabilities.[4]

The potential consequences of sensitive military systems being impaired by counterfeit semiconductors was underscored at a 2011 hearing before the Senate Armed Services Committee by Lt. Gen. Patrick J. O'Reilly, Director, Missile Defense Agency: "We do not want a $12 million missile defense interceptor's reliability compromised by a $2 counterfeit part."[5]

Also illustrative of the problem are prosecutions of brokers who have sold counterfeit semiconductors including:

- Mr. Picone who was sentenced to 37 months in prison in 2015 for importing thousands of counterfeit integrated circuits from China and reselling them to U.S. customers, including contractors supplying them to the U.S. Navy for use in nuclear submarines.[6]

- Ms. McCloskey was sentenced to 38 months in prison in 2011 for her role in importing counterfeit integrated circuits and selling hundreds of thousands of them to the U.S. Navy, defense contractors and others, marketing some of these products as "military-grade."[7]

Mr. Vasquez was charged in a 30-count indictment in May, 2018 for allegedly remarking and selling old devices with altered date codes to deceive customers and end users into thinking the integrated circuits were new devices. One of the counts related to eight integrated circuits that Mr. Vasquez allegedly knew were counterfeit military goods, "the use, malfunction, and failure of which were likely to cause serious bodily injury and death, the disclosure of classified information, impairment of combat operations, and other significant harm to a combat operation, a member of the Armed Forces, and to national security."[8]

[3] Senate Armed Services Committee, *Inquiry Into Counterfeit Electronic Parts In The Department of Defense Supply Chain* at i. (May 21, 2012) ("SASC Report").

[4] SASC report at 9.

[5] *Investigation into Counterfeit Electronic Parts in the Department of Defense Supply Chain: Hearing Before the S. Comm. on Armed Services*, 112th Cong. 39 (Nov. 8, 2011), available at http://armedservices.senate.gov/statemnt/2011/11%20November/OReilly%2011-08-11.pdf.

[6] Department of Justice press release at: https://www.justice.gov/opa/pr/massachusetts-man-sentenced-37-months-prison-trafficking-counterfeit-military-goods-0

[7] U.S. Immigration and Customs Enforcement release at: https://www.ice.gov/news/releases/visiontech-administrator-sentenced-prison-role-sales-counterfeit-circuits-destined-us

[8] Justice Department release at: https://www.justice.gov/usao-cdca/pr/orange-county-electronics-distributor-charged-selling-counterfeit-integrated-circuits

b. Prevalence of Counterfeit Semiconductors

It is difficult to quantify the prevalence of counterfeit semiconductors. Given that the global industry produced and sold almost a trillion individual units in 2017, in addition to the existing base of hundreds of billions of chips in existence, there would be a substantial number of counterfeits even if only a small fraction of semiconductors were counterfeit.

The limited data from law enforcement agencies suggest that counterfeit semiconductors is a widespread problem. For example, according to data on seizures by Customs and Border Protection (CBP), in a joint operation with European Union Customs over a three week period in November/December 2007, the agencies seized over 360,000 counterfeit integrated circuits and computer network components bearing more than 40 different trademarks.[9] During a follow-up Joint Customs Operation of EU Customs supported by US CBP, EUROPOL, and OLAF (European Anti-Fraud Office) in 2016, more than one million counterfeit integrated circuits were seized within a two week period.

Counterfeit semiconductor products have proliferated due to poor purchasing and supply chain practices. Tens of thousands of independent distributors and brokers worldwide established Internet sites to buy and sell semiconductor products outside of the authorized supply chain of OCMs and their Authorized Distributors/Resellers. Rather than facilitating the sale of counterfeit and otherwise questionable components by purchasing them over unauthorized channels, federal agencies should strengthen their procurement practices by purchasing semiconductors through e-commerce portals of a manufacturer’s authorized distributor or the manufacturer directly.

c. Availability of Secure Purchasing Alternatives

Fortunately, the federal government can significantly reduce the risks of counterfeit semiconductors from entering the supply chain by requiring purchase from authorized sources – original manufacturers and their authorized distributors. SIA urges the GSA to require government agencies, including contractors and subcontractors, to avoid counterfeit semiconductors by buying semiconductor components either directly from OCMs or directly from OCMs’ authorized distributors and authorized resellers or authorized aftermarket manufacturers. This approach is consistent with the Defense Federal Acquisition Regulation Supplement Sections 246.870, 252.246-7007, and 252.246-7008 relating to Detection and Avoidance of Counterfeit Electronic Parts; and industry best practices as outlined in the SAE Aerospace Standard AS5553 “Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition”; and The JEDEC Solid State Technology Association’s JESD243 standard “Counterfeit Electronic Parts: Non-Proliferation for Manufacturers.”

SIA urges federal agencies to employ a tiered approach in purchasing legitimate semiconductors from the authorized distribution chain.[10] For those components that are currently in production or in stock, SIA advocates that federal agencies purchase from the original manufacturers of the parts or their authorized dealers or authorized aftermarket manufacturers. Semiconductor companies generally avoid the creation of “legacy” products by providing customers with notice in advance of the discontinuance of products, in accordance

[9] Winning the Battle Against Counterfeit Semiconductor Products at p. 8.
[10] Id. at 21-22.

with industry standards.[11] Nonetheless, situations sometimes arise where parts are not available from original manufacturers, their authorized dealers, or authorized aftermarket manufacturers. Under these circumstances, then purchasers should buy legacy components from OCMs' Authorized Aftermarket Distributors/Manufacturers that obtain legacy products exclusively from OCMs in wafer, die, or final packaged form. Additionally, most OCMs have contracts with aftermarket manufacturers to manufacture OCM discontinued products. Thus, federal purchasers typically have options through the authorized distribution chain and can avoid unauthorized and unreliable e-commerce portals.

Semiconductors purchased through the authorized supply chain are manufactured, tested, handled, and stored in accordance with rigorous standards designed to prevent failures. In contrast, there is no current means to qualify a non-authorized electronic part as an OCM-authorized part. Purchases of electronic parts from non-authorized sources threaten the safety and integrity of the DoD supply chain. Therefore, it is critical that purchases of electronic parts be from OCMs, or from authorized distributors, authorized resellers, or authorized aftermarket distributors and manufacturers, that are authorized directly and only by the OCM to produce an item.

With regard to older, out-of-production semiconductors ("legacy products") that are not available from OCMs directly or through OCMs' authorized distributors and authorized resellers, purchasers can avoid buying counterfeits because these products are still generally available through aftermarket distributors and manufacturers that are authorized by OCMs to buy end-of-production products and/or obtain licensing to manufacture the original products. These authorized aftermarket distributors and manufacturers literally have billions of older products that meet all of the OCM's storage, handling, transportation, performance and reliability requirements. Federal procurement should fully utilize aftermarket manufacturers and distributors by requiring contractors to perform an exhaustive search of these sources. In many cases, products from aftermarket manufacturers and distributors are available for immediate delivery.

Government can significantly reduce the risks of counterfeit semiconductors from entering the supply chain by requiring purchase from authorized sources – original manufacturers and their authorized distributors. Products purchased through authorized sources are more cost effective in the long term, since they have superior quality and reliability levels, and carry full factory warranties. Any potential savings that federal agencies or their contract managers realize by purchasing semiconductor components from the open market or ordering components on e-commerce portals outside the authorized distribution chain would be dwarfed by the health and safety risks and costs of unreliable counterfeit components.

[11] Semiconductor companies avoid the creation of legacy products that are out of stock and no longer in production by providing customers with at least six months to place orders and one year to ship orders after a Product Discontinuance Notice (PDN) is issued for a given product. PDNs usually specify replacement products and/or alternate sources for products that are being discontinued. In many cases, customers expect to receive these PDNs, and they have little if any impact on their operations. These measures are consistent with an industry standard, JEDEC Standard JESD48C: "Product Discontinuance," December 2011 (available for download after registration at http://www.jedec.org/).

3. Program Design – Competition and Comparison of Products from Multiple Suppliers

SIA supports GSA's goal of ensuring competition and being able to compare products among multiple suppliers. This goal can be achieved while at the same time purchasing legitimate semiconductors from authorized sources.

Semiconductor companies have made it easy for customers to identify their Authorized Distributors. OCMs list their Authorized Distributors and any Authorized Resellers on their Internet sites. An industry association of component manufacturers and their authorized distributors, the Electronic Components Industry Association (ECIA), has developed and maintains an Authorized Directory listing for ECIA member companies.[12] This web-based search tool provides distributor information that is maintained, checked, and updated on a regular basis from the OCMs' websites who are members of ECIA.

Federal purchasers can use this tool to advance competition and compare products among authorized distributors, while at the same time maintaining safeguards for the security and reliability of the semiconductors it purchases.

+ \+ \+

SIA appreciates the opportunity to provide these comments.

[12] http://www.eciaauthorized.com/. When choosing Authorized Distributors, keep in mind that a given distributor may carry a very broad line of components and may only be an Authorized Distributor for a subset of those components. Thus, if a distributor makes a general statement that they are authorized, be sure to check that they are authorized by the specific OCM of interest to sell that OCM's components.