Submission of the
Semiconductor Industry Association
on

Request for Public Comments on Report on the State of Counterfeit and Pirated Goods Trafficking and Recommendations
84 FR 32861 (July 10, 2019)

July 26, 2019

The Semiconductor Industry Association (SIA) is submitting these comments in response to the Request for Public Comments on Report on the State of Counterfeit and Pirated Goods Trafficking and Recommendations. 84 FR 32861 (July 10, 2019)

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.

Semiconductors control the operation of many products, from PCs, tablets, smartphones, and smart-devices, to industrial devices including medical, automotive, manufacturing, and other vital electronics. Counterfeit semiconductor components can therefore, depending on the application, pose major risks to the health, safety, and security of people worldwide. Most people routinely use electronic products as well as infrastructure and other systems that require reliable embedded semiconductors to function properly over time. Each of these products and systems typically uses dozens, hundreds, or even thousands of semiconductor components. The failure of a single counterfeit semiconductor component in one of these products or systems may, depending on the application, have significant or even catastrophic consequences. As SIA summarizes in its Anti-Counterfeiting White Paper,[1] counterfeit semiconductors often have poor quality and low reliability, which threaten health, safety, and security when used in critical applications. Separately, counterfeit product may be used to try to defraud the brand-owner through warranty fraud schemes as well.

The importance of a concerted effort to stop trafficking in semiconductors was underscored by the recent prosecution[2] of Rogelio Vasquez, the owner of PRB Logics, an Orange County-based seller of electronic components. Vasquez sold counterfeit semiconductors that ended up in a

[1] https://www.semiconductors.org/wp-content/uploads/2018/06/SIA-Anti-Counterfeiting-Whitepaper-1.pdf
[2] https://www.semiconductors.org/semiconductor-counterfeiter-sentenced-to-46-months-in-prison/

classified weapon system used by the U.S. Air Force. He was sentenced to 46 months in prison after pleading guilty to a variety of charges, including trafficking in counterfeit goods. In 2015, Peter Picone was sentenced to 37 months in prison after he imported thousands of counterfeit semiconductors and sold them to U.S. customers, including contractors supplying them to the U.S. Navy for use in nuclear submarines.

SIA strongly supports the focus on combating trafficking in counterfeit and pirated goods. SIA offers the below feedback on the relevant sections in the Presidential Memorandum.

> *(1.) How are your interests affected by counterfeit or pirated goods imported through online third-party marketplaces and other third-party intermediaries as those terms are defined in the Presidential Memorandum? (Specific examples and/or data would be helpful, including on the origins of counterfeit and pirated goods and the types of counterfeit and pirated goods that are trafficked. Information that is not publicly available can be submitted as "business confidential" in accordance with the instructions in the ADDRESSES section).*

Counterfeit semiconductors typically are in the form of remarked/rebranded product intended to defraud the purchaser. Old product may be remarked to appear as a new/different product, a product of one manufacturer may be remarked to appear as that of another (called "clones"), product may be stolen and remarked, or otherwise harvested from electronic waste from end-user products like appliances (e-waste), often in China.

SIA member companies report that counterfeit semiconductors are sold on multiple online third-party marketplaces. One SIA member company reported that, each month, they request the removal of approximately 2,000 infringing listings, with the majority being on Chinese websites (including Taobao, Alibaba, HC360, and China.makepolo).

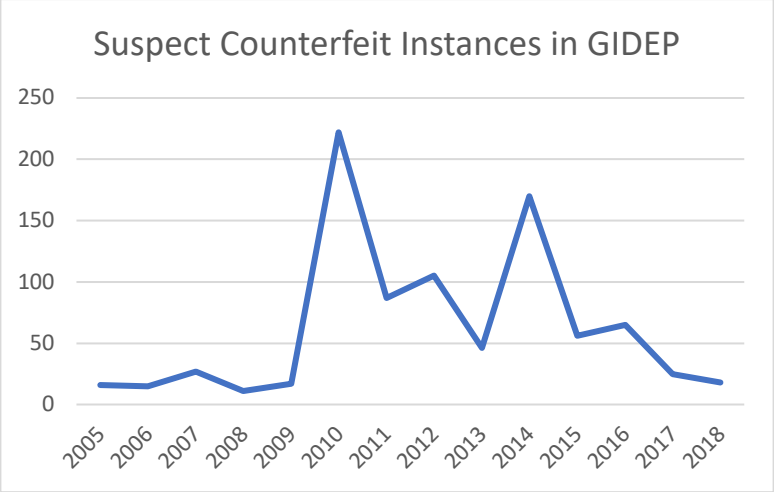
> *(5.) Are there Federal agency data collection or standardization practices, or practices involving provision of data to parties, that could promote more effective detection, interdiction, investigation or prosecution of underlying violations of U.S. customs laws and of intellectual property rights?*

One method that the federal government has used to detect and avoid counterfeit electronic parts is the Government-Industry Data Exchange Program (GIDEP). When used properly, GIDEP is a way for the government and for government contractors (both prime and sub-contractors) to share information about potential counterfeits that have entered government supply chains, with the goal of ensuring future procurement decisions do not purchase additional counterfeits. A March 2010 GAO report found that numerous contractors avoided reporting information to GIDEP over "concerns about the legal implications of reporting a part as suspect counterfeit before it had been proven".[3] To help combat this problem, DFARS Rule 252.246-7007 made reporting in GIDEP mandatory for any contractors or brokers that come across suspected counterfeits. However, reporting in GIDEP by contractors, brokers, and government has been dramatically declining (see data below). While this might lead some to believe that this has

[3] https://www.gao.gov/assets/310/302313.pdf

meant the problem of counterfeit semiconductors has been eliminated, SIA believes that this is not the case and that GIDEP data does not accurately reflect the scale, or the pattern, of counterfeits within government supply chains. Anecdotally, prosecutions of semiconductor counterfeiting has been continuing, with one case, that of Rogelio Vasquez, resulting in the seizure of over 160,000 counterfeit and suspected counterfeit data. Additionally, some private databases have shown the scale of suspected counterfeits to be much higher.

GIDEP Annual Reporting of Suspect Counterfeit Devices	
Year	**Instances**
2005	16
2006	15
2007	27
2008	11
2009	17
2010	222
2011	87
2012	105
2013	46
2014	170
2015	56
2016	65
2017	25
2018	18



(8.) What policy remedies, including administrative, regulatory, or legislative changes by the Federal Government (including enhanced enforcement actions) could substantially reduce the trafficking in counterfeit and pirated goods and/or promote more effective law enforcement regarding the trafficking in such goods? Please reference any available analyses that shed light on the efficacy and potential impacts of such proposed remedies.

One of the most effective mechanisms in stopping counterfeit semiconductors are through increased seizures at the border and not tying seizure data/recognition to the monetary value of the product, which makes seizing counterfeit luxury items more financially attractive than less expensive electronic components. Given the pivotal role of semiconductors in enabling the functionality of an array of technology products, counterfeit semiconductors may pose more significant risks than most other counterfeit products. Unfortunately, CBP metrics that track the number of shipments or the dollar value of counterfeits seized, underestimate the impact that seizures of counterfeit semiconductors have on health, safety, and national security. For example, a counterfeit semiconductor might only have a retail value of 10 cents, but its failure can cause a $1,000 electronic system to fail. The CBP port would only get 10 cents of credit if an officer seizes the semiconductor, but $1,000 credit for seizing the counterfeit system. CBP seizures of counterfeit semiconductors have declined in recent

years (as shown in the chart below), and **SIA calls on CBP and other agencies to prioritize the seizure of counterfeit semiconductors**. The problem of counterfeit semiconductors in this country has not been eliminated, it is still a real threat that deserves attention by CBP.

Fiscal Year	# of Seizures	One Year Change
2012	180	NC
2013	228	+27%
2014	240	+5%
2015	447	+86%
2016	386	-14%
2017	123	-68%
2018	142	+15%

SIA members report that CBP does a poor job in sharing seizure data internally and with HSI. There does not appear to be a common database for CBP officers or HSI investigators to identify patterns such as a broker importing counterfeits into different ports of entry. SIA members receive letters from the fines, penalties and forfeiture officers at various ports, but such letters appear to be kept at the local ports rather than being indexed and collated by CBP centrally. It is also not a consistent practice, and there is no way to connect a seizure letter to a detention inquiry. A central index should collect information on all seizures from all ports for the past three years of semiconductors from a specific shipper (or shipper address) or to a specific importer, or of a specific trademark owner's products. **SIA recommends that CBP establish a pilot program to centralize data for semiconductors and network equipment.**

SIA member companies have reported receiving notices of final goods that have been seized by CBP for having counterfeit semiconductors installed within them. However, it is currently unclear if CBP data collection practices currently count these seizures as seizures of counterfeit semiconductors. **SIA calls on CBP to clarify if current seizure data released on semiconductors includes seizures of final goods with counterfeit semiconductors installed within them, and to work to make this data publicly available if not.**

Recently, CBP has shared a new practice that counterfeiters have used to evade enforcement actions. There has been an increase in the importation of "blank" semiconductors. "Blank" semiconductors refer to semiconductors that are being imported without any trademarks or logos on them, but that will likely thereafter be marked with fraudulent markings. In this case, even though a CBP officer might suspect these blanks of being counterfeit because it is blank, or for some other reason (for example, unprofessional packaging), they are not able to seize the components since a counterfeit is defined as a "spurious mark." In the absence of a fake mark on the product that would give rise to a trademark violation, CBP is unable to seize the goods. While there may be some limited legitimate reasons for a rights holder to import "blank" semiconductors (for example, manufacturers shipping semiconductors too small to have something printed on them, in which case they would include logos and other information on outer packages and shipping documents), the majority of these blanks that CBP are seeing are likely to be used to create counterfeit marks to misrepresent the product with an intent to deceive the purchaser. **To address this practice, CBP should increase referrals of these suspected**

products to HSI. When an importer is bringing in blanks for a legitimate reason, HSI will be able to ascertain that fairly easily. But when an importer isn't bringing in blanks for a legitimate reason, and is either fraudulently marking them or selling them to be fraudulently marked so as to misrepresent the product for profit, either by reselling them or by seeking a warranty and committing warranty fraud, then a referral by CBP to HSI would enable HSI to investigate to see if the importer is marking the device with a counterfeit brand in the U.S..

Another effective method of combatting the proliferation of counterfeit semiconductors is to strengthen federal procurement practices to ensure that there is no market for their purchase. For those components that are currently in production or in stock, **federal agencies should purchase from the original manufacturers or their authorized dealers**. Semiconductor companies generally avoid the creation of "legacy" products by providing customers with notice in advance of the discontinuance of products, in accordance with industry standards. Nonetheless, situations sometimes arise where parts are not available from original manufacturers or their authorized dealers. Under these circumstances, purchasers should then buy legacy components from OCMs' Authorized Aftermarket Distributors/Manufacturers that obtain legacy products exclusively from OCMs in wafer, die, or final packaged form and are thus authorized and licensed to manufacture/distribute authentic product. 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 vendors that are typically the source of counterfeit semiconductors. Ensuring the federal government remains in the authorized distribution chain would be a significant step in fighting the proliferation of counterfeit semiconductors.

The Department of Defense's Defense Logistics Agency (DLA) maintains a "Qualified Suppliers List of Distributors"[4] for contractors seeking to purchase semiconductor devices. DLA claims that suppliers and distributors on the list provide products "that combine accepted commercial practices and quality assurance procedures that are consistent with industry and international quality standards." Unfortunately, this list includes distributors that have sold counterfeit semiconductors on multiple occasions. In one case, a distributor remained on the list for two years after pleading guilty to supplying falsely remarked semiconductors that were destined for use in U.S. military helicopters. **DLA should verify that all suppliers on the "Qualified Suppliers List of Distributors" have not been previously found to have sold counterfeit semiconductors, while removing (and keeping off) suppliers that have trafficked in counterfeits from the list.**

Finally, once ratified by all members, the United States-Mexico-Canada Agreement (USMCA) will include a significant step towards fighting the proliferation of counterfeit semiconductors. USMCA requires all countries to grant *ex officio* authority to law enforcement officials to allow them to stop suspected counterfeit goods when they enter, exit, or transit through their country. Ex officio authority is a strong tool that will allow customs authorities to seize suspected counterfeits when detected. **Once USMCA is ratified by all countries, the U.S. government should urge Canadian and Mexican law enforcement to use this *ex officio* authority, while also sharing best practices on counterfeit detection and detention.**

[4] https://landandmaritimeapps.dla.mil/Offices/Sourcing_and_Qualification/qsld.aspx