Submission of the
Semiconductor Industry Association
Regarding

Request of the U.S. Intellectual Property Enforcement Coordinator for Public Comments: Development of the Joint Strategic Plan on Intellectual Property Enforcement

83 Fed. Reg. 46,522 (September 13, 2018)

November 13, 2018

The Semiconductor Industry Association (SIA) is submitting this document in response to the "Request of the U.S. Intellectual Property Enforcement Coordinator for Public Comments: Development of the Joint Strategic Plan on Intellectual Property Enforcement."

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.

Intellectual property is the lifeblood of the U.S. semiconductors industry and the protection of IP is essential to technological progress and continued U.S. industry competitiveness. Strong IP protection and enforcement incentivizes companies and research institutions to invest in research and development and share technology without compromising their return on investments. The rapid pace of technological change in semiconductor technology requires constant advancement in semiconductor process technology and device capabilities. As a result, the investment of the U.S. semiconductor industry in R&D totals $34 billion, approximately 18.7% of sales. This percentage of revenue invested in R&D is among the highest of any industry sector.

While SIA is interested in the protection of all forms of IP, our top IP enforcement priorities relate to (1) the protection of trade secrets, and (2) efforts to reduce the prevalence of counterfeit semiconductors.

I. Trade Secrets

Trade secrets are a valuable component of the IP portfolio of semiconductor companies. In our industry, trade secrets include manufacturing know-how, chemical formulations, chip designs, and other proprietary information. Yet despite their tremendous importance, trade secrets remain extremely vulnerable, especially in jurisdictions with weak laws or weak enforcement.

SIA is particularly concerned that China's industrial policy to develop an indigenous semiconductor industry may encourage the misappropriation of trade secrets. China provides its domestic semiconductor industry, including state-owned enterprises, with massive subsidies and establishes specific technology development goals. While some Chinese semiconductor companies are seeking to develop technology by legitimate means, other Chinese state institutions, firms, and/or associated individuals may be enticed to illegally acquire or misappropriate the targeted technology from U.S. semiconductor companies as a short-cut to developing the technology necessary to design and manufacture advanced semiconductors and compete in the global market.

Chinese semiconductor companies have shifted tactics from acquisition of U.S. and other companies to acquiring hundreds of talented engineers and managers from foreign companies located in both China and foreign jurisdictions.[1] It has been reported that these Chinese state-owned firms have been highly successful in recruiting this high-tech engineering talent, which is enabled by massive Chinese government subsidies that allow for salaries to be offered at high, non-market rates.[2] Often high-level managers are lured away from targeted companies with compensation packages four or five times the market rate. These managers then target key former employees in technology development, manufacturing and facilities, promising outsized compensation.[3] In addition, in numerous publicly reported instances, individuals employed by Chinese state-owned firms and or their partners/affiliates have chosen to steal or misappropriate intellectual property, including trade secrets from their previous employer.[4] In sum, while it is unclear whether the IP theft and other related illegal activities are an official state-sanctioned means to achieving industrial policy goals, China's massive non-market industrial subsidies granted to state-owned enterprises

---

[1] China Poaching Taiwanese Tech Talent. Nikkei Asian Review, March 4, 2016: https://asia.nikkei.com/Business/Trends/Chinapoaching-Taiwanese-tech-talent.

[2] China Expected to Poach More Taiwan Chip Execs. EEtimes, January 1, 2017: https://www.eetimes.com/document.asp?doc_id=1331144.

[3] Exposing How Taiwan IC Engineers Jump Ship to the Mainland: Hired as Soon as They Depart With 2x-3x Salaries. EEtimes China, March 23, 2017: http://www.eet-china.com/news/article/201703231458; Talent Hunt in China's Memory Triangle. EETimes, January 26, 2017: https://www.eetimes.com/document.asp?doc_id=1331262, Taiwan Chipmakers Worried About Brain Drain, Asian Nikkei Review, April 29, 2017, https://asia.nikkei.com/Business/AC/Taiwan-chipmakers-worried-about-brain-drain.

[4] Authorities Bust Group Stealing Win Semiconductors Trade Secrets. Focus Taiwan, November 6, 2015 https://www.eetimes.com/document.asp?doc_id=1331144, Samsung Electronics Executives Pass on Core Technology. SBS News, September 22, 2016: http://v.media.daum.net/v/20160922211514100 (Korean).

create the conditions for encouraging bad actors to acquire key IP through improper means.

SIA applauds the enactment of the Defend Trade Secrets Act (P.L. 114-153), which provides a federal civil cause of action for the misappropriation of trade secrets, and several cases have been initiated in the semiconductor industry under this new authority. But civil remedies are not always available for some instances of trade secrets misappropriation, and therefore federal authorities must continue to prioritize theft of trade secrets for criminal prosecution and other penalties. We note that the Department of Justice and the Department of Commerce have recently taken action to address the misappropriation of trade secrets in the semiconductor industry,[5] and we call on the Administration to maintain a strong focus on the misappropriation of trade secrets.

II. Counterfeit Semiconductors

Because semiconductors are the "brains" behind a diverse range of end products, services and systems – including critical products such as healthcare and medical equipment, communication networks, transportation systems and controls, and military and security systems – semiconductor devices are designed and manufactured to meet exacting standards and the highest quality and reliability levels. Unfortunately, unscrupulous entities engage in counterfeiting of semiconductors, and many of these devices may enter the supply chain for critical products that are essential to health and safety.

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. While authentic semiconductors are complex products that are designed, manufactured and distributed under highly controlled conditions to meet exacting quality and reliability standards, counterfeit semiconductors are often salvaged from discarded electronic products ("e-waste") in a dirty, uncontrolled process that results in products that cannot be expected to operate reliably.[6] 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 or contract manufacturers.

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

[5] DOJ has announced a new initiative to combat IP theft from China, see https://www.justice.gov/opa/speech/file/1107256/download, and Commerce has recently taken action against one Chinese state-owned semiconductor company for using misappropriated technology in the development of its own products. See 83 Fed. Reg. 54,519 (Oct. 30, 2018).

[6] The Commerce Department Bureau of Industry and Security is currently exploring whether to impose new export control regulations on electronic waste as a means of addressing concerns regarding counterfeit goods that may enter the U.S. military and civilian electronics supply chain. 83 Fed. Reg. 53,411 (Oct. 23, 2018).

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.[7] During a follow-up Joint Customs Operation of EU Customs supported by U.S Customs and Border Protection, EUROPOL, and OLAF (European Anti-Fraud Office) in 2016, more than one million counterfeit integrated circuits were seized within a two week period.

Because semiconductors are an essential component in downstream electronic products, the harms from counterfeit semiconductors are disproportionately higher than most other counterfeit products, even where the monetary value of the semiconductor itself may be lower than other types of counterfeits. The harms include:

- Consumer losses can be multiples of the cost of the counterfeit semiconductor; for example, a $.50 counterfeit semiconductor can cause a $500 computer to fail.

- Instead of a sudden failure, a counterfeit semiconductor might degrade over time. A defective semiconductor in test equipment used to screen products exiting the factory floor can cause inaccurate readings that “pass” products that in fact do not meet specifications.

- Semiconductors are used in many applications with health and safety implications. There are actual examples of counterfeits found in, or destined for, an Automated External Defibrillator (AED), a braking system for high-speed trains in Europe, automotive braking systems and automotive airbag deployment systems, a power supply system used for airport landing lights. automated medication applications, including intravenous (IV) drip machines.[8] The consequences of using a counterfeit semiconductor that can result in product malfunction are obvious.

The risks posed by the infiltration of counterfeit semiconductors into national security systems is 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:

---

[7] SIA White Paper, *“*Winning the Battle Against Counterfeit Semiconductor Products” at p. 8, available at https://www.semiconductors.org/wp-content/uploads/2018/01/SIA-Anti-Counterfeiting-Whitepaper.pdf.
[8] World Semiconductor Council AntiCounterfeiting White Paper, p. 5, https://www.semiconductors.org/wp-content/uploads/2018/01/SIA-Anti-Counterfeiting-Whitepaper.pdf

> 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. Unfortunately, a flood of counterfeit electronic parts has made it a lot harder to prevent that from happening.[9]

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.[10] 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."[11] The Department of Defense has identified counterfeits as one area of concern in its strategy to ensure trusted and assured access to microelectronics.[12]

The Joint Strategic Plan on Intellectual Property Enforcement should include two specific measures with regards to semiconductor counterfeiting.

First, federal agencies should engage in renewed efforts to minimize the prevalence of counterfeit microelectronics by improving their procurement practices and employing a tiered approach in purchasing legitimate semiconductors from the authorized distribution chain.[13] 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.[14] Semiconductor companies generally avoid the creation of "legacy" products by

---

[9] Senate Armed Services Committee, *Inquiry Into Counterfeit Electronic Parts In The Department of Defense Supply Chain* at i. (May 21, 2012) ("SASC Report").
[10] SASC report at 9.
[11] *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.
[12] Department of Defense Response to National Defense Authorization Act for FY2017, Section 231: Strategy for Ensuring Access to Assured Microelectronics, available at https://www.acq.osd.mil/se/docs/2018-NDAA231-A.pdf.
[13] Winning the Battle Against Counterfeit Semiconductor Products at 21-22.
[14] Aftermarket manufacturers are entities who work with OCMs and stockpile billions of legacy components or are authorized by OCMs to produce legacy products using the same wafer fabrication process flows and tooling as well as the same packages as the original products. Id. at 21.

providing customers with notice in advance of the discontinuance of products, in accordance with industry standards.[15] 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.

Second, the Joint Strategic Plan on Intellectual Property Enforcement must require law enforcement agencies such as Customs and Border Protection (CBP) to prioritize the seizure of semiconductor counterfeits and the prosecution of counterfeiters. As noted in the enumeration of harms above, the harms from counterfeit semiconductors are disproportionately higher than most other counterfeit products. CBP metrics that track the dollar value of counterfeits seized underestimate the impact that seizures of counterfeit semiconductors have on health, safety, and national security. CBP and other agencies should prioritize their enforcement efforts based on the risk of harm from counterfeit products, not simply the dollar value of the product.

CBP seizures of counterfeit semiconductors have declined in recent years, which raises the question: Are there fewer counterfeit semiconductors, or are the counterfeits becoming harder to detect, or has CBP deemphasized semiconductor operations? Anecdotal evidence from SIA member companies suggests that it is primarily the latter two options and not a decrease in counterfeiters' efforts. It is time for CBP to again step up and focus on stopping semiconductor counterfeits.

Finally, in taking action against counterfeit semiconductors, it is also imperative that CBP and other agencies collaborate with brand owners. Semiconductor companies have the expertise to make the complex assessment of whether a device is authentic and counterfeit. SIA member companies have worked to train CBP officials on counterfeit semiconductors, and we urge enforcement agencies to continue this partnership. Among other things, enforcement agencies should share information with the industry in determining whether particular devices are counterfeit.

\+ + +

SIA appreciates the opportunity to contribute to the IP enforcement strategic plan.

---

[15] 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/).