

**Before the House Committee on Homeland Security
Subcommittee on Oversight, Investigations and Management**

Counterfeit Semiconductors – A Clear and Present Threat

July 7, 2011

Testimony of Brian Toohey, President, Semiconductor Industry Association

Executive Summary

The importation of counterfeit semiconductor “chips” is a growing national security threat. For years, manufacturers abroad (primarily in China) have used crude techniques, including open fires, surface sanding, and acid washes, to turn “e-waste” into counterfeit semiconductors. These chips – already weakened from their original state and at great risk of failure – are then re-labeled using digital printing and laser etching and packaged for sale to international brokers. However, counterfeiters have begun acquiring more sophisticated equipment and advanced counterfeiting techniques, making it increasingly difficult to identify counterfeit semiconductors. As a result, more and more counterfeit chips make it through our borders and into a wide range of products, including automobile technology such as brake systems, health care technology such as defibrillators, and, most troublingly, into military equipment such as missiles, navigation systems, and jets. Given their high failure risk, counterfeit infiltration places our citizens and military personnel in unreasonable peril.

SIA appreciates the Obama Administration’s commitment to intellectual property rights and its resolve to prevent counterfeit goods from entering the United States supply chain. Immigrations and Customs Enforcement (“ICE”), the Federal Bureau of Investigation (“FBI”), the Department of Justice (“DOJ”) and the Department of Defense (“DOD”) have all played crucial roles in combating the infiltration of counterfeit goods.

Historically, Customs and Border Protection (CBP) has also facilitated anti-counterfeiting efforts. Prior to 2000 when Port Officers suspected a shipment contained counterfeit chips, they would contact the trademark owner and share one of the products. After 2000 but before 2008, Port Officers photographed the outside of a suspect chip and sent the publicly viewable information to the chip manufacturer whose trademark appeared on the surface of the chip to determine whether the chip was counterfeit. Using a highly confidential database, the trademark owner could then determine very quickly, in almost 85% of the requests, whether or not the chips were counterfeits by analyzing the codes on the surface of the chip.

In mid-2008, however, CBP Officers were instructed to redact any identifying marks in the photographs, except the trademark, before sending them to manufacturers, thereby scuttling the cooperative system that worked so well for eight years. The current redaction practice makes it impossible for the industry, much less the importer or CBP, to authenticate suspected counterfeit semiconductors. U.S. Treasury officials argue that its policy shift is intended to shield Port Officers from criminal liability for the disclosure of confidential information. However, to the extent the codes on the surface of semiconductors, which are

publicly viewable to anybody who picks up a chip or looks at a chip's packaging label, are confidential, they belong to the manufacturers to whom photographs would be sent.

SIA simply asks CBP to revert to its historical pre-2008 practice and share unredacted photographs, and where necessary physical products, of suspected counterfeit semiconductors with semiconductor manufacturers. Such a policy is clearly in the nation's national security interest. Preventing counterfeit semiconductors from entering the U.S. will protect public safety and safeguard the military supply chain.

Chairman McCaul, Ranking Member Keating, and other members of the Subcommittee, my name is Brian Toohey. I am the President of SIA, the Semiconductor Industry Association (“SIA”). I thank the Committee for inviting me to testify about the dangers that counterfeit semiconductors pose to the U.S. military and the civilian population at large, as well as the common-sense steps the Obama Administration can take to prevent counterfeit semiconductors from entering highly sensitive military and civilian supply chains. This issue is more and more important as semiconductors are being used in an increasing number of mission critical applications such as medical lifesaving equipment, car brakes and air bag systems, nuclear reactors, airplanes and military weapon systems.

SIA is the voice of the U.S. semiconductor industry, America's largest export industry since 2005 and a bellwether of the U.S. economy. Semiconductor innovations form the foundation for America's \$1.1 trillion dollar technology industry affecting a U.S. workforce of nearly 6 million. Founded in 1977 by five microelectronics pioneers, SIA unites more than 60 companies from across the United States that account for 80 percent of the Nation’s semiconductor production. Our industry has an especially robust presence in Texas and Massachusetts, with SIA members AMD, Freescale, Intel, STMicroelectronics and Texas Instruments in Texas, and Analog Devices, Intel, Maxim and Rochester Electronics in Massachusetts. SIA seeks to strengthen U.S. leadership in semiconductor design and manufacture by working with Congress, the Administration and other industry groups to enable the right ecosystem for technology development and commercialization. Specifically, SIA encourages policies and regulations that fuel innovation, propel business and drive international competition in order to maintain a thriving semiconductor industry in the United States.

Background on Semiconductors

Semiconductor “chips” are used in everything that is computerized or uses radio waves. Indeed, semiconductors are components in a staggering variety of products, from computers and smart phones to medical devices, LEDs and smart meters, automobiles and military equipment, including missiles, navigation systems and jets. They are making the world around us smarter, greener, safer, and more efficient. They are also economically vital to the nation. In 2010, U.S. semiconductor companies generated over \$140 billion in sales — representing nearly half the worldwide market, and making semiconductors the Nation’s largest export industry. Our industry directly employs nearly 200,000 workers in the U.S., and another 6 million American jobs are made possible by the use of semiconductors. Studies show that semiconductors, and the information technologies they enable, represent 3 percent of the economy, but drive 25 percent of economic growth.

Increasing Prevalence of Counterfeits

Due to the increasing availability and decreasing price of equipment needed to counterfeit semiconductors, unscrupulous brokers looking to garner illicit profits are importing

ever greater numbers of counterfeit chips into the United States. In fact, the Department of Commerce has reported that counterfeit incidents discovered by the military and military suppliers more than doubled between 2005 and 2008, from 3,868 to more than 9,356 cases.¹ Alarmingly, these counterfeit chips can be found in automobile airbag systems, defibrillators, and even highly sensitive military equipment. As *BusinessWeek* explains:

The American military faces a growing threat of potentially fatal equipment failure – and even foreign espionage – because of counterfeit computer components used in warplanes, ships, and communications networks. Fake microchips flow from unruly bazaars in rural China to dubious kitchen-table brokers in the U.S. and into complex weapons. Senior Pentagon officials publicly play down the danger, but government documents, as well as interviews with insiders, suggest possible connections between phony parts and breakdowns. In November 2005, a confidential Pentagon-industry program that tracks counterfeits issued an alert that “BAE Systems experienced field failures,” meaning military equipment malfunctions, which the large defense contractor traced to fake microchips....In a separate incident last January, a chip falsely identified as having made by Xicor...was discovered in the flight computer of an F-15 fighter jet at Robins Air Force Base....Special Agent Terry Mosher of the Air Force Office of Special Investigations confirms that the 409th Supply Chain Management Squadron eventually found four counterfeit Xicor chips.²

Some experts have estimated that as many as 15 percent of all spare and replacement semiconductors purchased by the Pentagon are counterfeit.³

Many counterfeit chips are traced back to China. *BusinessWeek* writers visited China and described the counterfeiting economy as follows:

The traders typically obtain supplies from recycled-chip emporiums such as the Guiyu Electronics Market outside the city

¹ U.S. Department of Commerce, Defense Industrial Base Assessment: Counterfeit Electronics available at http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf; see also Michele Moss, *Systems Assurance, The Global Supply Chain, and Efforts to Increase Communication Between Acquisition and Development*, available at http://www.dtic.mil/ndia/2010CMMI/WednesdayTrack4_11328Moss.pdf; *Surge in counterfeit items in Pentagon's supplies*, Homeland Security Newswire, Aug. 10, 2010, available at <http://www.homelandsecuritynewswire.com/surge-counterfeit-items-pentagons-supplies>.

² Brian Grow et al., *Dangerous Fakes: How counterfeit, defective computer components from China are getting into U.S. warplanes and ships*, *BusinessWeek*, Oct. 2, 2008, available at http://www.businessweek.com/magazine/content/08_41/b4103034193886.htm.

³ *Id.*

of Shantou in southeastern China. The garbage-strewn streets of Guiyu reek of burning plastic as workers in back rooms and open yards strip chips from old PC circuit boards. The components, typically less than an inch long, are cleaned in the nearby Lianjiang River and then sold from the cramped premises of businesses such as Jinlong Electronics Trade Center. A sign for Jinlong Electronics advertises in Chinese that it sells “military” circuitry, meaning chips that are more durable than commercial components and able to function at extreme temperatures. But proprietor Lu Weilong admits that his wares are counterfeit. His employees sand off the markings on used commercial chips and relabel them as military. Everyone in Guiyu does this, he says: “The dates [on the chips] are 100% fake, because the products pulled off the computer boards are from the ‘80s and ‘90s, [while] consumers demand products from after 2000.”⁴

While the Chinese have admitted the prevalence of semiconductor counterfeiting in China, Chinese officials claim they can do little about the counterfeiting. As Wayne Chao, secretary general of the China Electronics Publishing Association and anticounterfeiting advocate said, “[e]veryone wants to blame China. But it’s difficult to differentiate between a legitimate product and a fake.”⁵

Administration Resolve to Combat Counterfeits

Mr. Chao is correct – it is difficult to differentiate between a legitimate semiconductor and a fake. And it is precisely because of the difficulties inherent in differentiating between a legitimate and counterfeit semiconductor that the government must place a single-minded emphasis on preventing the importation of counterfeit chips.⁶ Thankfully, the Obama Administration—like the previous Bush and Clinton Administrations—has shown an admirable resolve to combat counterfeiting and other forms of intellectual property theft. Indeed, President Obama himself has promised:

We’re going to aggressively protect our intellectual property. Our single greatest asset is the innovation and the ingenuity and creativity of the American people. It is essential to our prosperity and it will only become more so in this century.⁷

⁴ *Id.*

⁵ *Id.*

⁶ See Exhibit 1, a photograph comparing a genuine and counterfeit semiconductor.

⁷ Victoria Espinel, 2010 Joint Strategic Plan on Intellectual Property Enforcement 3, available at http://www.whitehouse.gov/sites/default/files/omb/assets/intellectualproperty/intellectualproperty_strategic_plan.pdf (“IPEC Report”).

Last year, DOJ, ICE, the Office of Homeland Security Investigations, Naval Criminal Investigative Service (“NCIS”), Postal Inspection Service, Internal Revenue Service, Department of Transportation and General Services Administration worked together with the semiconductor industry on an investigation that led to the indictments of the principals of a Florida-based company that generated nearly \$16 million in gross receipts between 2007 and 2009 by importing nearly 60,000 counterfeit semiconductors from China and selling them to the military as “military grade.”⁸ As the U.S. Attorney in charge of the investigation explained:

Product counterfeiting, particularly of the sophisticated kind of equipment used by our armed forces, puts lives and property at risk. This case shows our determination to work in coordination with our law enforcement partners and the private sector to aggressively prosecute those who traffic in counterfeit parts.

The Obama Administration’s Intellectual Property Enforcement Coordinator, Victoria Espinel, also understands the importance of enforcing intellectual property laws and preventing the importation of counterfeit semiconductors. In the Administration’s 2010 Joint Strategic Plan on Intellectual Property Enforcement, Ms. Espinel explained the vital role of intellectual property enforcement in protecting the consumer safety and national security:

Violations of intellectual property rights, ambiguities in law and lack of enforcement create uncertainty in the marketplace, in the legal system and undermine consumer trust. Supply chains become polluted with counterfeit goods. Consumers are uncertain about what types of behavior are appropriate and whether the goods they are buying are legal and safe. Counterfeit products can pose a significant risk to public health, such as...military systems with untested and ineffective components to protect U.S. and allied soldiers, auto parts of unknown quality that play critical roles in securing passengers and suspect semiconductors used in life-saving defibrillators....Intellectual property infringement [also] can undermine our national and economic security. This includes counterfeit products entering the supply chain of the U.S. military, and economic espionage and theft of trade secrets by foreign citizens and companies.⁹

⁸ Press Release, U.S. Department of Justice, Owner and Employee of Florida-based Company Indicted in Connection with Sales of Counterfeit High Tech Devices Destined to the U.S. Military and Other Industries (Sept. 14, 2010), available at <http://www.justice.gov/criminal/cybercrime/wrenIndict.pdf>; Spencer H. Hsu, *U.S. charges Florida pair with selling counterfeit computer chips from China to the U.S. Navy and military*, Washington Post, Sept. 14, 2010, available at <http://www.washingtonpost.com/wp-dyn/content/article/2010/09/14/AR2010091406468.html>.

⁹ IPEC Report at 4.

Unfortunately, despite the Obama Administration's understanding of the dangers posed by counterfeit semiconductors, a 2008 Customs and Border Protection ("CBP") action required by the Department of the Treasury is frustrating the efforts of other government agencies to combat the importation of counterfeit chips.

CBP Action Halts Industry Assistance in Combatting Counterfeiting

Historically, when a CBP Port Officer suspected that an imported semiconductor was counterfeit, CBP would send the manufacturer of the semiconductor (as identified by the trademarks featured on the semiconductor) either a sample of a suspect semiconductor or a photograph of the surface of the suspect chip. The surface of semiconductors contain identifying manufacturing marks – these usually represent part number, lot number, date of manufacture and place of manufacture – all in clear sight to anyone looking at the chip. The meaning of these identifying marks, however, is known only to the manufacturer – and only the manufacturer of the semiconductor can identify the authenticity of the chip using highly confidential and proprietary company-specific databases. After receiving a photograph of a suspected counterfeit chip, a semiconductor manufacturer would quickly locate the specific product in its internal computer systems, determine the product's authenticity, and inform CBP of its determination. CBP could then seize the counterfeit chips. While this policy did not prevent all counterfeits from entering the country, it did lead to numerous successful raids of counterfeit manufacturers in China and brokers in the United States.¹⁰

Unfortunately, in August 2008 manufacturers discovered that Customs Officers had been ordered to stop sending photographs (or samples) of suspect chips showing the information required by a manufacturer to authenticate a chip, even though CBP had been sending such photographs for nearly eight years. Instead, CBP began sending redacted photos that obscured identifying information and left only the manufacturer's trademark visible. Given the advanced labeling technology now available to counterfeiters, manufacturers cannot determine whether chips are counterfeit based on these logo-only pictures. Unsurprisingly, before August 2008, seizures of counterfeit semiconductors were increasing year after year. Since CBP changed its policy, SIA members have reported receiving an increased number of complaints about counterfeits. Semiconductor manufacturers were not notified or provided an opportunity to comment before CBP began implementing the new policy: one day in August 2008, the identifying markings on photographs sent to manufacturers were simply redacted.

The CBP's new post-2008 redaction practice is based on an April 2000 Customs Directive¹¹ which instructed Customs Officers to "remove or obliterate any information indicating the name and/or address of the manufacturer, exporter, and/or importer, including

¹⁰ See note 8; Press Release, U.S. Department of Justice, Three California Family Members Indicted in Connection with Sales of Counterfeit High Tech Parts to the U.S. Military (Oct. 9, 2009), *available at* <http://www.justice.gov/criminal/cybercrime/aljafflndict.pdf>.

¹¹ Customs Directive No. 2310-008A (April 7, 2000), *available at* <http://www.cbp.gov/linkhandler/cgov/trade/legal/directives/2310-008a.ctt/2310-008a.pdf>.

all bar codes or other identifying marks” before providing samples of chips suspected to bear “confusingly similar” trademarks to semiconductor manufacturers. Of course, Customs Officers understood that this policy could not effectively prevent the importation of counterfeit semiconductors, and did not interpret the restrictive Directive to apply to photographs until August 2008 when, we have been told, CBP Port Officers were “reminded” by Treasury officials that the April 2000 Directive applies to photographs.

Customs Needs Industry Support to Prevent the Importation of Counterfeit Semiconductors

CBP cannot effectively prevent the importation of counterfeit semiconductors without the industry’s assistance. A semiconductor is very different from apparel, for example, where a photograph of a fake Gucci handbag redacted per the Customs Directive’s instructions likely still provides sufficient information for an intellectual property rights holder to determine the authenticity of merchandise. In contrast, semiconductor manufacturers use common exterior packages (which fit in common board sockets) for their semiconductors. Moreover, counterfeiters have obtained professional laser etching equipment to place fake codes on counterfeit chips. Thus, it is nearly impossible to determine whether a given chip is legitimate or counterfeit based on the redacted photographs.¹²

Semiconductor manufacturers can only assist CBP in preventing importation of counterfeit merchandise if CBP provides manufacturers with sufficient information to determine whether suspect chips are authentic. An unredacted photograph of a suspect chip would ordinarily be sufficient to provide the manufacturing codes (that usually represent lot numbers, dates and locations of manufacture) that a manufacturer needs to authenticate a chip. Alternatively, CBP could provide manufacturers with these numbers or a sample chip. However, a photograph that has been redacted to remove these numbers does not provide sufficient information to determine the authenticity of a chip. Unless CBP provides manufacturers unredacted photographs of suspect chips (or provides the manufacturing codes and dates and locations of manufacture reflected on the face of the suspect chips that only manufacturers can decipher), CBP cannot discharge its statutory obligation to ensure that imports comply with U.S. intellectual property laws. In such circumstances, the risk that counterfeit chips will enter U.S. commerce and ultimately end up as components in commercial, industrial and military devices increases as we have witnessed since Treasury’s policy shift.

Customs Has the Authority to Get Industry Help

The most frustrating aspect of the current policy is the fact that CBP has all the legal authority necessary to provide semiconductor manufacturers with the information necessary to stem the tide of counterfeit chips. Treasury officials have claimed that the 2000 Directive is meant to protect Customs Officers from liability under the Disclosure of Confidential

¹² See Exhibit 1.

Information (“DCI”) provision of the Trade Secrets Act.¹³ However, such protection is unnecessary, as Customs Officers are only exposed to DCI liability to the extent that CBP decides that information is confidential.¹⁴ Therefore, CBP can effectively protect Customs Officers by simply declaring that the information included on the surface of semiconductors is not confidential information, as it had implied prior to its policy shift. Indeed, it is unclear how a code that is readily visible to anyone looking at the product label on a container containing semiconductors or the surface of a semiconductor can be confidential information. Tellingly, when Customs promulgated the rule that the 2000 Directive was intended to “fix,”¹⁵ it identified two potential trade secrets that might be divulged when disclosing information: the identity of the manufacturer and the identity of the importer.¹⁶ But sharing the codes on the surface of semiconductors and product labels on the packaging with semiconductor manufacturers would not reveal either, as the manufacturer knows its own identity and the surface codes reveal no information about a chip’s importer.

CBP has failed to understand that even if the publicly viewable codes were confidential, Congress clearly contemplated CBP disclosing such information to rights holders in order to permit CBP to fulfill the many laws and treaties requiring it to stop counterfeits from entering the U.S. The DCI simply prohibits government officials from disclosing confidential information that “concerns or relates to ... the identity ... of any person” to “any extent not authorized by law.” Accordingly, Congress has authorized CBP to provide unredacted photos to semiconductor manufacturers through the Tariff Act of 1930, the Lanham Act, the North American Free Trade Agreement and the GATT Agreement on Trade-Related Aspects of Intellectual Property Rights. In addition, CBP’s own Disclosure of Information Regulation authorizes such disclosure.¹⁷ It is truly difficult to understand why CBP believes disclosing information to semiconductor manufacturers is unlawful when ICE, DOD, DOJ, NCIS, and even the FBI – the agency tasked with enforcing the Trade Secrets Act – do not, and in fact routinely disclose such information to semiconductor manufacturers.

¹³ 18 U.S.C. § 1905.

¹⁴ In *United States v. Wallington*, 889 F.2d 573 (5th Cir. 1989), the Fifth Circuit logically found that the DCI only prohibits the disclosure of confidential information. In addition, the Fifth Circuit clarified that Customs agents cannot be held liable for DCI violations without “*at least*...knowledge that the information is confidential in the sense that its disclosure is forbidden by agency official policy (or by regulation or law).” Thus, since the Trade Secret Act does not address the information at issue, CBP Officers could be shielded from any potential DCI liability (to the extent such liability may exist) with a stroke of a pen if CBP were to clarify the Directive to permit Customs agents to share with semiconductor manufacturers unredacted photographs.

¹⁵ 19 C.F.R. § 133.25 (“Customs may disclose to the owner of the trademark or trade name...in order to obtain assistance in determining whether an imported article bears an infringing trademark or trade name...[a] description of the merchandise”).

¹⁶ Copyright/Trademark/Trade Name Protection; Disclosure of Information, 63 Fed. Reg. 11996, 11997 (Mar. 12, 1998); see also Gray Market Imports and Other Trademarked Goods, 64 Fed. Reg. 9058 (Feb. 24, 1999).

¹⁷ See note 15.

Conclusion

As a trade association that represents one of America's most vital industries, SIA hopes that all executive agencies will support the Obama Administration's intellectual property enforcement efforts by resolving this counterfeit issue expeditiously. Counterfeit semiconductors are a clear and present national security threat and danger to human health because they are used in many mission critical applications. SIA is pleased with the efforts by the U.S. Attorney for the District of Columbia, ICE, NCIS, and other Federal law enforcement agencies to bring to justice unscrupulous brokers selling dangerous counterfeits into the civilian and military supply chain. However, the 2000 CBP policy, further refined in 2008, prevents the U.S. government from most effectively working with industry to prevent counterfeit chips from being imported into the United States. This is alarming, especially given the danger such chips so obviously present.

We respectfully request this Subcommittee and Congress to work with CBP and Treasury to ensure that the pre-2008 practice of sharing unredacted pictures of suspected counterfeit semiconductors and product labels with manufacturers is reinstated in the interest of safeguarding the health and safety of the American public and our military.

Exhibit 1



Authentic



Counterfeit

Voltage Regulator for Automotive Airbag & Brake Systems