Before the Senate Committee on Armed Services
Counterfeit Electronic Parts in the U.S. Military Supply Chain
November 8, 2011

Counterfeit Semiconductors – A Clear and Present Threat
Testimony of Brian Toohey, President, Semiconductor Industry Association

Executive Summary

Chairman Levin, Ranking Member McCain, and other members of the Senate Committee on Armed Services, my name is Brian Toohey. I am the President of SIA, the Semiconductor Industry Association. I thank the Committee for inviting me to testify about the dangers counterfeit products and specifically semiconductors pose to the U.S. military and the civilian population at large.

The importation of counterfeit semiconductor "chips" is a growing national security threat. For years, counterfeiters abroad (primarily in China) have used crude techniques, including open fires, surface sanding, and acid washes, to turn "e-waste" into counterfeit semiconductors. This is in stark contrast to SIA Members high-quality production of semiconductors. The counterfeits are re-labeled using digital printing and laser marking and packaged for sale to international brokers. The processes used for converting these chips to remarks or counterfeits weakens them and ensures that they will fail sooner than expected and/or not perform to specification. However, counterfeiters have begun acquiring more sophisticated equipment and advanced counterfeiting techniques, making it increasingly difficult to identify counterfeit semiconductors.

This puts tools, systems, vehicles, and missions at great risk of failure and endangers lives. As a result, more and more counterfeit chips make it through our borders and into a wide range of technologies, including automotive products such as brake systems, medical devices such as defibrillators, and, most troublingly, into military equipment such as missiles, navigation systems, and jets. Given the high risk of failure, counterfeit infiltration places our military personnel and citizens, critical infrastructure and mission-critical applications across the United States and the world in unreasonable peril.

To address the threat with military applications, SIA and the Department of Defense (DOD) have been working closely to develop a new product authentication process to increase the ability of our industry, with DOD and other agencies to work more cooperatively to identify counterfeit products and potentially their sellers or importers. Our goal is to develop a process that will make both industry and government more effective and timely in fighting counterfeiters. The SIA Anti-Counterfeiting Task Force (ACTF), DOD, as well as NASA, Jet Propulsion Laboratory, and other trade associations and companies formed the DOD Working Group. The Working Group has created a Product Identification/Authentication Request Form that will assist government agencies in requesting authentication services, from the manufacturer, for suspect products

found during acquisition or already in the government supply chain. That form and authentication process are in the final review stage. The next Working Group project will be to draft recommendations for better procurement procedures for mission-critical and life/safety products to avoid procuring counterfeit products or products with embedded malware and back doors. Finally, SIA's Anti-Counterfeit Task Force, DOD and other government agencies are participating in the Department of Justice's D.C. Counterfeit Microelectronics Working Group where government agencies and industry exchange information on counterfeiting and anti-counterfeiting activities with a focus on identifying, investigating and prosecuting people that make or sell counterfeits in the United States.

Unfortunately, a U.S. Customs and Border Protection (CPB) policy is undermining our cooperative anti-counterfeiting partnership with DOD and could endanger working relationships with other Federal law enforcement agencies. Despite our efforts with DOD and others, today the number of counterfeit semiconductors coming into the United States is on the rise and unfortunately is being inadvertently aided by the application of this policy.

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, for 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 CBP, to authenticate suspected counterfeit semiconductors. CBP officials argue this change in practice 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 by 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 and not the importer.

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 their original manufacturers. Such a policy is clearly in the nation's interest to continuously improve our security. Preventing counterfeit semiconductors from entering the U.S. will safeguard the military supply chain and protect public health and safety.

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, radar, navigation systems and jets. They are making the world around us smarter, greener, safer, and more efficient. They form that backbone of our critical infrastructure and are economically vital to the nation's growth and productivity.

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 on a five year average. Our industry directly employs nearly 200,000 workers in the U.S. Studies show that semiconductors, and the information technologies they enable, represent three percent of the economy, but drive 25 percent of economic growth.

Background on the SIA

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 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 Arizona, California, Colorado, Idaho, Maine, Massachusetts, New York, New Hampshire, North Carolina, South Carolina, Oregon, Rhode Island, Texas and Virginia.

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.

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]

[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*

In July of this year Greg Schaffer, the acting deputy undersecretary for the DHS National Protection and Programs Directorate, provided testimony to the House Oversight and Government Reform Committee. During the hearing Schaffer was asked, and admitted that DOD had purchased counterfeit electronic products with embedded security risks that were found in the DOD supply chain.[2]

Schaeffer went on to say, "imported consumer electronics have been sold in this country containing malware or spyware. Unknown foreign parties have preloaded the devices with code that could compromise security." Schaffer added, "many devices made in the U.S. contain foreign components and that it is possible that these components could also contain malware."[3]

Alarmingly, counterfeit chips can be found in automobile airbag systems, defibrillators, and even highly-sensitive military equipment. As a 2008 *BusinessWeek* article 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 been 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.[4]

Some experts have estimated that as many as 15 percent of all spare and replacement semiconductors purchased by the Pentagon are counterfeit.[5]

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

---

supplies, Homeland Security Newswire, Aug. 10, 2010, *available at* http://www.homelandsecuritynewswire.com/surge-counterfeit-items-pentagons-supplies.

[2] *DHS: Imported Devices Infected with Malware*, https://infosecisland.com/blogview/15095-DHS-Imported-Devices-Infected-with-Malware.html.

[3] *DHS: Imported Consumer Tech Contains Hidden Hacker Attack Tools*, http://www.datamation.com/news/dhs-imported-consumer-tech-contains-hidden-hacker-attack-tools-.html.

[4] 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.

[5] Id.

> The traders typically obtain supplies from recycled-chip emporiums such as the Guiyu electronics Market outside the city 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."[6]

The methods used by the counterfeiters to produce counterfeit chips differ significantly from those of our semiconductor manufacturers. Our members invest billions of dollars in state of the art facilities – most located in the U.S. – and manufacture semiconductors in ultra-clean rooms. The chips are then tested to make sure they function to their specifications and – in the case of many military specification circuits – further tested to rigid environmental standards. As noted above, the counterfeiters strip chips from eWaste – subjecting the chips to high temperature and vibration – then acid wash the leads, grind off the surface, literally wash them in a local river, dry them on the sidewalk, and re-top coat them and etch fake production codes on to the semiconductors' surface.

Using such a counterfeit chip is like playing Russian roulette. With luck, the chip will not function at all and will be discovered in testing. But in some cases the chip may work for a while, but because of the environmental abuse it could fail at a critical time – when the product containing the chip is stressed – as in combat. Attached is a detailed presentation of the various threats counterfeit chips pose to reliability, prepared by and submitted with the permission of Analog Devices, Inc. – an SIA member.[7]

While Chinese Officials have admitted to the prevalence of semiconductor counterfeiting in China, they claim they can do little about it. As Wayne Chao, secretary general of the China Electronics Publishing Association and anti-counterfeiting advocate said, "[e]veryone wants to blame China. But it's difficult to differentiate between a legitimate product and a fake."[8]

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

[6] Id.
[7] Attachment 1.
[8] Id.

legitimate and counterfeit semiconductor that the government must place a single-minded emphasis on preventing the importation of counterfeit chips.[9]

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.[10]

Last year, Department of Justice (DOJ), Immigration and Customs Enforcement (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."[11] 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.[12]

From 2006 to 2010, VisionTech Components knowingly sold counterfeit integrated circuits to approximately 1,101 buyers in the United States and abroad, including counterfeit integrated circuits destined for military applications. VisionTech shipped 75 counterfeit chips destined for naval vessel and land-based Identification Friend or Foe system. As the U.S. Attorney noted, "if the system failed during an engagement and could not identify an approaching threat aircraft 25 miles away, a missile fired from the threat aircraft could hit a ship one minute later."[13] Other shipments included 1,500 counterfeit memory chips destined for the Harm Testing System

---

[9] *See* Exhibit 1, a photograph comparing a genuine and counterfeit semiconductor.

[10] 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").

[11] 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.

[12] Id.

[13] Government's Consolidated Memorandum In Aid Of Sentencing and Motion for Downward Departure Pursuant to U.S.S.G. § 5K1.1, September 9, 2011 at 50.

installed on F-16s to track hostile radar systems,[14] 350 counterfeit ICs intended for an application in the Beam Steering Control Module board within Multiple Sub-Array of Testable Antenna for the U.S. Navy Cobra Judy Replacement Program,[15] 1,500 counterfeit chips to control the braking system in a high speed train,[16] and 196 counterfeit chips to be used in a hand-held portable nuclear identification tool, a device offered for sale on the FEMA (Federal Emergency Management Agency) website as suggested emergency equipment for first responders.[17] For her part in the scheme, VisionTech's administrator, Stephanie McCloskey, was sentenced to 38 months imprisonment and $166,141 in fines.

The VisionTech case has exposed a truly dangerous type of fraud our country is facing. Our industry is grateful to the investigators and prosecutors that have contributed to the successful prosecution and penalties. Lives are put at risk if these devices are not reliable, safe, effective and free of counterfeit parts. This is why it is absolutely imperative that counterfeiters and the people knowingly sell them – and who violate our trust – are brought to justice.

The Obama Administration's Intellectual Property Enforcement Coordinator (IPEC), 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.[18]

Cooperation Between DOD and the Semiconductor Industry

The SIA Anti-Counterfeiting Task Force and DOD have been collaborating to develop a new product authentication process to increase the ability of our industry and the U.S. government to work more cooperatively to identify counterfeit products and potentially their sellers or importers. Our goal is to develop a process that will make both industry and government more

[14] Id. at 51.
[15] Id. at 54.
[16] Id. at 55.
[17] Id at 56-57.
[18] IPEC Report at 4.

effective and timely in fighting counterfeiters. The SIA Anti-Counterfeiting Task Force (ACTF), DOD, as well as NASA, Jet Propulsion Laboratory, and other trade associations and companies formed the DOD Working Group. The Working Group has created a Product Identification/Authentication Request Form that will assist DOD and other government agencies in authenticating suspect products during acquisition or already in the government supply chain. That form and authentication process is in the final review stage.

In addition, last year DOJ started a cross-agency and cross-industry working group on microelectronics counterfeiting last year that has enabled better working relationships, information sharing and investigative coordination. This effort has contributed to current investigations into counterfeits being sold into the supply chain destined for DOD and their prime contractors and suppliers.

Finally, working with DOJ to convict felonious distributors, such as in the VisionTech case, will deter those who would profit from selling dangerous counterfeits into the military and civilian supply chain.

Current Government Purchasing Practices Increase Counterfeits in the DOD Supply Chain

The next Working Group project will be to draft recommendations for better procurement procedures for mission-critical and life/safety-critical products to avoid procuring products with embedded counterfeits.

Changing the procurement regulations requiring government contractors and subcontractors to purchase critical components from authorized brokers is another important step. Today's practice of purchasing based on low price allows the government to procure products containing semiconductors that can be either counterfeit or, even if authentic, doomed to fail unexpectedly because of improper salvage, storage, transportation and handling. We have picked, at random, some purchases made by DOD and found the seller to be not what they advertised. Such sellers are unable to guarantee that such products are authentic. Even if legitimate, such sellers are unable to ensure that the government receives products with a clear chain of custody and appropriate handling since leaving the manufacturer.

In some cases a simple Google Maps search shows that instead of a brick and mortar facility, as shown on the seller's web page, the products were being sold from an apartment or farm house. **The clear and present danger is that, unlike some other products, semiconductors, even if authentic, if mishandled, exposed to static electricity, harsh chemicals, or corrosive environments will either not perform to specification or will stop working long before expected.** This endangers military personnel and missions and at a minimum costs the government significant dollars to identify and replace the products even if the failure was minor.

The Semiconductor Industry Association respectfully recommends that the U.S. government, and in particular DOD, should change its purchasing policies to ensure that products critical to life, health, safety, mission-critical applications and critical infrastructure are purchased from the manufacturer's authorized distributors when available. When those products are no longer

available, such as legacy hardware five to 30 years old, then the government should implement new purchasing and product security processes. Buying critical components at low prices only saves money up front and in the end could cost DOD far more in lives, failed missions, and replacement costs.

CBP Action Halts Industry Assistance in Combating Counterfeiting

Unfortunately, despite the Obama Administration's understanding of the dangers posed by counterfeit semiconductors, and the excellent working relationship on anticounterfeiting between SIA, DOD, DOJ, NCIS, ICE, FBI and other federal agencies, **a 2008 Customs and Border Protection ("CBP") action is frustrating the efforts of those government agencies to combat the importation of counterfeit chips.**

Historically, when a CBP Port Officer suspected an imported semiconductor was counterfeit, CBP would send the semiconductor manufacturer (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 a semiconductor contains 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.[19]

However, in August 2008 manufacturers discovered 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. Not surprisingly, before August 2008, seizures of counterfeit semiconductors were increasing year after year.

Since CBP changed its practice, interdictions at the border have been down and SIA members have reported receiving an increased number of complaints about counterfeits from end customers when the chip fails. Semiconductor manufacturers were not notified or provided an

[19] *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/aljaffIndict.pdf.

opportunity to comment before CBP began implementing the new practice; 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 Directive which instructed Customs Officers to "remove or obliterate any information indicating the name and/or address of the manufacturer, exporter, and/or importer, including all bar codes or other identifying marks" before providing samples of chips suspected to bear "confusingly similar" trademarks to semiconductor manufacturers.[20] Of course, Customs Officers understood that this policy could not effectively prevent the importation of counterfeit semiconductors. The Officers 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 Manufacturers' Support to Prevent the Importation of Counterfeit Semiconductors

CBP cannot effectively prevent the importation of counterfeit semiconductors without the manufacturers/trademark owners' assistance. A semiconductor is very different from apparel, for example, where a photograph of a fake luxury 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 designs) for their semiconductors. Moreover, counterfeiters have obtained professional and up-to-date laser etching equipment to place fake codes on counterfeit chips. Thus, it is almost always impossible to determine whether a given chip is legitimate or counterfeit based on the redacted photographs.[21]

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 assembly) 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 assembly 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 increases that counterfeit chips will enter U.S. commerce and ultimately end up as components in**

[20] 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.
[21] See Exhibit 1.

commercial, industrial and military systems, as we have witnessed since Treasury's policy shift.

Customs Has the Authority to Enlist 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. CBP officials have claimed the 2000 Directive is meant to protect Customs Officers from liability under the Disclosure of Confidential Information ("DCI") provision of the Trade Secrets Act.[22] However, such protection is unnecessary, as Customs Officers are only exposed to DCI liability to the extent that CBP decides that information is confidential and may not be disclosed.[23] 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 the 2000 Directive was intended to "fix,"[24] it identified two potential trade secrets that might be divulged when disclosing information: the identity of the manufacturer and the identity of the importer.[25] 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

[22] 18 U.S.C. § 1905.

[23] 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.

[24] 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").

[25] 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).

authorizes such disclosure.[26] 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.

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 working together to reduce counterfeit imports 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 member companies have a long history of working side-by-side with Federal agencies, law enforcement and DOD to prevent counterfeits from entering the defense supply chain. We have: cofounded university research to maintain U.S. leadership in semiconductor technologies that are important for our defense, participated in the trusted foundry program to provide trusted devices for defense applications; and been advisors on measures to maintain the robust industrial base necessary for a vibrant defense supply chain.

We are pleased with the SIA-DOD Working Group's progress on creating a system for assisting our armed forces in detecting counterfeit chips already in the DOD supply chain. We are optimistic that the Working Group will also craft recommendations to reform government procurement practices to ensure that products critical to life, health, safety, mission-critical applications and critical infrastructure are purchased from the manufacturers' authorized distribution when available.

SIA is also pleased with the efforts by the U.S. Attorney for the District of Columbia, ICE, NCIS, FBI, and other Federal law enforcement agencies to bring to justice unscrupulous brokers selling dangerous counterfeits into the military and civilian supply chains. However, the post-2008 CBP policy 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 Committee and Congress work with DOD to require government contractors and subcontractors to purchase critical components from authorized sources. We also respectfully request this Committee and Congress to work with CBP 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.

[26] *See* note 24.

In summary the fight against counterfeiting and counterfeit products is to:

- Ensure that the critical infrastructure that supports our economy and citizens performs to expectations;
- Protect U.S. intellectual property and the U.S. jobs it supports;
- Safeguard the equipment we use, fly or drive or treat our illnesses; and,
- Ensure the safety and protection of our military in their day-to-day operations.