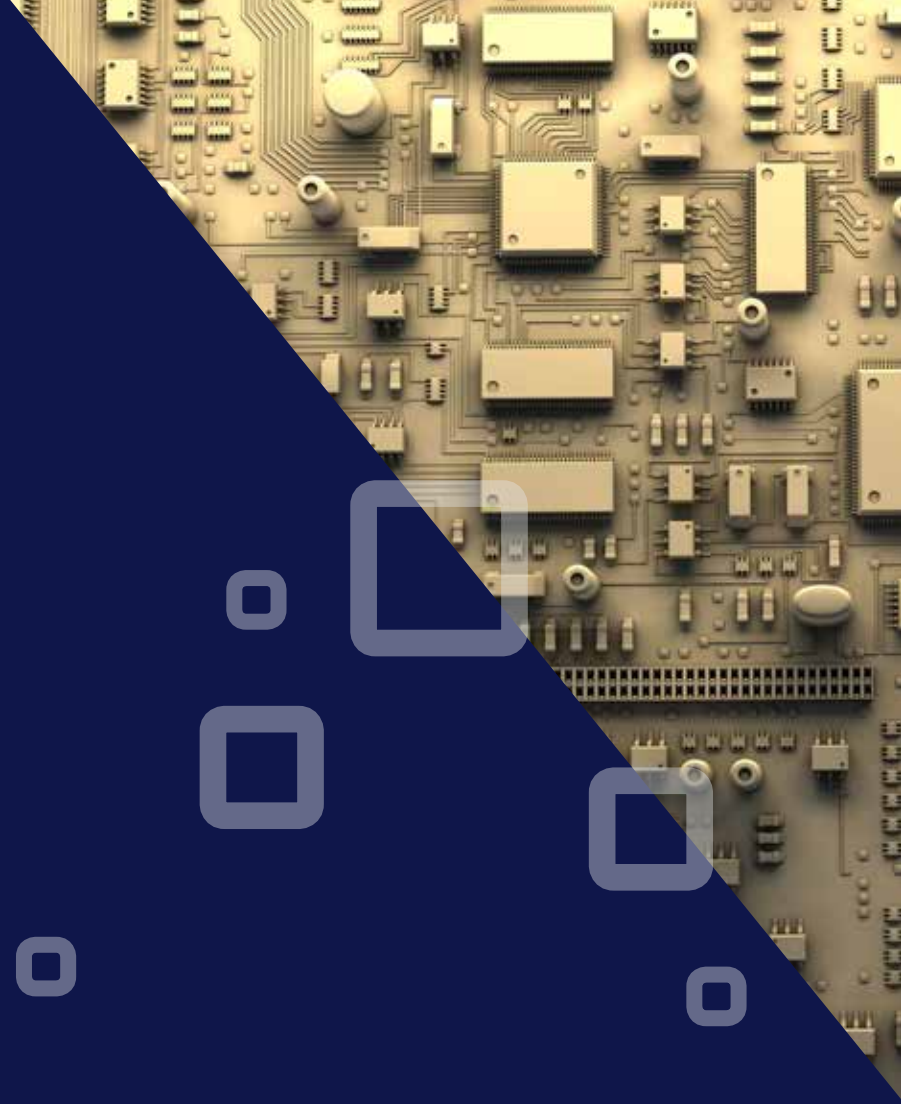

WINNING THE BATTLE AGAINST COUNTERFEIT SEMICONDUCTOR PRODUCTS

A report of the SIA Anti-Counterfeiting Task Force

August 2013

SIA SEMICONDUCTOR INDUSTRY ASSOCIATION

Winning the Battle Against Counterfeit Semiconductor Products

SIA Anti-Counterfeiting Task Force

August 2013

Executive Summary

As with every type of product, ranging from jewelry to wine to currency, semiconductor products can be counterfeited. Semiconductors are the "brains" inside critically-important electronic systems, including healthcare and medical equipment, electric power grids, communications systems, automotive braking and airbag systems, and military and aerospace systems. Because they control the operation of these and other vital electronics, counterfeit semiconductor components pose major risks to the health, safety, and security of people worldwide. Often harvested from electronic waste (e-waste), most counterfeit semiconductors are components re-marked to indicate they are newer than the original units or they perform to a higher standard. Semiconductor companies and their Authorized Distributors, Authorized Resellers, and Authorized Aftermarket Distributors/Manufacturers have extensive, proven controls to ensure products are properly manufactured, tested, handled, and stored to prevent failures. Counterfeiters have few if any such controls. The result is that, unlike legitimate semiconductors from authorized sources, counterfeits and other semiconductors available from non-authorized sources often have low quality and poor reliability.

Due to the dangers posed by counterfeits, the Semiconductor Industry Association (SIA) Anti-Counterfeiting Task Force (ACTF) continuously works to curtail the supply and demand for these illegal products and to educate customers on how to avoid purchasing counterfeits. The ACTF works closely with government agencies worldwide, including Customs and other law enforcement agencies, to identify and stop parties involved in manufacturing or trafficking in counterfeit goods. In addition, the ACTF has been instrumental in driving anti-counterfeiting legislation, regulations, and policies. The ACTF conveys counterfeit component avoidance strategies via conferences, webinars, and white papers.

Counterfeit semiconductor products have proliferated due to poor purchasing and supply chain practices. Counterfeit components reported to SIA member companies and reported through the Government-Industry Data Exchange Program (GIDEP) consistently involve purchases from open market sources that are not authorized by the Original Component Manufacturers (OCMs) to manufacture or sell semiconductor products. The open market includes independent distributors, brokers, and on-line component exchanges that obtain products from a wide range of suppliers. Unfortunately, some suppliers either intentionally or unknowingly introduce counterfeits into the open market supply chain.

The only way to ensure that semiconductor components are authentic, and have optimal quality and reliability levels, is to buy them exclusively through authorized sources. The upfront costs of products purchased through authorized sources are sometimes higher than those offered by open market sources. However, products purchased through authorized sources are usually more cost effective in the long term, since they have superior quality and reliability levels, and carry full factory warranties.

Table of Contents:

Note: Sections are hyperlinked to immediately take readers to the sections of most interest.

I. Background on Counterfeit Semiconductors

Reports of counterfeit semiconductors first became widespread during the 1997-2000 dot-com boom, but counterfeit semiconductors have been around since at least the 1970s. Although counterfeit semiconductors are not a new problem, there is no universally-accepted definition of counterfeit electronic components. In January 2010, the Bureau of Industry Security, which is part of the US Department of Commerce, published a report that defined a counterfeit electronic part as *"one that is not genuine because it: is an unauthorized copy; does not conform to original OCM design, model, or performance standards; is not produced by the OCM or is produced by unauthorized contractors; is an*

off-specification, defective, or used OCM product sold as "new" or working; or has incorrect or false markings or documentation, or both." [Reference 1.] This is an excellent definition for a counterfeit semiconductor, albeit rather lengthy. A task force of experts on counterfeit semiconductors from six worldwide semiconductor industry associations has agreed on the following more concise definition: "*Semiconductor counterfeiting is considered the act of fraudulently manufacturing, altering, distributing, or offering a product or package that is represented as genuine."* As with other counterfeit goods, counterfeiters are trying to trick purchasers into thinking they are buying legitimate products.

Until media coverage of counterfeit semiconductors became widespread in recent years, most people in the semiconductor and electronics industries had little or no awareness of counterfeit semiconductors. The prevailing view was that semiconductor products were too difficult and too expensive to counterfeit, and that the supply chain for semiconductors minimized the likelihood of counterfeits being introduced. While this view had some validity many years ago, four major changes since the mid-1990s have allowed counterfeit components to proliferate:

1. The dot-com boom in the late 1990s and subsequent periods of strong semiconductor demand resulted in extended lead-times and rising prices for semiconductor components that made these components attractive to counterfeiters.

2. Increased environmental awareness resulted in electronics waste (e-waste) no longer always ending up in landfills. Instead, electronic components were often removed from scrap circuit boards sent for "recycling," and some of these used components were then refurbished and re-marked to indicate they were new and/or higher performing components.

3. Tens of thousands of independent distributors and brokers worldwide established Internet sites to buy and sell semiconductor products outside of the traditional supply chain of OCMs and their Authorized Distributors/Resellers. As with other industries, the Internet and electronic commerce have facilitated the sale of counterfeit and otherwise questionable components due to the ease and speed at which companies and individuals can establish professional-looking Internet sites and then quickly change company names, web addresses, contact information, etc. in an effort to avoid liability.

4. Component purchasers increasingly focused on price and availability, often ordering semiconductor products from Internet-based brokers and on-line exchanges offering the lowest prices and "immediate" delivery.

While in the 1970s and 1980s there were negligible counterfeit semiconductors in the supply chain, beginning in the late 1990s, the combination of the above developments allowed counterfeit semiconductors to proliferate. Many Original Equipment Manufacturers (OEMs) and their Contract Manufacturers (CMs) were oblivious to the risks of counterfeit components until they encountered high failure rates in their production lines and/or large warranty claims that were subsequently found to be due to counterfeits. OEMs and CMs have understandably been reticent to publicize their problems and associated financial losses due to counterfeit components, but these losses can be huge. In addition,

field failures of electronic systems due to counterfeit components can severely damage the reputations of OEMs that otherwise provide reliable products. Fortunately, OEMs and CMs are able to easily avoid counterfeits by always buying semiconductor components either directly from OCMs or directly from OCMs' Authorized Distributors/Resellers. Many component buyers are not aware that older, out-of-production products that are not available through most OCMs' Authorized Distributors/Resellers, are still generally available through Authorized Aftermarket Distributors/Manufacturers who buy end-of-production products and/or obtain licensing to reproduce the original products. These Authorized Aftermarket Distributors/Manufacturers of legacy products literally have billions of older products that meet all of the storage, handling, transportation, performance and reliability requirements of the OCM. In many cases, these products are available for immediate delivery.

II. Overview of the Semiconductor Industry

Semiconductors are the "brains" inside an incredibly diverse range of end products and systems. These include products for:

- Everyday communications and entertainment: Computers, servers, cell phones, video games, digital cameras and camcorders, televisions, security systems, electronic tolls, networking, etc.;
- Healthcare and medical equipment: Patient monitoring including bedside-to-server data exchange systems, medical imaging including x-ray and CAT scan systems, pacemakers and defibrillators, blood pressure and heart rate monitors, robotic surgery equipment, etc.;
- Critical infrastructure: Electric power grids including nuclear and solar power generation systems, banking and stock market systems, local and national communication networks, emergency response systems, etc.;
- Industrial and automation systems: Motor control systems, thermal and vibration sensors, factory control systems, electronic test and measurement, environmental monitoring, etc.;
- Transportation systems and controls: Engine controls, braking systems, air bag systems, seat belt tensioners, collision avoidance radar, GPS navigation systems, train control systems, traffic lights, etc.; and
- Aerospace and defense: Navigation systems, flight control and radar systems, identification friend or foe (IFF) systems, space and satellite communication systems, missile systems, defense electronics, etc.

Semiconductor components are classified as either discrete devices, such as diodes and individual transistors, or Integrated Circuits (ICs), which consist of multiple transistors and other devices that are interconnected on one or more "chips" to form an electronic circuit. Discrete devices are sold in chip-form, wafer-form, or package-form, and they only have two or three electrical terminals. Average Selling Prices (ASPs) for a single discrete semiconductor range from less than one cent to hundreds of dollars. ICs are available in chip-form and wafer-form as well as a very wide range of package styles and sizes, with package pin/package solder ball counts ranging from just two to several thousand, depending on the complexity of the IC. Transistor counts for a given IC range from single-digits to hundreds of millions. Not surprisingly, given the extremely wide range in IC complexities and IC packages, ASPs for a single IC range from a few cents to tens of thousands of dollars.

III. The Semiconductor Industry Association [Reference 2]

SIA is the voice of the US semiconductor industry, one of America's top export industries and a bellwether of the US economy. Semiconductor innovations form the foundation for America's $1.1 trillion technology industry affecting a US workforce of nearly 6 million people. Founded in 1977 by five microelectronics pioneers, SIA unites companies that account for 80 percent of the semiconductor production of this country. Through this coalition SIA seeks to strengthen US leadership of semiconductor design and manufacturing by working with Congress, the Administration and other key industry groups. The SIA works to encourage policies and regulations that fuel innovation, propel business and drive international competition in order to maintain a thriving semiconductor industry in the United States. More information on SIA is available at http://www.semiconductors.org.

IV. How Counterfeit Semiconductors Threaten Health, Safety, and Security

Due to the widespread use of semiconductors in a myriad of applications worldwide, counterfeit components pose major threats to the health, safety, and security of everyone that relies on electronics. While consumers do not usually buy semiconductor components directly, 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 can have catastrophic consequences. OEMs that sell electronic products and systems are reluctant to disclose incidents of counterfeit components causing failures since this can damage their reputations. However, known incidents of counterfeits causing or potentially causing health, safety, and security issues include:

1. A counterfeit semiconductor component was identified in an Automated External Defibrillator (AED), resulting in a defibrillator over-voltage condition. Failure to detect and address this issue could have resulted in improper electrical shocks being applied to heart attack victims, thus jeopardizing their lives.

2. A counterfeit semiconductor component caused a fire in the control circuitry in a vacuum cleaner for residential use. This fire was successfully contained, but it had the potential to result in major property damage or even loss of life.

3. A counterfeit semiconductor failed in a power supply used for airport landing lights. This did not result in any reported airline take-off or landing incidents, but the potential for such incidents was obvious.

4. A broker shipped counterfeit microcontrollers intended for use in braking systems in high-speed trains in Europe.

5. A broker shipped counterfeit microprocessors intended for use in automated medication applications, including intravenous (IV) drip machines.

6. A broker shipped counterfeit voltage regulators intended for use in automotive braking systems and automotive airbag deployment systems.

7. A broker shipped counterfeit semiconductors intended for use in radiation detectors that emergency responders would use in cases of a nuclear power accident.

8. A broker shipped counterfeit semiconductors intended for use in nuclear submarines.

The preceding examples represent just a fraction of the incidents where counterfeit semiconductor components jeopardize the health, safety, and security of the general public worldwide. While some counterfeited products, such as jewelry and apparel, do not endanger consumers, counterfeit semiconductors can be particularly dangerous depending on their end application. This is why it is so critical that semiconductor components be procured exclusively through authorized sources.

V. How Counterfeit Semiconductors Cause Economic Harm

In addition to jeopardizing health, safety, and security, counterfeit semiconductors cause significant harm to the economy. Semiconductor companies spend tens of billions of US dollars per year developing, manufacturing, and supporting products that will operate reliably for many years in customer applications. In contrast, counterfeiters spend minimal money developing and "manufacturing" products, and they provide no post-sales customer support. When an Original Component Manufacturers' products are counterfeited, the low quality and poor reliability of the counterfeit components can cause damage to an OCM's reputation, especially if the parties that experience failing components do not realize that these components are counterfeit. This damage to an OCM's reputation can result in loss of business even though the "manufacture" and sale of the counterfeits was completely outside the control of the OCM.

Due to their low-cost operations based on theft of OCMs' Intellectual Property (IP), counterfeiters can usually undercut the Average Selling Prices (ASPs) of OCMs and their Authorized Distributors. While component purchasers may think they are getting a good deal in terms of pricing and/or availability by turning to the open market and ordering components based on quick Internet searches, there are no assurances that these components are consistently authentic and reliable. Just one counterfeit semiconductor component in an electronic system can cause the entire system to completely fail unexpectedly during end-customer use. If this system is a video game console or an electronic toy, the economic consequences of failure are minimal. However, if this system is a computer server for financial transactions or a control system for electric power grids, the economic damage from failures can be very substantial.

Components bought through the open market carry no factory warranties, and most non-authorized sources are too small to be in a financial position to pay large liability claims stemming from high rates of OEM system failures caused by counterfeit components. Thus, component purchases from the open market that are initially viewed as inexpensive can turn into an extremely costly mistake, particularly if system failures result in millions of dollars in warranty expenses and/or liability claims against the OEM or their CM. Moreover, the cost of high failure rates on electronic systems due to counterfeit components can be even greater if these failures result in major damage to the OEM's/CM's reputation and the loss of future business. The economic harm can be almost incalculable if counterfeit semiconductors result in critical infrastructure failure or if counterfeits in safety-critical electronic equipment cause loss of life. The OEMs/CMs can avoid these major risks by always buying components directly from OCMs or directly from their Authorized Distributors/Resellers. By avoiding counterfeits and otherwise inferior products by adopting procurement policies requiring purchases through authorized sources, the OEMs/CMs will protect the health, safety, and security of everyone that depends on reliable electronic products and systems on a daily basis.

Individuals and companies involved in the sale of counterfeit components/electronic systems to the US Department of Defense (DoD) can face nearly unlimited financial liabilities along with severe criminal penalties. Section 818 of the National Defense Authorization Act for Fiscal Year 2012 (NDAA) requires defense contractors to establish effective policies and procedures to detect and avoid counterfeit components. [Reference 3.] Even if defense contractors have implemented comprehensive safeguards against counterfeits, they may be financially liable for all costs associated with completely remediating any issues stemming from counterfeit components in electronic systems. As detailed in Section IX, authentication determinations on suspect components are difficult to make and are often erroneous. Consequently, most counterfeit mitigation programs will not be effective unless they require that component purchases be exclusively through authorized sources. If counterfeit components are incorrectly deemed authentic and integrated into complex military systems deployed worldwide, the financial costs may be enormous to replace suspect or confirmed counterfeits. Thus, any savings that defense OEMs or their CMs may have realized by purchasing semiconductor components from the open market would be dwarfed by the costs of replacing previously-installed counterfeit components in fielded military systems. Moreover, the reputations of defense contractors and their suppliers involved in counterfeit issues can be badly damaged. NDAA Section 818 and subsequent related legislation cover additional provisions including reporting requirements for suspect counterfeit components and criminal penalties for trafficking in counterfeit goods and services. For example, per Section 818, an individual who intentionally traffics in counterfeit goods to the DoD can be fined up to $2 million and/or imprisoned for up to 10 years, double the penalties under previous laws. [Reference 3.]

VI. Prevalence of Counterfeit Semiconductors

As with most illegal activity, accurately determining the magnitude of semiconductor counterfeiting is not possible. However, the data that exists on semiconductor counterfeiting clearly shows that this is a major issue:

1. Over a three week period in November/December 2007, United States Customs and Border Protection (CBP) and European Union Customs seized over 360,000 counterfeit integrated circuits and computer network components bearing more than 40 different trademarks as part of "Operation Infrastructure," the first joint intellectual property rights enforcement operation undertaken by CBP and the European Union. [Reference 4.] Following this success, at SIA's request, CBP initiated Operation Infrastructure II and in May/June 2008 seized 420,000 counterfeit ICs and computer networking components bearing 50 different trademarks. [Reference 5.] Considering that these enforcement operations were for only a few months, did not cover all US ports, and likely did not capture 100% of the counterfeits entering the agency's targeted ports, the total counterfeit semiconductors imported that year was many multiples of the 780,000 seized components.

2. In April 2012, market research firm IHS iSuppli reported that "The five most prevalent types of semiconductors reported as counterfeits represent $169 billion in potential risk per year for the global electronics supply chain." [Reference 6.]

The US government has been particularly interested in quantifying the extent of counterfeits entering the military end-use segment of the market.

1. In January 2010, the Bureau of Industry Security (part of the US Department of Commerce) published a report that highlighted "an increasing number of counterfeit incidents being detected, rising from 3,868 incidents in 2005 to 9,356 incidents in 2008." This finding was based on a survey of 387 companies and organizations in the defense industrial base. [Reference 1.]

2. In November 2011, the Senate Armed Services Committee (SASC) issued a Background Memo detailing the investigation by SASC staff that "uncovered approximately 1,800 cases of suspect counterfeit electronic parts being identified by some companies in the defense supply chain, with the total number of suspect parts exceeding 1 million." [Reference 7.]

3. In November 2011, during an SASC hearing, SIA President Brian Toohey provided oral testimony that "Experts have estimated that as many as 15 percent of all spare and replacement semiconductors purchased by the Pentagon are counterfeit. Overall, we estimate that counterfeiting costs US-based semiconductor companies more than $7.5 billion per year, which translates into nearly 11,000 lost American jobs." [Reference 8.]

The military end-use segment is particularly prone to counterfeits because of the price gap between military and commercial components and because of a greater reliance on legacy products. However, the significant numbers of counterfeits documented in this segment that represents less than one percent of the worldwide semiconductor market is indicative of the very large number of counterfeits in the total market.

VII. Manufacturing of Legitimate vs. Counterfeit Semiconductors

Due to the critical importance of having electronic products and systems function as expected for many years, semiconductor companies spend billions of dollars per year to design and manufacture products to the highest quality and reliability levels. Semiconductor manufacturing consists of four high-level steps: wafer fabrication, package assembly, electrical test/burn-in, and final packing/boxing.

1. **Wafer fabrication occurs in some of the cleanest, most advanced, and most expensive factories (referred to as "fabs") in the world.** A new, advanced-technology wafer fab that can process 12" wafers patterned with nanometer-scale feature sizes costs several billion dollars. The wafer fabrication process transforms a "bare" wafer (a thin, round, high-purity slice of an ingot made from a semiconductor material such as silicon or gallium arsenide) into a fully-patterned wafer typically consisting of hundreds or thousands of small, identical circuits or "chips" separated by narrow lines called streets. The circuits consist of layers including diffusions/implants (where the conductivity of the semiconductor surface is increased), dielectrics (nonconductors), metallization and vias (horizontal and vertical conductors), and a final glass-like layer (a protective insulator). Each new layer is built upon the previous layer using a complex, repetitive process based on depositing (adding) and/or etching (removing) materials. A process called photolithography is used to pattern each layer, with the specific pattern defined by a photomask. A set of photomasks for a single IC product with minimum feature sizes measured in nanometers (billionths of a meter) can cost over one million dollars. In addition to the photomasks, what makes wafer fabrication so expensive is that the wafer processing must be conducted in ultra-clean rooms with highly-advanced equipment that constantly maintains extreme controls over wafer curvature, alignment, temperature, etc. Since minimum feature sizes for transistor gate oxide layers on advanced processes can be on the order of just 1 nanometer (about 1/70,000th the width of a hair!), airborne particles and other contaminants must be eliminated to prevent defects that could cause an IC to function incorrectly or be unreliable. This is accomplished through many costly measures, including using highly advanced air cleaning systems; manufacturing with ultra-pure chemicals, gases, and deionized water; and having fab personnel wear "bunny suits" (cleanroom suits). This is one of the reasons that a wafer fabrication facility is so expensive to build and operate.

2. **The package assembly process transforms wafers into individual ICs housed in packages with electrical terminals typically consisting of metal pins or metal solder balls.** The packages have a wide range of sizes and materials. Historically, most packages have been assembled by first sawing the wafer along the streets between each chip on the wafer, with each chip (also known as a die) then mounted on a metal leadframe or a laminate (essentially a small printed circuit board). After this die attach process, thin gold, aluminum, or copper wires (typically 25 microns or less in diameter) are bonded between metal bond pads on the die and metal fingers or pads on the leadframe or laminate. The final major assembly step is to encapsulate the wire-bonded die, typically using mold compound (plastic). Many other semiconductor packages are used by the industry, including ceramic and metal packages where the packages provide hermetic seals

between the semiconductor die and the outside world. Traditional plastic, ceramic, or metal packages are increasingly being replaced by what are commonly referred to as wafer-level packages or bumped die where the die has solder bumps (solder balls) attached directly on its bond pads. In this case, the x- and y-dimensions of the "package" are the same as the die after it is sawn from the wafer, thus resulting in a very small package (sometimes less than 1 square millimeter in area). While package assembly needs to be conducted in clean environments, packages generally are not assembled in the most advanced cleanrooms since package feature sizes are significantly larger than die circuitry feature sizes. Thus, due to reduced capital equipment and cleanroom requirements relative to wafer fabs, package assembly facilities are significantly less expensive to build and operate than wafer fabs.

3. **The next major manufacturing process for semiconductors is final electrical test and, in some cases, burn-in.** Components are electrically tested on Automatic Test Equipment (ATE) using sophisticated test programs with hundreds or thousands of lines of code that can take many months for Product Test Engineers at OCMs to develop. The ATE systems, which can cost hundreds of thousands of dollars to several million dollars each, are connected to ATE handlers which feed components into the test sites on the ATE systems. Most commercial-grade components are ATE tested at room temperature (e.g., +25 °C = +77 °F) or elevated temperature (e.g., +70 °C = +158 °F). Automotive-grade and military-grade components are often also tested at extremely cold (e.g., -55 °C = -67 °F) and extremely hot temperatures (e.g., +125 °C = +257 °F) to guarantee they will operate correctly over very wide temperature ranges. ATE testing at cold temperatures is particularly challenging given the components tend to "frost up" unless expensive, specialty ATE handlers are used. Products used in high-reliability applications are sometimes subjected to burn-in whereby components are electrically operated in high-temperature ovens for extended periods of time to screen out any latent defects. Based on the ATE results and, if applicable, the burn-in results, each component is "binned out" as passing or failing. All failing components are physically destroyed; this often is accomplished by incinerating components and recovering the metals (gold, silver, copper, etc.) used in packages. Passing components are sometimes further segregated into different performance grades based on the specific ATE results. The tops of the packages for passing ICs are typically laser-marked with the OCM's logo, part number (including any performance grade), and production codes. The specific markings vary somewhat between OCMs, and physical package sizes sometimes constrain the amount of information that can be marked on components.

4. **The last high-level manufacturing process is packing/boxing of components prior to shipping finished goods to OCMs' Authorized Distributors/Resellers as well as to some customers that buy components directly from OCMs.** Automated equipment is used to take components that pass ATE testing and insert or place them in carrier media including canisters, tubes, trays, and reels. Products that are sensitive to moisture are baked (e.g., at +125 °C = 257 °F for 12 hours) to remove any moisture from the packages. The carrier medium containing the baked components is then inserted into a static-protected moisture barrier bag along with desiccant and a humidity indicator card. The moisture barrier bag, which has a label that includes the

Moisture Sensitivity Level (MSL) of the components, is then properly evacuated and sealed. Sealed moisture barrier bags are then placed in static-protected boxes along with static-protected dunnage (such as specialty crumpled paper), and the boxes are sealed and labeled. As with all prior manufacturing steps, OCMs and their subcontractors have advanced controls throughout the packing and boxing operations to ensure that components are properly handled and stored and are never subjected to electrostatic discharge (ESD) events that could result in damage.

The contrast between manufacturing of legitimate semiconductors and counterfeit semiconductors could not be more extreme. In the case of counterfeits, components are often "harvested" from electronics waste (e-waste) using crude processes, and then re-marked to indicate they are new or are otherwise different from how they were originally marked. The typical "manufacturing" process for counterfeit components [Reference 9] is as follows:

1. Using "mountains" of scrap electronics as an input, workers remove printed circuit boards (PCBs) from old electronic systems.

2. PCBs are heated over an open flame to melt the solder used to secure components to the boards. The boards are then banged against a hard surface so that the components will fall out into buckets. The components are then sorted, typically based on the package sizes and styles, and the electrical functions of the components.

3. The original markings on the components are removed using methods of increasing sophistication ranging from sanding to chemical etching to "black-topping" to "micro-blasting."

4. New markings, including trademarked OCM logos, are added to the components. These new markings generally are intended to make the parts more marketable and/or more expensive. For example, parts with old product codes may be marked with new product codes; packages that contain the element lead (Pb) may be marked to indicate they are lead-free (Pb-free); parts that have low performance may be marked to indicate they have high performance; and inexpensive commercial-grade parts may be marked to indicate they are more expensive automotive-grade or military-grade parts.

5. The external pins, pads, or solder balls on the packages are reworked to make them appear new. This sometimes entails using harsh chemicals to clean these external package connections.

In addition to this particular form of "manufacturing" of counterfeit components, counterfeiters have developed numerous other ways to try to deceive component purchasers. In some cases, the counterfeiters simply have packages assembled with no die in them, the wrong die in them, or no bond wires. Such components are completely useless, but the purchaser may not be able to get his or her money back if the seller is a fly-by-night operation. More sophisticated counterfeiters sometimes take used or new low-grade components and have them re-marked as high-grade components with the same functionality. These components may operate as expected under nominal conditions, but then fail when used at elevated temperature, increased clock frequency, decreased supply voltage, etc. Finally,

counterfeiters may remove die from the original packages and have them re-assembled in new packages. In some cases, this involves removing die from old plastic packages and assembling them in new hermetic packages, since products in hermetic packages usually sell at a significant premium over the same products in plastic packages. Detecting re-packaged die is particularly challenging since the packages are new and the packages are not re-marked or otherwise physically altered.

While many of the "manufacturing" processes used by counterfeiters are manual and primitive relative to the advanced, automated processes used by OCMs, the workmanship on these counterfeits is often excellent. Counterfeiters realize that customers will be checking the physical appearance of packages including the markings on the packages, and counterfeiters usually now go to great lengths to make their illicit components look indistinguishable from legitimate components. Thus, unlike years ago, package visual inspection with a microscope and other straightforward analytical techniques are usually ineffective at detecting counterfeit components.

VIII. Quality/Reliability of Legitimate vs. Counterfeit Semiconductors

By adhering to rigorous Quality Management Systems and by conducting manufacturing operations in highly advanced factories as described in Section VII, failures of legitimate products are extremely rare. Quality Management Systems ensure that components are not subjected to any conditions which could reduce the quality and reliability levels of components. For example, OCMs and their Authorized Distributors and Authorized Resellers ensure that:

1. Components are continuously protected against electrostatic discharge (ESD) and electrical overstress (EOS) events during manufacturing and handling.

2. Components that are sensitive to moisture are properly baked and dry-packed.

3. Components are properly stored to avoid exposure to contamination as well as to temperatures, humidity levels, shock levels, and other environmental stresses beyond the rated limits of the components.

The net result of the highly advanced design and manufacturing controls used by OCMs as well as the proper handling and storage of components by OCMs and their Authorized Distributors/Resellers is that failures of legitimate semiconductor components are very unusual. Industry data has shown that <0.01% of legitimate semiconductor products will ever fail during operation in electronics systems.

Counterfeit semiconductors have far higher failure rates than legitimate semiconductors. While some counterfeit semiconductors will fail immediately when electrically tested or first used, other counterfeit semiconductors pose a much larger threat in terms of their susceptibility to failure after days, months, or years of operation. This is because counterfeiting operations often introduce latent defects that can remain undetected during testing of electronic systems. These subtle defects can later result in either sudden failures during system use, or, more insidiously, can cause erratic performance and produce

unexpected results, which may be undetectable until the counterfeit component completely fails. The causes of these reliability failures are numerous and include the following:

1. **Package cracking, package delamination, and/or die cracking may be induced by component removal from scrap Printed Circuit Boards (PCBs).** Counterfeiters rarely take any precautions against package damage during board removal. Flexing of PCBs and removal of components from boards can cause subtle cracking, either on the outside or inside of the package, that is not visible with component inspection. A common form of damage caused by board removal is stress fracturing at the metal pins or metal solder balls on the outside of the package. Components having pins or solder balls with subtle stress fracturing may pass electrical testing after they are re-mounted on new PCBs. However, during customer application, particularly in harsh environments, the stress fracturing can progress to the point that the component fails intermittently or continuously. Components removed from PCBs and re-marked to indicate they are new may fail at the worst possible time. For example, if the flight control system for a jet plane has a counterfeit component with a micron-scale crack in the silicon chip, the mechanical stress on the chip from flight turbulence could cause the crack to propagate, resulting in complete electrical failure of the component. The resulting failure of the flight control system could result in loss of control of the plane, jeopardizing the lives of everyone onboard.

2. **"Popcorning" of counterfeit components may occur during PCB assembly since counterfeiters rarely handle or store components properly.** Many components, including components with mold compound (plastic) encapsulant, will absorb significant moisture. While OCMs always properly bake and dry-pack moisture-sensitive components, counterfeiters usually skip one or both of these manufacturing operations or take shortcuts to save time and cost. Even if counterfeit components are dry-packed in sealed moisture barrier bags, they may not have been properly baked first. The net result is that during component mounting on PCBs using high-temperature reflow ovens, the moisture in the counterfeit components expands very rapidly (since steam forms above 100 °C = 212 °F), causing the package to "popcorn," which can result in cracking or delamination inside the package. As in the previous case, this internal cracking or delamination can become worse during end-customer use, resulting in total electrical failure of the component.

3. **Counterfeit components are often marked to indicate they do not contain the element lead (Pb) or other restricted materials when they in fact do, and this can result in major component reliability risks.** Components "harvested" from old scrap PCBs are often years or even decades old, and most of these components contain Pb and/or other materials covered by the Restriction of Hazardous Substances Directive (RoHS). Often, the Pb was incorporated in the solder used in component packages to reduce the melting point of the solder. For example, tin-lead (SnPb) solder was very common until RoHS and other environmental legislation went into effect over the past decade. Since component packages with SnPb solder were generally mounted on PCBs using relatively low peak solder reflow temperatures (typically between 220 °C = 428 °F and 235 °C = 455 °F), the materials in the package did not need to be reliable to

particularly high temperatures. However, with the industry transition to Pb-free packages over the past decade, component packages are now usually mounted on PCBs using significantly higher peak reflow temperatures (typically between 240 °C = 464 °F and 260 °C = 500 °F). Semiconductor companies therefore re-engineered component package materials (such as mold compound and die attach) so that they would be reliable at these higher temperatures. Since most of the electronics industry has transitioned to Pb-free packages to meet RoHS requirements, the demand for Pb-bearing packages has dropped precipitously. Thus, counterfeiters usually re-mark old components to indicate they are Pb-free (when they are not). In addition to the use of such counterfeit components causing RoHS compliance issues, PCB manufacturers that assume these components are Pb-free and mount them on PCBs at temperatures of up to 260 °C = 500 °F can unknowingly induce major reliability hazards since the package materials were not designed to handle these high temperatures. For example, counterfeit Pb-bearing packages that are mounted at such high temperatures may "popcorn," resulting in cracking or delamination of the package. As previously detailed, internal package cracking or delamination can worsen during component field use, resulting in a sudden catastrophic failure. In addition to die cracks propagating in the field, delamination can spread to the point that internal bond wires snap, again causing the component to completely stop functioning. While marking Pb-bearing packages as Pb-free is very common, counterfeiters sometimes do the inverse and mark Pb-free packages as Pb-bearing to meet remaining demand for legacy Pb-bearing packages. Due to the lack of controls in "manufacturing" and handling these counterfeits, this results in a different set of reliability risks, such as the potential for tin whisker formation that can result in shorting between electrical terminals on components.

4. **Electrostatic discharge (ESD) damage may occur to semiconductors during component removal from scrap PCBs or during subsequent operations such as stripping of original package markings, adding new counterfeit markings, etc.** All these "manufacturing" operations for counterfeit components can cause them to become electrically charged, especially since counterfeiters almost never take any precautions against ESD (such as using ESD ground straps and using ionizers to safely discharge components). When the charged components subsequently contact metal surfaces such as a metal storage bins, they will discharge via high-current transients that can slightly damage thin dielectric layers in the component circuitry, such as nanometer-scale gate and capacitor dielectrics. These dielectric layers, which are meant to be insulators, then conduct leakage currents. These leakage currents may be too low to result in electrical failures during initial use. However, after weeks or months of operation, the leakage currents can increase to the point that components suddenly fail catastrophically.

5. **Chemicals used by counterfeiters to strip original markings and/or to clean component package connections can result in reliability failures due to corrosion.** In their effort to make old or used components look new, counterfeiters often use harsh chemicals to "recondition" packages. These chemicals are sometimes incompatible with the package materials, and thus the integrity of the packages will be compromised by these chemicals. Even if the chemicals are compatible with the packages, they may not be fully rinsed off by the counterfeiters. For

example, acid used by counterfeiters to clean oxide layers and other contaminants from package pins, pads, and solder balls will initially penetrate only the surfaces of packages. However, weeks, months, or years later, the acid can work its way to active circuitry on the semiconductor chip, thus corroding away this circuitry and resulting in loss of functionality. This corrosion mechanism is accelerated by temperature and humidity; the time-to-failure of the counterfeit components will decrease as the temperature and/or humidity they are exposed to increases. Even if the PCB manufacturer washes circuit boards and/or applies conformal coatings to circuit boards, any acid that had partially penetrated packages during counterfeiting will be trapped in the packages and can eventually lead to catastrophic failure.

6. **Finally, counterfeiters can introduce reliability issues by incorrect laser marking of component packages.** As the semiconductor industry has largely transitioned from ink-marked components to laser-marked components, counterfeiters have followed suit. Conducting laser marking on components in plastic packages has become increasingly challenging as these packages have become thinner. More specifically, the laser marking needs to be sufficiently deep into the package to make it legible without reaching bond wires or other critical internal package features. Due to their expertise at developing, characterizing, qualifying, and monitoring laser marking processes, semiconductor companies do not compromise package integrity during laser marking operations. However, counterfeiters usually do not know the depth of bond wires and other critical features on a given component. This is especially the case if counterfeiters have chemically or mechanically removed the original package markings and have thus reduced the thickness of the package. When bond wires or other interconnects inside packages are hit by lasers used by counterfeiters, the current-carrying capability of these interconnects is reduced. This can result in time-dependent failures when the damaged interconnect eventually fuses open during component use. Hermetic packages may likewise have poor reliability due to laser marking by counterfeiters. For example, in the case of iron-based lids that are plated with nickel and/or gold, if laser marking removes the plating, subsequent exposure of the package to moisture will cause the iron to corrode. Prolonged exposure to moisture will cause the iron to corrode away to the point that holes develop in the package lid, resulting in loss of package hermeticity and likely catastrophic failure due to moisture entering the package.

The net result of the above issues is that counterfeit components that pass electrical testing after board mounting may still have significant field reliability problems. If even one counterfeit semiconductor component ends up in an electronic system with hundreds or thousands of components, the reliability of the entire system may be greatly compromised by this one bogus component. Classic system-level Mean Time Between Failure (MTBF) reliability calculations, such as those detailed in MIL-HDBK-217, are completely meaningless if one or more components in the system are counterfeit. [Reference 10.]

IX. Authenticity Determinations

As counterfeiters have refined their "manufacturing" processes, making authenticity determinations has become increasingly difficult for everyone except the Original Component Manufacturer (OCM). Years ago, many counterfeit semiconductors had irregular solder on external package pins, poorly-marked logos, sloppy alphanumeric characters, and/or evidence of package surface sanding or "blacktopping." These and other telltale signs of counterfeiting made it easy for anyone with a good, low-power microscope and some general training to identify the more blatant counterfeits. Some of these older, relatively crude counterfeits are still available through non-authorized purchase sources. More recently, however, counterfeiters have become far more sophisticated. For example, semiconductor package surfaces and external pins/solder balls as well as package markings (including logos) may be essentially identical to those on legitimate products. In addition, tubes, trays, reels, dry-pack bags, desiccants, humidity indicator cards, shipping boxes, shipping labels, certificates of conformance, and other packing materials and documents may be counterfeit or forged and may be indistinguishable from those used for legitimate shipments. Moreover, while very low retail prices were historically an indicator that components were likely bogus, counterfeits now often cost nearly as much as legitimate components, thus boosting the profits for counterfeiters and their supply chains while making retail prices a poor indicator of product authenticity.

Many third-party laboratories and some Original Equipment Manufacturers (OEMs) and/or Contract Manufacturers (CMs) claim they can make authenticity determinations with a high degree of accuracy, but this often is not the case. Various standards, including SAE AS5553 and IDEA-STD-1010, provide detailed guidelines on identifying counterfeit components. [References 11-12.] These standards are sometimes helpful in identifying counterfeits where component packages have obviously been "refurbished" and/or components have been re-marked. However, SIA member companies have numerous examples where third-party laboratories reportedly using these standards have made incorrect authenticity determinations. Moreover, these standards are generally ineffective for identifying the latest forms of counterfeiting. For example, counterfeits where used, low-grade, or second-source die are assembled in new packages and are marked as higher-grade components would likely escape detection. In addition, some of the test techniques used for counterfeit detection that are considered non-destructive can cause subtle damage to components. For example, x-ray inspection can result in shifts in key electrical parameters for components, particularly in the case of high-performance products. Third-party laboratories and OEMs/CMs routinely conclude that components are legitimate based on their own electrical testing, which usually consists of curve tracer testing that measures the current vs. voltage characteristics of component pins. However, while curve tracer testing can identify the most obvious counterfeits, this and other simple bench-top electrical testing cannot begin to replicate OCMs' thorough electrical testing of ICs using expensive Automatic Test Equipment (ATE) running up to thousands of lines of test code as detailed in Section VII. Curve tracing only checks a few transistors connected directly to each IC pin, while ATE testing by OCMs with proprietary test programs assesses the full functionality of even the most complex ICs that can each have millions of transistors. Thus, unless ICs have been tested on OCMs' ATE that is designed to ensure only high quality and

reliability products are shipped, conclusions about product authenticity should never be based on ICs "passing" electrical testing.

A common problem with authenticity testing is working on the false assumption that testing samples pulled from a population of suspect parts will allow conclusions to be drawn about all the parts. Due to the time and expense of conducting laboratory tests to try to identify counterfeits along with the destructive nature of some tests (e.g., package decapsulation followed by die visual inspection), usually only a small fraction of the parts in a shipment of suspect components is tested. However, counterfeiters are familiar with sampling protocols, and thus they often "seed" legitimate units at the beginning and end of tubes and reels so that if these easily-sampled parts are tested they will pass. Even in cases where good parts are not "seeded" in an otherwise counterfeit reel, tray, or tube of parts, any assumption that a population of parts is homogenous is almost always incorrect in the case of counterfeits. More specifically, due to the variability in the processes used during the "manufacturing" of counterfeits, only some of the parts may be damaged by mechanisms such as ESD, corrosion, die or package cracking, etc. The bottom line on authenticity determinations made by anyone other than the OCM is that they are time-consuming, expensive, and often inaccurate. Moreover, even if testing correctly identifies that components are authentic, there is no way to prove that components outside the authorized supply chain have not been mishandled or improperly stored, thus jeopardizing their quality and reliability.

Although counterfeiters have become very sophisticated, OCMs can readily make authenticity determinations on suspect products marked with their logos. OCMs incorporate overt and covert features into semiconductor packages as well as packing materials. In many cases, technical experts at OCMs can quickly make authenticity determinations when provided with high-resolution photos of the top-side and bottom-side of semiconductor packages as well as associated shipping labels and packing materials. OCMs' methodologies for making authenticity determinations are only valuable when they are kept secret, so OCMs do not divulge any details on covert features and authenticity methodologies. In cases where authenticity determinations cannot be made from photos, OCMs can consistently make accurate determinations when provided with physical samples of suspect components marked with their logos.

While OCMs are proficient at making authenticity determinations on "their" components, most OCMs limit their authenticity determination services to suspect products detained by Customs and to suspect products that are the subject of law enforcement investigations. OCMs generally do not provide authenticity determinations as a free service for non-government agencies. This is because many billions of suspect components are available on the open market, and OCMs would need to staff large departments to try to respond to tens of thousands of authenticity requests from independent distributors and brokers as well as individuals or companies buying from these non-authorized sources. OCMs provide extensive post-sales support to customers that buy their products from authorized sources, but, as with other industries, there is no viable business model for OCMs to provide free support on suspect products that may not have been manufactured by the OCM. Again, as with other industries, OCMs support products they sell through authorized channels; OCMs are not in the business of supporting counterfeits and other suspect products available on the open market.

X. Authenticity Does Not Guarantee Performance and Reliability

A major misconception is that if an authenticity determination is made (by whatever means) and the associated semiconductor components are deemed legitimate, then they will have high quality and reliability levels. In many cases, nothing could be farther from the truth. Any components outside the authorized supply chain (whether authentic or not) may not have been handled, stored, and transported properly. Even if a customer buys components from a broker or an independent distributor that has always handled and stored components correctly, the broker/independent distributor may have obtained the components from an "upstream" source that did not do so. Unfortunately, unlike with some other products, semiconductor components can be mishandled or stored improperly yet show little or no physical evidence that they have been abused. Examples of damage that can occur due to improper handling and storage when components are outside the authorized supply chain include:

1. Electrostatic Discharge (ESD) damage due to handling without adequate ESD controls;
2. Bent pins, scratched pads, and deformed solder balls due to rough handling;
3. Solderability issues caused by exposure to excessive temperature and/or humidity;
4. Package contamination due to handling and storage in a dirty environment;
5. Package "popcorning" caused by incorrect or missing dry-packing.

Unfortunately, as detailed in Section VIII, some of the above issues do not always result in immediate component failure. Both ESD damage and package contamination can result in time-dependent failures. Since the quality and reliability of components can be severely degraded by improper handling and storage, semiconductor companies do not offer warranties on components that are outside the authorized supply chain. Thus, if components bought on the open market have high fail rates in electronic systems, semiconductor companies have no liability. Although the component purchaser may try to pass warranty costs and other large financial liabilities on to the company they bought the parts from, most open market sources are not in a financial position to pay out large liability claims. For example, fly-by-night operators often "disappear" when faced with liability claims or lawsuits. The net result is that the Original Equipment Manufacturers (OEMs) and/or their Contract Manufacturers (CMs) are saddled with high financial liabilities and in many cases damaged reputations due to selling systems with poor reliability. The OEMs/CMs can avoid all these problems by buying components directly from OCMs or directly from their Authorized Distributors/Resellers.

XI. How Authorized Supply Chains Prevent Counterfeit Infiltration

The authorized supply chain for semiconductor components is very clear and ensures that this supply chain is not contaminated by counterfeits. Original Component Manufacturers (OCMs) sell their products in two ways:

1. Directly through their sales force and through their Internet sites;
2. Directly through Authorized Distributors, and, in some cases, Authorized Resellers.

Each OCM identifies and qualifies their Authorized Distributors using a broad set of criteria including long-term business viability, quality systems, order placement and fulfillment processes, customer support, and customer returns policies. While the details of the processes for selecting Authorized Distributors vary somewhat between semiconductor companies, the contracts between OCMs and their Authorized Distributors always require them to obtain components solely from OCMs. Contracts specify that Authorized Distributor relationships can be terminated if distributors ever allow product not sold by them to be "returned." OCMs periodically audit their Authorized Distributors to ensure products are always handled and stored properly to prevent ESD and other damage. These audits also include validating that the distributors' policies and procedures cannot allow counterfeit or otherwise questionable components into the supply chain. The net result is that, just as with component purchases directly from OCMs, customers buying from Authorized Distributors are assured of receiving legitimate products with high quality and reliability levels. Components bought from Authorized Distributors carry the same factory warranties as those bought directly from OCMs.

Semiconductor companies have made it easy for customers to identify their Authorized Distributors. OCMs list their Authorized Distributors and any Authorized Resellers on their Internet sites. If a link to authorized sources is not available on a given OCM's home page, just search on "distributors" to find them. The SIA ACTF has partnered with SIA member Rochester Electronics to create, develop and maintain the Electronics Authorized Directory at the following URL: http://www.authorizeddirectory.com/. [Reference 13.] This web-based search tool provides distributor information that is maintained, checked, and updated on a regular basis from the OCMs' websites. No user registration or password is required to access this website, and the user can readily search by OCM and by location to find Authorized Distributors worldwide. When choosing Authorized Distributors, keep in mind that a given distributor may carry a very broad line of components and may only be an Authorized Distributor for a subset of those components. Thus, if a distributor makes a general statement that they are authorized, be sure to check that they are authorized by the specific OCM of interest to sell that OCM's components.

XII. How Counterfeits Can Enter Non-Authorized Supply Chains

OCMs and their Authorized Distributors have proven systems for ensuring that components bought from them are legitimate and are handled, stored, and transported properly. However, once components are out of the authorized channel there are no assurances that the component is legitimate or functional. Components on the open market often pass through many different hands. For example, during his opening statement at the Senate Armed Services Committee (SASC) Hearing on Counterfeit Electronic Parts in the Department of Defense's Supply Chain, SASC Chairman Senator Carl Levin described how one set of suspect counterfeit parts went through six different brokers/independent distributors in three different countries before they were assembled into an electronic system. [Reference 14.] Given the number of parties involved and the associated extensive shipping and handling operations, there are numerous opportunities for counterfeit components to enter non-authorized supply chains. In many cases, the majority of parties in the supply chain are unaware that they are dealing with counterfeits. It is not surprising these parties usually plead ignorance if an investigation takes place and civil or criminal charges are filed. However, any individual or company that is knowingly or unknowingly involved in the distribution of counterfeit components can be charged with trafficking in counterfeit goods.

While many brokers/independent distributors are diligent about avoiding counterfeits, some open market sources intentionally engage in the distribution and sale of counterfeit components. For example, the SIA Anti-Counterfeiting Task Force worked with US government agencies to analyze suspect components, many of which were determined to be counterfeit, sold by brokers MVP Micro, J.J. Electronics, VisionTech Components, Epic International Electronics, and their affiliated companies. [References 15-18.] The defendants in the MVP Micro case manufactured counterfeit semiconductors in the US, thus illustrating that the manufacturing of counterfeit components is not just limited to countries with a history of providing minimal Intellectual Property (IP) protection. In the J.J. Electronics, MVP Micro, and VisionTech Components cases, the defendants knowingly sold counterfeit electronic components to the US military and other customers via their professional-looking websites. The defendants in these cases later served time in prison for trafficking in counterfeit components and other unlawful activities. The defendant in the Epic International Electronics case was charged in July 2013 with importing counterfeit semiconductors for sale in the US. Some of these counterfeits were intended for use in nuclear submarines, thus underscoring the major risks that counterfeit semiconductors pose to health, safety, and security.

Although the majority of brokers and independent distributors in the US do not knowingly sell counterfeit components, SIA member companies, working in conjunction with US Customs and Border Protection (CBP) as well as OEMs and CMs, have identified hundreds of brokers and independent distributors that have attempted to import and/or have imported or otherwise obtained counterfeit components. This SIA and CBP data is consistent with Government-Industry Data Exchange Program (GIDEP) alerts detailing incidents where hundreds of open market suppliers worldwide have sold suspect or confirmed counterfeit components to GIDEP member companies. [Reference 19.] Thus, unfortunately, the sale of counterfeit components is not just limited to a few rogue brokers and independent distributors; counterfeits have infiltrated much of the open market and are commonly seen on web-based purchases where the buyers' primary purchasing criterion is lowest price. As a final example illustrating this point, the Government Accountability Office (GAO) published a report that concluded that "Suspect counterfeit and bogus—part numbers that are not associated with any authentic parts—military-grade electronic parts can be found on Internet purchasing platforms, as none of the 16 parts vendors provided to GAO were legitimate." [Reference 20.]

XIII. How to Avoid Counterfeit Legacy Products

Due to industry changes and customer demand for the latest and most advanced technologies, OCMs routinely discontinue the manufacture of products. Consistent with JEDEC JESD48C [Reference 21], semiconductor companies generally provide 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. For example, the Restriction of Hazardous Substances (RoHS) Directive and other environmental legislation have driven the demand for many non-military components in Pb-bearing packages to zero. As customers have transitioned their PCB manufacturing operations to Pb-free processes, they have no need for legacy Pb-bearing packages. Thus, OCMs have issued many PDNs on

Pb-bearing packages, but in most cases the same products are available in Pb-free packages, and for most customers these PDNs are just a formality. In other cases, PDNs are issued when old wafer fabrication processes will be shut down. Often, these same products or very similar products will be available on newer wafer fabrication processes, though the specifications for the recommended replacement parts may vary from the parts being discontinued. In such cases, whenever possible, component customers should transition their future orders to the recommended replacement products. The transition should be scheduled to be completed by the time the customer runs out of the legacy product bought during the last-time shipment period. Customers that use a large number of different components should consider having SIA member companies and/or OCM-Authorized Distributors that specialize in product life cycle management handle some or all their business processes for ensuring continuous availability of components.

Several options are available to customers requiring legacy products where the customer cannot use recommended replacement parts for any reason, including potentially high costs for qualifying a new product. These options will ensure that customers are receiving authentic products with high quality and reliability levels as well as full warranty coverage and post-sales support.

1. **The first option is to buy legacy components from OCMs' Authorized Aftermarket Distributors/Manufacturers that obtain legacy products exclusively from OCMs in wafer, die, or final packaged form.** [Reference 13.] For many legacy products, decades of supply are available for immediate delivery from Authorized Aftermarket Distributors that have literally billions of packaged components in stock. In cases where the product needs to be packaged but is only currently available in die or wafer form, Authorized Aftermarket Distributors/Manufacturers for legacy products can have the product assembled as per the customer's needs using either subcontracted or internal package assembly processes. As with products assembled by the OCM and marked with the OCM's logo, products assembled by the Authorized Aftermarket Distributor/Manufacturer and marked with the Aftermarket Distributor/Manufacturer's logo have full warranty coverage and post-sales support.

2. **Additionally most Authorized Aftermarket Distributors/Manufacturers are authorized by OCMs to manufacture discontinued products.** Several SIA member companies have extensive portfolios of products that OCMs have authorized them to produce using the same wafer fabrication process flows and tooling as well as the same packages as the original products. These aftermarket products have comparable or better performance, quality, and reliability as the original products, and they carry full warranties from the Authorized Aftermarket Distributors/Manufacturers. In cases where they do not already have the capability to manufacture legacy products of interest, Authorized Aftermarket Distributors/Manufacturers usually can re-engineer these products after obtaining authorization from the OCMs. Due to the time and cost of doing so, this option is generally only used when no Authorized Distributors have the ability to meet customer demand requirements (shipment quantities with specified delivery dates) for the products of interest.

XIV. ACTF Strategies and Initiatives to Combat Counterfeits

Since its formation in 2006, the Semiconductor Industry Association (SIA) Anti-Counterfeiting Task Force (ACTF) has been actively battling against counterfeit semiconductors. Through the ACTF, major

semiconductor companies in the US have jointly developed and advanced ongoing initiatives and strategies to reduce the supply and demand for counterfeit semiconductor products. Major accomplishments include:

1. **The ACTF has driven counterfeit component awareness and actions.** SIA members provide leadership and give presentations at conferences, technical symposia, and webinars, including Counterfeit Electronic Parts and Electronic Supply Chain Symposia, and Diminishing Manufacturing Sources and Material Shortages (DMSMS) Conferences. [References 22-23.] These presentations focus on the quality and reliability risks posed by counterfeit semiconductors, along with the critical importance of always buying components directly from OCMs or their Authorized Distributors and Authorized Resellers to avoid problems with counterfeit components. SIA President Brian Toohey has testified before both the Senate Armed Services Committee and the House Homeland Security Committee on how counterfeit semiconductors jeopardize the safety and effectiveness of US military personnel and operations. [Reference 8.] SIA members also regularly meet with House, Senate, Department of Commerce, Department of Defense, Administration, and other government officials to brief them on how counterfeit semiconductors are a danger to the health and safety of the public, and to work with them on solutions to this insidious problem. Through written responses to Requests for Information and to Notices of Proposed Rulemaking, the ACTF provides government agencies with specific recommendations on how to avoid counterfeit semiconductor products. The ACTF has also been instrumental in driving anti-counterfeiting legislation, regulations, and policies, including legislation that increases government-industry sharing on suspected counterfeit semiconductors, and that increases penalties for selling counterfeit components to the military.

2. **The ACTF works closely with Customs to keep counterfeit components from crossing borders.** Since 2006, the ACTF has partnered with US Customs and Border Protection (CBP) in the battle against counterfeit components, and the ACTF has a very effective working relationship with the CBP Center of Excellence and Expertise – Electronics that was formed in October 2011. [Reference 25.] ACTF member companies conduct CBP Port Officer training on an ongoing basis; this training allows CBP to identify suspect counterfeit components based on specific telltale signs. In cases where they cannot readily make authenticity determinations on their own, Port Officers have contacts at SIA companies. When provided with photographs and/or other details on suspect shipments, SIA companies rapidly determine whether the shipments are legitimate or are most likely counterfeit. Shipments of legitimate semiconductors are released by CBP, while shipments of counterfeit semiconductors are seized and later destroyed. CBP has published Intellectual Property Rights (IPR) seizure statistics showing that the total Manufacturer's Suggested Retail Price (MSRP) for counterfeit consumer electronics/parts that were seized in Fiscal Year 2012 was approximately $101 million. [Reference 26.] Although this only represents a small fraction of the counterfeit electronics entering the US, these seizures are reducing the supply of counterfeit semiconductors and are serving as a deterrent to open market suppliers that are knowingly or unknowingly attempting to import counterfeits into the US. While the ACTF's focus has been primarily with Customs in the US, SIA member companies have also conducted training for Customs officials in other countries, including China, France, India, and Italy. As in the US, SIA companies provide Customs officials worldwide with rapid responses to component authenticity requests.

3. **The ACTF also partners with law enforcement to help prosecute those involved in the manufacturing and/or trafficking of counterfeit semiconductor components.** SIA companies conduct in-depth laboratory analyses on suspect components from undercover buys made by government agencies. Using CBP seizure data as well as OCM laboratory reports on confirmed

counterfeit components, law enforcement agencies obtain search warrants and conduct enforcement actions (raids) resulting in the arrest of suspects dealing in counterfeit components. SIA companies provide on-site support to law enforcement immediately after enforcement actions occur. This support includes identifying the manufacturing processes used by counterfeiters and determining which seized components are counterfeit. Subsequent support includes testifying in court cases and providing Victims Statements to sentencing judges. Recent cases that the ACTF assisted government agencies in investigating and prosecuting, including MVP Micro in Irvine, California, and VisionTech Components in Clearwater, Florida, have resulted in defendants being ordered to pay restitution and being sentenced to several years of incarceration. [References 16-17.] The Epic International Electronics case is in the prosecution phase, but the defendant is facing up to 20 years in prison if convicted. [Reference 18.] These and other high-visibility cases, which have received significant media coverage, serve as a major deterrent to those manufacturing and/or selling counterfeits or those contemplating doing so.

4. **The ACTF is active in evaluating component security features and in developing international standards relating to supply chain assurance and anti-counterfeiting.** SIA member companies use a wide range of security features, both overt and covert, and they work both independently and with third-parties to continue to advance these features to stay ahead of counterfeiters. Semiconductor companies do not plan to adopt a single, industry-wide security feature since counterfeiters would then only need to figure out this one feature, and if they did so, they could readily counterfeit components from any semiconductor company. Rather, OCMs use security features that change over time and are tailored to the specific components being manufactured. This approach has proven to be the most effective at deterring counterfeiters. These security features only have value when they are dynamic and are kept secret. Therefore, semiconductor companies do not disclose security features to customers, governments, or any other entities.

5. **While the semiconductor industry is opposed to any mandates for a single authentication technology, SIA member companies are actively involved in the development and deployment of a consolidated set of standards covering anti-counterfeiting.** The ACTF has highlighted that much more coordination is required between the numerous standards and regulatory bodies that have issued or are developing anti-counterfeiting standards and specifications. For example, NASPO, SAE, ANSI, ISO, and JEDEC all either have or are developing such standards and specifications, many of which overlap with each other and sometimes conflict with each other. Unfortunately, too many of these standard and specifications are geared toward providing users with detailed methods to try to identify counterfeits. As described in Section VIII, no suite of test methods, even if conducted on 100% of suspect units, can provide full assurance that products are authentic and reliable. Open market sources and third-party laboratories that claim they can electrically test suspect components almost never can do so as rigorously as OCMs and their Authorized Distributors that use test hardware and test software developed and maintained by product experts. Thus, the only way to guarantee that products are authentic and reliable is to buy them directly from authorized sources. Component purchasers can avoid issues with counterfeits by always adhering to standards and specifications requiring that purchases be from OCMs and their Authorized Distributors/Resellers.

6. **In addition to industry-government initiatives, the SIA ACTF has joined forces with other associations to advance the battle against counterfeit semiconductor components.** The United States SIA is a leading member of the World Semiconductor Council (WSC) Anti-Counterfeiting Task Force (ACTF) that has been active since 2012. The WSC unites the six SIAs from the six major semiconductor-producing countries/regions of the world, i.e., China, Chinese Taipei, Europe, Japan,

Korea, and the United States. [Reference 25.] The WSC ACTF recognizes that the counterfeit semiconductor problem cannot be solved by any one country, but rather requires worldwide strategies and initiatives focused on both the supply and demand for counterfeits. The WSC ACTF is reviewing best practices identified by individual SIAs and is working to deploy them more broadly. This requires extensive interaction with governments worldwide, and a key forum for formalizing these interactions is the Government and Authorities Meeting on Semiconductors (GAMS), which is held annually. [Reference 27.] In addition to working with the WSC ACTF and GAMS, the SIA ACTF interfaces with other associations involved in anti-counterfeiting initiatives, including the Electronic Components Industry Association (ECIA), the Aerospace Industries Association (AIA), and the US Chamber of Commerce. [References 28-30.]

7. **When an OCM discovers that an open market supplier is erroneously indicating they are an Authorized Distributor, the OCM will typically take legal action to stop this misrepresentation.** This is an ongoing problem since open market suppliers continuously establish websites that are intended to make customers think they are Authorized Distributors. For example, when broker websites have banners and/or line cards showing OCMs' logos, the OCMs will issue cease and desist letters. In most cases, brokers will promptly remove OCMs' logos from their websites. In rare cases when brokers do not do so, additional legal actions are taken to prevent brokers from continuing to infringe logos and to deceive customers. In addition, as previously detailed, the SIA ACTF promotes use of the Electronics Authorized Directory so that customers can easily identify Authorized Distributors for all major OCMs. [Reference 13.]

XV. Summary of How to Win the Battle Against Counterfeit Semiconductors

The key to winning the battle against counterfeit semiconductors is elegantly simple: Exclusively buy semiconductor products either directly from the Original Component Manufacturer (OCM) or directly from the OCM's Authorized Distributors/Resellers. By eliminating poor purchasing practices that allow or even encourage procurement from the open market, the Original Equipment Manufacturers (OEMs) and their Contract Manufacturers (CMs) can avoid encountering counterfeits. The OEMs/CMs that procure components exclusively through authorized sources, including Authorized Aftermarket Distributors/Manufacturers, will also eliminate the need to conduct costly, time-consuming, and error-prone authenticity testing. The Authorized Distributors for a given OCM can be easily found on the OCM's website. Alternatively, the following website sponsored by the Semiconductor Industry Association (SIA) provides instant access to Authorized Distributors for most component OCMs: http://www.authorizeddirectory.com/.

The critical importance of buying in-production semiconductor products from OCMs and their Authorized Distributors, and buying legacy products from OCM's Authorized Aftermarket Distributors/Manufacturers, is underscored by the many risks posed by buying components through the open market. As compared to the authorized market, the open market, including independent distributors, brokers, and Internet-based component exchanges, has far fewer controls over proper handling, storage, and transportation of components, and often lacks component traceability to the manufacturer. This lack of controls and traceability, along with the frequency and ease at which components move through this non-authorized supply chain, make the open market an easy target for counterfeiters to infiltrate to sell their illegal products that often have poor reliability. Semiconductor products purchased on the open market may be cheaper in the short-term than those bought from

authorized sources, but they can be far more expensive in the long-term if they are counterfeit and/or were improperly handled and stored, thus potentially resulting in major rework costs and high warranty or liability claims. OCMs and their authorized sources have extensive, proven systems for ensuring semiconductor products are authentic. Thus, OEMs/CMs that have procurement policies requiring purchases exclusively from OCMs and their authorized sources will consistently receive authentic products with high quality and reliability levels and full factory warranties. This in turn will protect the health, safety, and security of people throughout the world that count on reliable electronic products and systems in their daily lives.

XVI. References

1. "Defense Industrial Base Assessment: Counterfeit Electronics," published by the Department of Commerce's Bureau of Industry and Security, January 2010: http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf.
2. Semiconductor Industry Association website: http://www.semiconductors.org/.
3. National Defense Authorization Act for Fiscal Year 2012, H.R. 1540, Section 818: http://www.gpo.gov/fdsys/pkg/BILLS-112hr1540enr/pdf/BILLS-112hr1540enr.pdf.
4. US Customs and Border Protection press release on Operation Infrastructure: http://cbp.gov/archived/xp/cgov/newsroom/news_releases/archives/2008_news_releases/feb_2008/02222008.xml.html.
5. US Customs and Border Protection press release on Operation Infrastructure II: http://cbp.gov/archived/xp/cgov/newsroom/news_releases/archives/2008_news_releases/nov_2008/11202008_7.xml.html.
6. IHS ISuppli press release, "Top 5 Most Counterfeited Parts Represent a $169 Billion Potential Challenge for Global Semiconductor Market," April 4, 2012: http://www.isuppli.com/Semiconductor-Value-Chain/News/Pages/Top-5-Most-Counterfeited-Parts-Represent-a-$169-Billion-Potential-Challenge-for-Global-Semiconductor-Market.aspx.
7. Background Memo: "Senate Armed Services Committee Hearing on Counterfeit Electronic Parts in the Department of Defense's Supply Chain," November 8, 2011: http://www.levin.senate.gov/newsroom/press/release/background-memo-senate-armed-services-committee-hearing-on-counterfeit-electronic-parts-in-the-dod-supply-chain.
8. Oral Testimony of SIA President Brian Toohey during the Senate Armed Services Committee Hearing on Counterfeit Electronic Parts in the Department of Defense's Supply Chain, November 8, 2011: http://www.semiconductors.org/news/2011/11/08/news_2011/sia_president_testifies_at_senate_armed_services_committee_on_dangers_of_counterfeit_chips/.
9. Business Week article and video from October 13, 2008: http://images.businessweek.com/ss/08/10/1002_counterfeit_narrated/index.htm.
10. MIL-HDBK-217F: "Military Handbook - Reliability Prediction of Electronic Equipment," December, 1991: http://www.sre.org/pubs/Mil-Hdbk-217F.pdf.
11. SAE AS5553, "Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition," available for purchase at http://www.sae.org/.

12. IDEA-STD-1010. “Acceptability of Electronic Components Distributed in the Open Market,” available for purchase at http://www.idofea.org/.
13. Electronics Authorized Directory: http://www.AuthorizedDirectory.com/.
14. “Senate Armed Services Committee Hearing on Counterfeit Electronic Parts in the Department of Defense’s Supply Chain,” Slide 01, November 8, 2011: http://www.armed-services.senate.gov/statemnt/2011/11%20November/Documents%2011-08-11/1.pdf.
15. Federal Bureau of Investigation press release on the J.J. Electronics case: http://www.fbi.gov/losangeles/press-releases/2009/la012109a.htm.
16. US Department of Justice press release on the VisionTech Components case: http://www.justice.gov/usao/dc/news/2011/oct/11-472.html.
17. US Department of Justice press release on the MVP Micro case: http://www.justice.gov/usao/dc/news/2012/feb/12-065.html.
18. US Department of Justice press release on the Epic International Electronics case: http://www.justice.gov/opa/pr/2013/July/13-crm-790.html.
19. Government-Industry Data Exchange Program: http://www.gidep.org/.
20. Government Accountability Office (GAO) Department of Defense (DoD) Supply Chain Report: “Suspect Electronic Parts Can Be Found on Internet Purchasing Platforms,” February 2013: http://www.gao.gov/assets/590/588736.pdf.
21. JEDEC Standard JESD48C: “Product Discontinuance,” December 2011, available for download after registration at http://www.jedec.org/.
22. Counterfeit Electronic Parts and Electronic Supply Chain Symposium: http://www.smta.org/counterfeit/.
23. Diminishing Manufacturing Sources and Material Shortages (DMSMS) Conference: http://www.dmsms2012.com/.
24. Customs and Border Protection (CBP) Centers of Excellence and Expertise (CEE): http://www.cbp.gov/linkhandler/cgov/trade/trade_transformation/industry_int/cee_overview.ctt/cee_overview.pdf.
25. Customs and Border Protection (CBP) Intellectual Property Rights (IPR) Fiscal Year 2012 Seizure Statistics: http://www.cbp.gov/xp/cgov/trade/priority_trade/ipr/.
26. World Semiconductor Council website: http://www.semiconductorcouncil.org/wsc/.
27. Government and Authorities Meeting on Semiconductors: http://www.semiconductors.org/news/2012/08/27/trade-article/13th-government-and-authorities-meeting-on-semiconductors-gams-sept.-24-28-2012/.
28. Electronic Components Industry Association: http://www.eciaonline.org/default.aspx.
29. Aerospace Industries Association: http://www.aia-aerospace.org/.
30. US Chamber of Commerce: http://www.uschamber.com/.

XVII. Acknowledgements

SIA would like to thank the following people for their contributions to this paper: Andrew Olney, Analog Devices, Inc., Chairman of the SIA Anti-counterfeiting Task Force, for editing the paper and providing much of the content; Corrina Sinatro, Advanced Micro Devices; Brian Way, Altera Corporation; Tom Kane, Analog Devices, Inc.; Brad Bryson and Jack Taylor, Freescale Semiconductor; Taffy Kingscott, IBM Corporation; Steven Jeter, Infineon Technologies; Greg Warder, Integrated Device Technology; David Brown and Lawrence "Lonnie" Hurst, Intel Corporation; Lee Mathiesen, Lansdale Semiconductor; Daryl Hatano and Gary Pugsley, ON Semiconductor; Ron Davis, Qualcomm; Dan Deisz, George Karalias, and Steve Hirschfeld, Rochester Electronics; Barry Dove and Billy Nixon, STMicroelectronics; Lisa Maestas, Paula Collins, and Rick Logsdon, Texas Instruments; James Burger, Thompson Coburn LLP.

