As originally published in the SMTA International Conference Proceedings.

AN INDUSTRY UNITED TO FIGHT COUNTERFEITING. A COUNTERFEIT EEE PARTS SOLUTION

Daniel DiMase
Honeywell Technology Solutions Inc.
Columbia, MD, USA
daniel.dimase@honeywell.com

Phillip Zulueta
Jet Propulsion Laboratory
Pasadena, CA, USA
phillip.j.zulueta@jpl.nasa.gov

INTRODUCTION

Counterfeit electrical, electronic, and electromechanical (EEE) parts pose a significant threat in the global supply chain. Equipment failures or malfunctions can present situations that cause mission failures, health and safety concerns and could jeopardize national security. The counterfeit issue is magnified as an increasing number of companies outsource portions or all of their assemblies to reduce labor, overhead and capital expenditures. Companies often experience complications when trying to control or maintain quality as they outsource procurements or manufacturing and lose the associated visibility and control. As a result, companies are becoming increasingly co-dependent to continue production of quality product.

Material circulates among companies, across borders, and around the world. Once the supply chain has been tainted with bad product, no company is immune. Original component manufacturers (OCMs), franchised and independent distributors, brokers, original equipment manufacturers, and government agencies need to have processes and procedures in place to combat the problem. The problem will not get solved with only a few links of the supply chain combating the issue. If each link in the supply chain would create and implement a counterfeit parts control plan that would tighten controls, the risk of this growing dilemma could be mitigated.

This paper will segment the market and present a possible solution in an industry that unites to combat the counterfeit problem. It will address solutions to the counterfeit EEE parts problem and what each link in the supply chain could do to help eliminate the problem.

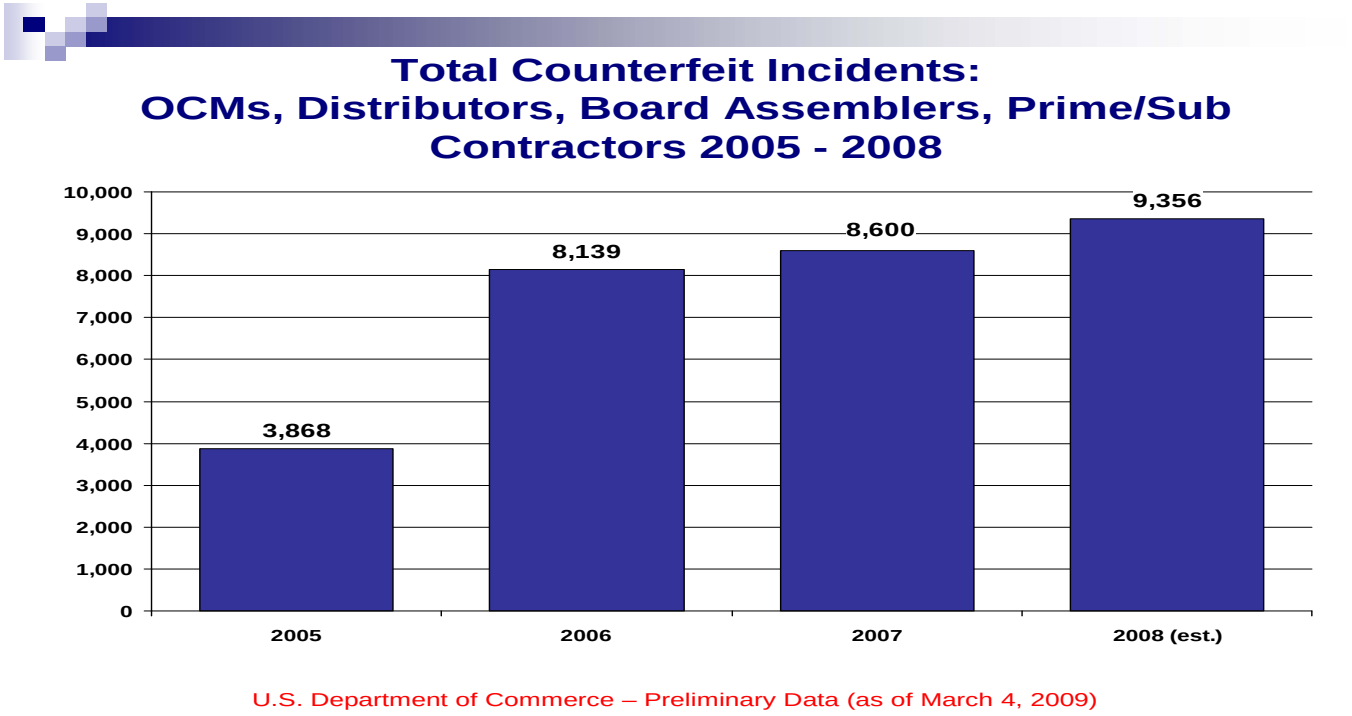
Key words: Combating Counterfeiting, Counterfeit Part Mitigation

MAGNITUDE AND SCOPE OF COUNTERFEIT PROBLEM

Many organizations are still trying to determine the scope and magnitude of the counterfeit problem and more importantly, determine how it affects or can affect them. In reality, counterfeiting has become a global epidemic. The U.S. Chamber of Commerce has estimated that counterfeiting costs the global economy over $600 billion per year and accounts for over 7% of global merchandise trade.[1] Interpol has reported that counterfeiting is one of the preferred methods of financing for terrorist organizations and crime syndicates.[2] The fines in some nations for counterfeiters are small, and even if they are prosecuted, there typically isn't any jail time. Even though the U.S. Department of Justice (DOJ) is doing more than at any other time in history, it only reports filing a total of 217 intellectual property cases in fiscal year 2007. This is less than one-third of one percent of the total criminal cases filed by the DOJ last year.[3] The number of counterfeit electronics seizures as a percentage of total value seized from U.S. Customs and Border Protection has increased from 5% in 2006 to over 9% in 2007.[4]

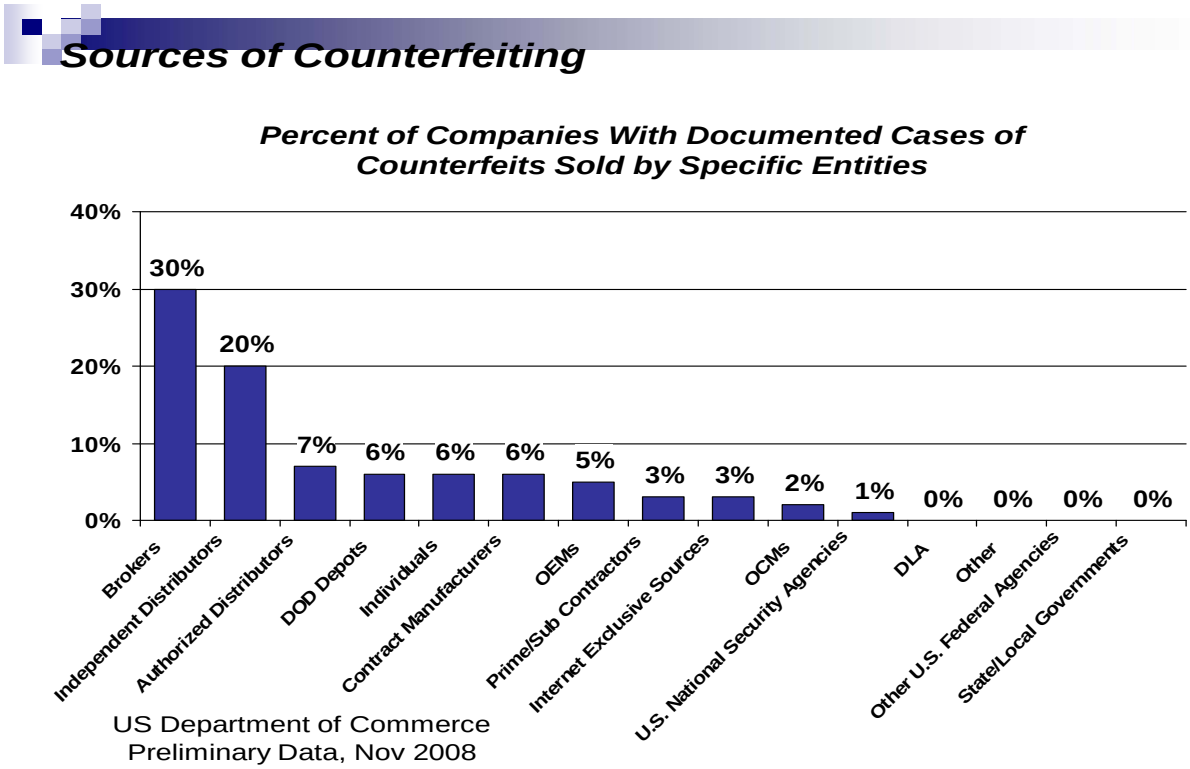
The U.S. Department of Commerce, Office of Technology Evaluation recently surveyed 498 participants in the industry to assess the scope and magnitude of the EEE counterfeit parts problem. The participants included original component and equipment manufacturers, franchised and independent distributors, prime contractors, subcontractors, Department of Defense arsenals, depots, and the Defense Logistics Agency. 39% of the respondents encountered counterfeits. The results further report that the total number of incidents the participants saw in 2008 was over 9,500, up an additional 10% from the prior year [see Exhibit 1]

Exhibit 1



The report also revealed that 2% of the original component manufacturers surveyed experienced counterfeits, proving that no one is immune from the problem [see Exhibit 2].

Exhibit 2



CONSEQUENCES OF COUNTERFEIT EEE PARTS

The consequences of counterfeit EEE parts can be devastating. Imagine a counterfeit EEE part in a defibrillator or other health related electronic device. How about a counterfeit part on a navigation system for a commercial or military plane, or an electronic device controlling the brakes on your vehicle? Counterfeits could pose a variety of health and safety concerns. Real life examples prove how devastating counterfeits can be. There was a report of an exploding counterfeit cell phone battery that blew fragments into a 13-year-old boy's face.[5] There have been incidents of recalled counterfeit Square D circuit breakers that may not trip when they are required, posing the risk of fire hazards.[6] In another example, NASA recently detected an unspecified counterfeit on the Kepler spacecraft, possibly contributing to the nine month delay and project cost overrun.[7]

There have also been reports of counterfeit computer networking gear installed in a number of government agencies.[8] This should cause serious concern, particularly if the product was sold for state-sponsored purposes to gain internal access to computer systems and data. The F.B.I. and the Pentagon have elevated their concerns after Operation Cisco Raider led to 15 criminal cases and the discovery of over 3,500 counterfeit Cisco network components, involving products bought by military agencies and contractors, and electric power companies in the United States.[9] Counterfeit electronics could be fabricated to include an electronic Trojan horse with hidden circuitry that allows "backdoor" entry to gain entry or extract data from a system, or contain a hidden kill-switch to disable an electronic system, or for some other sinister purpose. A recent Wall Street Journal article reported that computer spies broke into the Pentagon's F-35 fighter jet database and have siphoned off several terabytes of data about the plane's design and electronics systems.[10] The article didn't report counterfeit parts as the root cause of the problem, but one can speculate based on the overwhelming evidence. National security could be compromised in a variety of fronts with counterfeit EEE parts. As an example, there were rumors that a sophisticated Syrian radar system was shut down remotely by a kill-switch on a counterfeit microprocessor that allowed Israel to fly in undetected and bomb a suspected nuclear facility.[11]

COUNTERFEITS AND THE OUTSOURCING TREND

The counterfeit issue is further magnified with the outsourcing trend. More and more companies are outsourcing, even among original chip manufacturers (OCM). Very few OCMs design and manufacture their own devices and they have gone "fabless" in recent years, meaning they no longer produce their own chips. Complex equipment such as airplanes and satellites require coordination among thousands of suppliers to complete the final assembly. Controlling and maintaining quality becomes a complicated effort as organizations lose quality visibility and control, particularly as the visibility becomes more clouded further down the supply chain.

SOLUTIONS

Within the last year, a standard was developed and recently published through SAE International that provides requirements, practices and methods to counteract the counterfeit threat. SAE AS5553 was created to provide uniform requirements, practices and methods to mitigate the risks of receiving and installing counterfeit electronic parts. The document is intended for use in aviation, space, defense, and other high performance/reliability electronic equipment applications and is recommended for use by all contracting organizations that procure electronic parts, whether such parts are procured directly or integrated into electronic assemblies or equipment. The requirements of the standard are generic and intended to be applied/flowed down to all organizations that procure electronic parts, regardless of type, size, and product provided. The document requires organizations to create and implement a counterfeit parts control plan (CPCP) that documents its processes used for risk mitigation, disposition, and reporting of counterfeit parts. Guidance for the development of this control plan is provided and contains specific processes to address counterfeit electronic parts issues.

SAE AS5553 outlines requirements in several specific areas in an organizations structure. It requires processes to maximize the availability of authentic parts throughout the product life cycle, including management of obsolescence. A purchasing process is required that specifies a preference to procure directly from original component manufacturers and their authorized sources. This process requires the assessment and mitigation of risks when procuring parts from sources other than OCMs or authorized suppliers. Additionally, the purchasing process requires maintaining a register of approved suppliers in the supply chain base. Information on the source of supply needs to be gathered and maintained to mitigate the risk of receiving counterfeit parts, which may include reports, audits, surveys, and reviews on suppliers. Purchase order quality requirements need to be included in the plan. Verification plans need to be included in the CPCP to assure detection of counterfeit parts. The standard requires a plan for material that is still being manufactured and material that is in the field. In addition, the standard requires a process that specifies control methods for documents. Finally, it requires a reporting process when counterfeit parts are detected in an organizations process. Information and guidelines for reporting counterfeit parts are provided in the standard.

Addressing counterfeit issues will increase the cost of doing business. Procedures in the way business is conducted will change. Some existing procedures will only be modified with minimal changes in effort. However, the implementation of new supplier control programs, audits, new purchasing procedures, new receiving inspection procedures and training, new counterfeit detection methods/testing and the replacement of counterfeit parts will likely increase costs and impact schedules. Ignoring the threat of counterfeit parts can also increase costs; however,

as each link in the supply chain works to improve their processes, these costs can be partially mitigated.

LINKS IN THE SUPPLY CHAIN - OCM

One of the first steps in ensuring that a company's intellectual property, products, services and public image are protected is to register their trademark. The intent of a trademark is to "brand" or differentiate the products of one company with that of another, so as to clearly indicate the originating producer. A trademark may include a single word, a unique phrase, a name, a symbol, a specific logo design, or it may be a combination of any or all of those. A proper trademark is represented by the trademark symbol - ™ and while on the surface, this process may seem unnecessary, a trademark is a highly valuable business asset and must be registered to be protected by law and used exclusively.

An additional action an OCM can take is recordation of their validly registered trademarks and copyrights with U.S. Customs and Border Protection (CBP). Recordation enables OCMs to electronically record their trademarks and copyrights with CBP and makes information readily available to CBP personnel to protect their intellectual property. CBP uses this information to actively monitor shipments crossing the U.S. borders and assist them when they are facilitating counterfeit seizures. It can prevent the importation or exportation within the U.S. of counterfeit goods. Applications can be submitted online for a one-time fee of $190, which is valid for the term of the trademark. The process is detailed on www.cbp.gov.

Once a counterfeit incident is reported to an OCM by a consumer, the OCM can assist the consumer in verifying the supply chain of custody in attempts to verify original sourcing. However, there are some OCMs that will not assist a consumer if they learn the device was not purchased directly from them or their authorized distributors. This practice makes it difficult for the industry to combat counterfeiting. The OCM and their authorized distributors have information that can assist the consumer in verifying authenticity of the device. Information such as authentic date codes, lot codes and serial numbers, accepted part markings, material content, and sample x-ray patterns of the components they supply could be retained and compared to suspect material to identify obvious cases of counterfeits. OCMs have this information, but it may not be readily available in a centralized database that is available for reference when a suspect counterfeit incident occurs.

OCMs could ensure they have adequate controls for their scrap material. There are many documented cases of rejected parts that have made their way out of the factories and into the gray market,[12] which is the market for the trade of electronics through distribution channels which, while legal, are unofficial, unauthorized, or unintended by the original manufacturer. Prior to the sudden rise of counterfeiting, many OCMs did not have processes to control their scrap material. However, many have instituted controls over the last few years, but there may be room for improvement. If material is going to be smelted for metal recovery, it could be crushed before it is sent to a recycler. If it is being disposed, it could also be crushed to avoid "dumpster diving", a practice where fraudulent individuals will search dumpsters for material to resell. Surveillance and security measures could be instituted to control scrap material and to ensure untested material isn't being sneaked out of the factory by unscrupulous employees.

LINKS IN THE SUPPLY CHAIN - OEMS

Original equipment manufacturers (OEMs) could also to do their part in combating the problem. SAE AS5553 provides excellent guidance appropriate for OEMs. In addition, OEMs could retain photographs of authentic parts and x-ray patterns they use for comparison of incoming inspection. Their engineering drawings could include accepted part markings and dimensions of individual parts for use at incoming inspection. If they subcontract their assembly with contract manufacturers (CMs), they can flow down AS5553 requirements to better ensure their CMs and lower tier contractors have appropriate controls and security in place.

Erick Prause, the Director of Supplier Development for a contract manufacturer, Jabil, commented that they are working with their OEM customers by identifying additional key areas that can mitigate the risk of receiving counterfeit parts. These include predictive obsolescence management, design for manufacturability, and validation of design, alternate component management, inventory management, and monitoring market conditions and inventory positions.

There are a number of service providers that offer predicted life cycles and obsolescence status of electronic parts. The capabilities of predictive obsolescence management could be employed during the design phase to ensure the optimum component choice based on the longest potential life cycle. Multiple sources are recommended whenever possible and practical. In some cases, the printed circuit board may include pads to accommodate different sized parts to maximize alternatives. For instance, the board may be designed to accommodate a 300-mil or 400-mil memory chip.

Validation of design occurs after launch of the project with continuous monitoring of the bill of materials (BOM) and the capabilities of predictive obsolescence management. Items on the BOM reaching the end of their life cycle or that are discontinued become inputs that trigger a lifetime buy or potential redesign of the project. Engineers focus on the maintenance of the design by identifying alternative components and bundling changes to minimize overall costs. Additionally, better utilization of component manufacturers' capabilities due to Moore's Law reduces the level of product validation required to make changes. Through greater visibility of the projected life cycle of components on the BOM and open communication with the design team, better decisions can be made if and when to

make last time buys from more reliable sources on products or if design changes are more practical.

Last, monitoring inventory positions and market conditions help to make good inventory management decisions. Extra inventory may need to be bought from reliable sources if the lead-times are getting longer for particular items on the BOM to avoid buying it from riskier sources.

LINKS IN THE SUPPLY CHAIN – Franchised/Authorized Distributors, Independent Distributors, and Brokers

Distributors could also contribute to the solution. A database recording shipment date codes, lot codes, serial numbers, photographs, x-ray images, packaging and part dimensions could be established and cross referenced to invoices and packing lists. This information becomes a valuable resource if a customer inquiry arises and is also useful before or when customer returns are made. The database allows a comparison to the original shipments to ensure substitutions haven't been made. These additional efforts add value to the extent that the database becomes a quality tool to compare lots of materials against known good parts.

Independent distributors (ID) and brokers can provide assistance in addressing counterfeit issues. Most of the counterfeit incidents reported have occurred through a broker or an ID. Brokers and IDs can have processes and procedures in place to address the problem. All personnel that handle the parts can be trained to identify suspect product. The Independent Distributors of Electronics Association (IDEA) has a standard (IDEA-STD-1010A) available to train personnel to visually identify suspect counterfeit product. They also have a certification program for inspectors. Checklists can be established and maintained for each shipment, detailing the inspection performed. Invoices, purchase orders, date codes, lot codes, and serial numbers should be cross referenced on the checklists. A free sample checklist is available on the IDEA website. More information is available at www.idofea.org Inspection records and checklists can be retained and copied to customers.

Since brokers and independent distributors often have a wide range of sources, they are often the victims of counterfeit components. However, they also have the ability to collect and maintain significant data on their suppliers. For example, there are blogging sites available for traders to communicate such as www.orafec.org and many of the internet sourcing engines they use provide a blogging site to share experiences. Brokers and IDs can avoid falling victim to unscrupulous individuals if they review industry comments on suppliers and set up the appropriate precautions.

Fraudulent individuals will often change the name of their company after they commit a crime, but may not change other critical information like a telephone number or address. Software tools to discover organizations that have multiple aliases could be established by looking for duplicate telephone, mobile and fax numbers, address, web-sites, bank account numbers, bank beneficiaries, e-mail addresses, shipping account numbers, tax numbers such as the federal identification number and state tax resale certificate, DUNs numbers, and CAGE code numbers.

Independent distributors and brokers could maintain approved supplier lists that include a risk ranking process. In addition, they could maintain a database of items that have been identified as counterfeit to ensure problems aren't repeated. The ranking could be based on past-performance and industry information. They could review information about past problems from their own organization and from the Government/Industry Data Exchange Program (GIDEP) www.gidep.org and ERAI www.erai.com. Both GIDEP and ERAI maintain information on counterfeit parts and quality issues and report the data back to their members. They could inform their inspectors on the risk ranking of their suppliers and flag items that have been known to be counterfeited in the past, and step up inspection on riskier suppliers and parts. A database of manufacturer datasheets can also be a useful tool in the authentication of parts. Obsolete part data sheets are available from a number of service providers. These data sheets could be made available to inspection personnel for every shipment.

LINKS IN THE SUPPLY CHAIN – END USER

Similar to OEMs, the End User of electronic components has the ability, often significantly, to mitigate counterfeit part issues through compliance with SAE AS5553 and flowing down requirements to their suppliers, subcontractors and lower tier subcontractors. When the End User buys from Distributors or Brokers, they can require and retain copies of any inspection reports and perform additional testing and inspection as required to authenticate the product.

It should be noted that third party test and analysis facilities can also be a valuable supplier resource to the End User in conducting device authentication. These facilities have varying capabilities and perform different services. These tests and services should be evaluated on the basis of device criticality in the particular application.

GOVERNMENT AGENCY INVOLVEMENT

Government agencies can also provide some assistance combating counterfeiting. U.S. Customs and Border Protection (CBP) have legal authority to intercept and confiscate suspect counterfeit product that crosses the U.S. border. U.S. companies involved in the transaction have 30 days to dispute the findings and could be fined up to the quantity confiscated multiplied by the manufacturer's suggested resale value of the product. Known repeat offenders could also get audited by CBP to evaluate the company's import and export procedures.

There has been recent debate that CBP should not delegate to the rights holders to make a determination if an item is

counterfeit.[13] The alternative suggested is that the Original Component Manufacturers (OCMs) provide production records and chip markings to CBP as opposed to CBP sending data to the OCMs for their review, to avoid violation of the Trade Secrecy Act. Experts agree that the rights holders (e.g. Original Component Manufacturers) are best qualified to determine device authenticity. OCMs may not be willing to provide proprietary data to CBP, and even if they were, it may be difficult to create a unified database to store information on multiple products from multiple OCMs. Industry can support legislation that would allow CBP the statutory authority to consult IP and trademark rights holders for assistance in determining whether or not goods crossing the U.S. border are authentic. This could include allowing CBP to provide photographs of the complete components markings and other shipping artifacts to the OCM to assist in their authenticity assessment.

Timothy Trainer, President of the Global Intellectual Property Strategy Center, P.C. recently testified before the U.S. House Committee on Foreign Affairs regarding global protection of intellectual property. He made several recommendations in his testimony to combat the counterfeiting problem:[14]

1. Instruct U.S. Customs and Border Protection (CBP) to adopt its proposed IP rules that were published on October 5, 2004, that will help IP owners and CBP improve overall enforcement;
2. Strengthen border and criminal enforcement to provide for clear ex officio IP enforcement by CBP and U.S. Immigration and Customs Enforcement (ICE), FBI and the Justice Department in accordance with our laws and Free Trade Agreements;
3. Improve consumer protection against counterfeit and pirate products by instructing CBP to take immediate steps to seize infringing goods before they are released and subject to redelivery, which may not be possible once goods are in the stream of U.S. commerce;
4. Amend relevant trademark, copyright and customs laws to clearly authorize enforcement actions against infringing goods that are being exported and moving in-transit;
5. Provide the Department of Homeland Security (DHS)/CBP attorneys the legal authority to collect administrative fines and pursue judicial forfeiture of infringing goods, including in cases when the Department of Justice refuses to pursue these cases;
6. Increase IP-dedicated CBP/ICE officers to IP enforcement;

CBP could make some additional changes that could help combat the problem. Currently, CBP does not report confirmed counterfeit part incidents to the Government/Industry Data Exchange Program (GIDEP). The discovery of a counterfeit part incident is not isolated to a single incident and the likelihood of continued proliferation of the same counterfeit device remains. Reporting information to GIDEP increases industry awareness and potentially removes more counterfeit material from circulation.

In a more radical move, CBP could expand their Customs-Trade Partnership Against Terrorism (C-TPAT) program with a proposed "Trusted Importer" program. C-TPAT is a voluntary government-business initiative to build cooperative relationships that strengthen and improve overall international supply chain and U.S. border security. C-TPAT recognizes that CBP can provide the highest level of cargo security only through close cooperation with the ultimate owners of the international supply chain such as importers, carriers, consolidators, licensed customs brokers, and manufacturers. The concept of a "Trusted Importer" program would be to unite government and industry in combating the counterfeit problem, since CBP cannot inspect every inbound shipment. Participating companies would surrender imported suspect counterfeit parts they discover from their inspection process to CBP.

To participate in the program, organizations could submit an application to CBP that would include supporting evidence they are practicing due-diligence in supply chain management and adhering to the rules of the Office of Foreign Asset Control, a listing of the equipment they use in counterfeit part detection, a copy of their inspection process and a copy of their counterfeit parts control plan to ensure they have processes and controls to mitigate the risk. The concept of the "Trusted Importer" application is to encourage trade-risk conscientious importers that have the ability to identify counterfeits to work with the government in combating the problem.

CBP could use the increased data from the "Trusted Importer Program" to target risky suppliers and high-risk material. The program could also allow CBP to determine if a company participating in the program is "going rogue". If an importer is regularly engaging with companies that have been identified as a risk, then CBP may elect to conduct an audit on the organization to determine if they are adhering to the rules of the program.

COUNTERFEIT REPOSITORY

When a counterfeit part is encountered, there is typically a financial dispute between the buyer and seller regarding payment. A financial dispute can occur when the parties argue over the return and payment of material. Many buying companies are now including terms and conditions that enable them to quarantine parts and skip payment of material if parts are counterfeit. However, most selling companies won't credit an invoice until they receive material back on a return. A buying company claiming material is counterfeit and seizing the material without payment is a conflict of interest for the buying company since they need the material. The action could lend itself to fraud. Fraudulent companies could incorporate terms and conditions to address the problem and claim legitimate

material is counterfeit, not pay for it, and use the material. An independent third-party organization (possibly a government agency) that acts as a repository would be the best way to avoid such a problem.

A program like this could also assist investigative agencies. To describe the current situation, a typical investigation and prosecution may cost the government over $100K, so they are typically looking for larger dollar amounts than what is typically seen in the electronics industry individually. A problem under $500K isn't viewed as large, allowing the crooks to fly under the radar in most cases. This type of service would allow the government to track aggregate issues and target problem areas more affectively.

In addition, most companies don't know which investigative agency they need to report to when they encounter a counterfeit incident. In the U.S., depending on the issue, it may require involvement with Defense Criminal Investigation Service, Immigrations and Customs Enforcement, Customs and Border Protection, Federal Bureau of Investigation, Naval Criminal Investigation Service or others. Organizations typically won't know who to contact even if they pick the appropriate agency. When they contact the right agency, they may not get the time the incident deserves due to low dollar amounts involved. U.S. Immigration and Customs Enforcement has created a National Intellectual Property Rights Coordination Center in Washington, D.C. in an attempt to coordinate the counterfeit effort among agencies, but it has been slow in receiving support and gaining the resources it needs to tackle the problem. The repository could track counterfeit activity in the market, make sure the appropriate agency is informed on the issue, report the incident to GIDEP, and elevate the problem if it warrants any further action.

A program like this would not be easy to put together logistically. It would require some serious planning to implement effectively, but it could help get counterfeit material out of circulation, inform the appropriate investigative agencies, help avoid trade disputes among buying and selling companies, accumulate data on seized items, and last, inform GIDEP so that their members can avoid counterfeit material that may still be circulating in the supply chain.

Industry could also support changes to the U.S. Federal Acquisition Regulations (FAR), which currently encourages government agencies to award contracts to the company who offers the lowest price and does not look at other parameters such as quality performance, source selection, and supply chain traceability. This policy is a major cause for counterfeits getting into government agencies. The FBI has announced that the current procurement rules are one of the primary causes for counterfeit computer networking gear finding their way into government computer systems.[15] The U.S. government could incorporate FAR instructions and clauses that will explicitly address and mitigate the problem. Changes to the FAR could include source selection, supply chain traceability, contractor certificate of authenticity, and test and inspection paperwork. Industry creates approved vendor lists based on quality and performance. Government should also participate in these best practices.

An additional step the government could take is to fund research and assemble a team that creates advanced forensic techniques for detecting hidden counterfeit circuitry or "Trojan Horses" in electronic devices. The U.S. Pentagon's Defense Advanced Research Projects Agency began distributing tainted chips to military contractors who are participating in the Trusted Integrated Circuits program to see if they have the ability to detect hidden circuitry.[16] This project could be expanded with a dedicated team of experts that could be available to assist government agencies in identifying authenticity for military and government sensitive electronic devices. Additionally, CBP could flag items that are crossing borders and have been identified as mil-spec items or used in a critical applications, and work with the team to identify counterfeit problems and ensure authenticity in critical applications.

INTERNATIONAL COOPERATION

Counterfeiting is a global epidemic that can be mitigated with expanded international cooperation. There are a number of international forums where countries engage in discussions and trade agreements where intellectual property rights (IPR) issues are discussed. Continued discussion, education, and cooperation could assist in combating the problem.

IPR legislation and enforcement is foreign to many countries who may not understand the benefit of creating them. Continued dialog and education regarding the benefits of strengthening IPR legislation and enforcement at international forums could have a significant impact on mitigating the problem. Innovation and creativity are the foundation of global economic development. IPR infringement hinders growth by destroying the foundation that is necessary to support and encourage innovation and creativity. Counterfeiting also damages the economies of the countries in which it occurs as they lose potential tax revenue. Counterfeiters typically do not pay taxes or duties in their transactions. In many cases, they forge the paperwork of their transactions to significantly reduce the value of their trades, or in other cases, exploit Free Trade Zones to circumvent taxes and duties.

International cooperation regarding IPR issues are discussed at a number of forums including the G-8, the US-EU summit, and the Organization for Economic Cooperation and Development (OECD). The Office of the United States Trade Representative (USTR) lists some of the various mechanisms they are promoting to ensure adequate protection and enforcement of IPR issues. Initiatives such as the World Trade Organization agreements and the Council for Trade Related Aspects of Intellectual Property Rights (TRIPS), bilateral and regional initiatives including free trade agreements, and the Anti Counterfeiting Trade Agreement (ACTA) are just some of the internationally

coordinated efforts that the USTR are engaging to promote and expand international cooperation.[17]

International cooperation among government enforcement agencies could also assist in combating the counterfeit problem. The U.S. and the European Union recently conducted a joint investigation that resulted in over 360,000 fake computer components being seized in their joint operation.[18] Continued cooperation could help mitigate and combat the problem.

Tim Trainer makes some global recommendations in his testimony to U.S. Congress that include:[19]

1. Continue efforts to raise IP enforcement standards in the territories of our trading partners regarding criminal and border enforcement;
2. Use inter-governmental organizations such as INTERPOL and the World Customs Organization, to promote increased enforcement activity and new standards;
3. Identify cases that strike at organized crime groups;
4. Provide better IP enforcement assistance programs that address the operational implementation of enforcement activity, not just changes in laws; and
5. Expand IP technical assistance programs to include IP awareness raising among the general public abroad by:
    a. Balancing the emphasis on enforcement with more programs addressing the benefits of IP; and
    b. Using technology to create more interesting IP education programs.

Organizations like the World Intellectual Property Organization, World Trade Organization, Interpol and the World Customs Organization would be logical organizations that could expand services, international agreements, and enforcement that help unite countries and multi-national agencies combating the problem on a global basis.

SUMMARY

In summary, the industry needs to unite in order to combat the growing counterfeit dilemma. Counterfeiting is big business that creates health and safety concerns, threatens national security, eliminates jobs, damages the economies of the countries in which it occurs, and supports financial activity for terrorist organizations and crime syndicates. The first step to control the problem is to create a plan. All sectors of the supply chain could create counterfeit parts control plans that will address the issue and the unique concerns of their individual sector and supply chain channels. The U.S. government has been a worldwide leader in protecting the rights of intellectual property holders. Some of their practices and laws could be instituted in other countries to combat the problem. Industry and government agencies worldwide need to cooperate and create radical programs to address this very serious issue. Together, an industry united with global cooperation and government assistance can make a difference and help mitigate the counterfeit parts problem.

REFERENCES

[1] U.S. Chamber of Commerce, press release: **"**Chamber Praises New Senate Anti-Counterfeiting Bill Urges Quick Passage," 16 Sep. 2005.

[2] United States. Congress. Text of public testimony of by Ronald K. Noble, Secretary General of Interpol before the United States House Committee on International Relations One hundred eighth congress. Washington, D.C.: 16 Jul. 2003.

[3] United States. Congress. House of Representatives. Committee on the Judiciary. Markup of H.R. 4279, The Prioritizing Resources and Organization for Intellectual Property Act of 2008. Washington, D.C.: 30 Apr. 2008.

[4] Sperling, Ed. "The battle over counterfeit goods." Electronic Business. 10 Nov. 2007.

[5] "Exploding cell phones prompt warnings." Associated Press. 23 Nov. 2004.

[6] U.S. Consumer Product Safety Commission, press release: "Connecticut Electric Recalls Counterfeit Square D Circuit Breakers Due To Fire Hazard," Release #08-054, 30 Oct. 2007.

[7] "Aerospace & Defense News – Space." AirGuide Business. 9 Mar. 2009.

[8] Grow, Brian, et al. "Dangerous Fakes." BusinessWeek. 2 Oct. 2008.

[9] Markoff, John. "F.B.I. Says The Military Has Bogus Computer Gear." The New York Times. 9 May 2008.

[10] Gorman, Siobhan, August Cole, and Yochi Dreazen. "Computer Spies Breach Fighter-Jet Project." The Wall Street Journal. 21 Apr. 2009.

[11] Adee, Sally. "The Hunt for the Kill Switch." ieee Spectrum. May 2008.

[12] "IC resale scandal rocks AMD, Seagate, ST." EE Times. 29 Sep. 2005.

[13] United States. U.S. Department of Homeland Security. U.S. Customs and Border Protection. The Departmental Advisory Committee on Commercial Operations of Customs and Border Protection And Related Functions (COAC). IPR minutes March 20th 2009

[14] United States. Congress. House. Committee on Foreign Affairs. Sinking the Copyright Pirates: Global Protection of Intellectual Property. Van Nuys, CA: 6 Apr. 2009.

[15] Brewin, Bob. "FBI partially blames procurement rules for fake IT products." Nextgov. 12 May 2008.

[16] Markoff, John. "F.B.I. Says The Military Has Bogus Computer Gear." The New York Times. 9 May 2008.

[17] United States. Office of the United States Trade Representative. 2009 Special 301 Report. 30 Apr. 2009.

[18] U.S. Department of Homeland Security. Customs and Border Protection, press release: "CBP, European Union Announce Results of Joint Operation to Combat Pirated Goods," 22 Feb. 2008.

[19] United States. Congress. House. Committee on Foreign Affairs. Sinking the Copyright Pirates: Global Protection of Intellectual Property. Van Nuys, CA: 6 Apr. 2009.