AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 112–340

THE COMMITTEE'S INVESTIGATION INTO COUNTERFEIT ELECTRONIC PARTS IN THE DEPARTMENT OF DEFENSE SUPPLY CHAIN

HEARING

BEFORE THE

COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

NOVEMBER 8, 2011

Printed for the use of the Committee on Armed Services

Available via the World Wide Web: http://www.fdsys.gov/

U.S. GOVERNMENT PRINTING OFFICE

72–702 PDF WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON ARMED SERVICES

CARL LEVIN, Michigan, *Chairman*

JOSEPH I. LIEBERMAN, Connecticut
JACK REED, Rhode Island
DANIEL K. AKAKA, Hawaii
E. BENJAMIN NELSON, Nebraska
JIM WEBB, Virginia
CLAIRE MCCASKILL, Missouri
MARK UDALL, Colorado
KAY R. HAGAN, North Carolina
MARK BEGICH, Alaska
JOE MANCHIN III, West Virginia
JEANNE SHAHEEN, New Hampshire
KIRSTEN E. GILLIBRAND, New York
RICHARD BLUMENTHAL, Connecticut

JOHN MCCAIN, Arizona
JAMES M. INHOFE, Oklahoma
JEFF SESSIONS, Alabama
SAXBY CHAMBLISS, Georgia
ROGER F. WICKER, Mississippi
SCOTT P. BROWN, Massachusetts
ROB PORTMAN, Ohio
KELLY AYOTTE, New Hampshire
SUSAN M. COLLINS, Maine
LINDSEY GRAHAM, South Carolina
JOHN CORNYN, Texas
DAVID VITTER, Louisiana

RICHARD D. DEBOBES, *Staff Director*
DAVID M. MORRISS, *Minority Staff Director*

CONTENTS

CHRONOLOGICAL LIST OF WITNESSES

THE COMMITTEE'S INVESTIGATION INTO COUNTERFEIT ELECTRONIC PARTS IN THE DEPARTMENT OF DEFENSE SUPPLY CHAIN

NOVEMBER 8, 2011

	Page
Sharpe, Thomas R., Vice President, SMT Corporation and Liberty Component Services	15
Hillman, Richard J., Managing Director, Forensic Audits and Investigative Service, Government Accountability Office; Accompanied by Dr. Timothy Persons, Chief Scientist, Center for Science, Technology, and Engineering, Government Accountability Office	25
Toohey, Brian C., President, Semiconductor Industry Association	34
O'Reilly, LTG Patrick J., USA, Director, Missile Defense Agency	72
Kamath, Vivek, Vice President, Supply Chain Operations, Raytheon Company	83
DeNino, Ralph L., Vice President, Corporate Procurement, L–3 Communications Corporation	86
Charles Dabundo, Vice President and P–8 Poseidon Program Manager, Boeing Defense, Space and Security	90
Tab 1	129
Tab 2	130
Tab 3	131
Tab 4	133
Tab 5	135
Tab 6	137
Tab 7	138
Tab 8	140
Tab 9	141
Tab 10	145
Tab 11	146
Tab 12	147
Tab 13	151
Tab 14	155
Tab 15	156
Tab 16	159
Tab 17	174
Tab 18	175
Tab 19	176
Tab 20	180
Tab 21	184
Tab 22	185
Tab 23	191
Tab 24	195
Tab 25	196
Tab 26	199
Tab 27	201
Tab 28	202
Tab 29	203
Tab 30	205
Tab 31	209

THE COMMITTEE'S INVESTIGATION INTO COUNTERFEIT ELECTRONIC PARTS IN THE DEPARTMENT OF DEFENSE SUPPLY CHAIN

TUESDAY, NOVEMBER 8, 2011

U.S. SENATE,
COMMITTEE ON ARMED SERVICES,
Washington, DC.

The committee met, pursuant to notice, at 9:34 a.m. in room SD–G50, Dirksen Senate Office Building, Senator Carl Levin (chairman) presiding.

Committee members present: Senators Levin, Udall, Hagan, Manchin, McCain, Inhofe, Chambliss, Brown, Ayotte, and Collins.

Committee staff members present: Richard D. DeBobes, staff director; and Leah C. Brewer, nominations and hearings clerk.

Majority staff members present: Joseph M. Bryan, professional staff member; Ilona R. Cohen, counsel; Ozge Guzelsu, counsel; Richard W. Fieldhouse, professional staff member; and Peter K. Levine, general counsel.

Minority staff members present: David M. Morriss, minority staff director; Daniel A. Lerner, professional staff member; and Bryan D. Parker, minority investigative counsel.

Staff assistants present: Kathleen A. Kulenkampff, Brian F. Sebold, and Bradley S. Watson.

Committee members' assistants present: Casey Howard, assistant to Senator Udall; Roger Pena, assistant to Senator Hagan; Joanne McLaughlin, assistant to Senator Manchin; Jordan Baugh, assistant to Senator Gillibrand; Charles Prosch, assistant to Senator Brown; Brad Bowman and John Easton, assistants to Senator Ayotte; and Ryan Kaldahl, assistant to Senator Collins.

OPENING STATEMENT OF SENATOR CARL LEVIN, CHAIRMAN

Chairman LEVIN. Good morning, everybody. Today's hearing is a product of the Armed Services Committee's ongoing investigation into counterfeit electronic parts in the Department of Defense's (DOD) supply chain. We will probably hold at least one additional hearing to discuss what the Department is doing to keep counterfeit electronic parts out of defense systems.

We have three panels of witnesses today, so I expect that the hearing may continue into the afternoon, and I also expect that we will break for lunch. This will all be determined by how long these first two panels take. We also have a vote scheduled, I understand, for 12:15 which also could affect that decision.

I want to thank Senator McCain for his efforts in this investigation. I want to thank our staffs, the investigative staffs, for their very, very hard work.

The systems that we rely on for national security and the protection of our military men and women depend on the performance and reliability of small, highly sophisticated electronic components. Our fighter pilots rely on night vision systems enabled by transistors the size of paper clips to identify targets. Our troops depend on radios and Global Positioning Systems (GPS) devices and the microelectronics that make them work to stay in contact with their units and to get advance warning of threats that may be just around the next corner. The failure of a single electronic part could leave a soldier, sailor, airman, or marine vulnerable at the worst possible time. A flood of counterfeit electronic parts has made it a lot harder to have confidence that will not happen.

In some industries, the term "counterfeit" suggests an unauthorized fake, a knock-off of an original product. The definition of "counterfeit" as it relates to electronic parts, which has been endorsed by DOD and defense contractors alike, includes both fakes and previously used parts that are made to look new and are sold as new.

In March of this year, we announced an Armed Services Committee investigation into counterfeit parts in the DOD supply chain. During the course of the committee's investigation, virtually every one of the dozens of people our investigators have spoken with, from defense contractors to semiconductor manufacturers, to electronic component brokers—every one of them has pointed to China, specifically the City of Shenzhen in Guangdong Province as the primary source of counterfeit electronic parts.

While this hearing is focused mainly on the national security implications of counterfeit electronic parts, the rampant theft of U.S. Intellectual Property by Chinese counterfeiters also severely impacts our economic security. According to the Semiconductor Industry Association (SIA), U.S. semiconductor manufacturers employ nearly 200,000 American workers. Counterfeiting puts those jobs at risk and robs us of American jobs yet to be created. The SIA estimates that counterfeiting costs U.S. semiconductor manufacturers $7.5 billion a year in lost revenue and costs U.S. workers nearly 11,000 jobs.

This spring, we attempted to send Armed Services Committee staff to mainland China to get a firsthand look at the counterfeiting industry. I wrote the Chinese Ambassador to the United States informing him that the trip was part of the committee's official duties. Shortly after my letter, an official at the Chinese embassy told committee staff that if the results of the investigation were not positive, it could be "damaging to the U.S.-China relationship." That is exactly backwards. What is damaging to U.S.-China relations is China's refusal to act against brazen counterfeiting that is openly carried out in China.

In June, we sent our staff to Hong Kong where a visa is not required and the staff again sought entry into mainland China. But appeals on our behalf through our most senior diplomats in Hong Kong and Beijing fell on deaf ears and our staff was refused entry. That refusal only highlights the Chinese Government's total lack of

transparency and their unwillingness to act to stem the tide of dangerous counterfeits produced in China that are swamping the market.

Looking at just a slice of the defense contracting universe, committee staff asked a number of large defense contractors and some of their testing companies to identify cases in which they had found suspected counterfeit parts over a 2-year period. They reported 1,800 cases covering a total of 1 million individual parts. Of those 1,800 cases, we selected about 100 to track backwards through the supply chain. So where did the trails ultimately lead? The overwhelming majority, more than 70 percent, led to China, and with few exceptions, the rest came from known resale points for parts that came from China.

Counterfeit parts from China all too often end up in critical defense systems in the United States. China must shut down the counterfeiters that operate with impunity in their country. If China will not act promptly, then we should treat all electronic parts from China as suspect counterfeits. That would mean requiring inspections at our ports of all shipments of Chinese electronic parts to ensure that they are legitimate. The cost of these inspections would be borne by shippers, as is the case with other types of border inspections.

I want to describe now how these counterfeits are made and why they are so dangerous.

Much of the material used to make counterfeit electronic parts is electronic waste, e-waste, shipped from the United States and the rest of the world to China. E-waste is shipped into Chinese cities like Shantou in Guangdong Province where it is disassembled by hand, sometimes washed in dirty river water, and dried on city sidewalks. Once they have been washed, parts may be sanded down to remove the existing part number and other marks on the part that indicate its quality or performance. In a process known as "black topping," the tops of the parts may be recoated to hide sanding marks. State-of-the-art printing equipment is used to put false markings on the parts showing them to be new or of higher quality, faster speed, or able to withstand more extreme temperatures than those for which they were originally manufactured. When the process is complete, the parts are made to look brand new to the naked eye. Once they have been through the counterfeiting process, the parts are packaged and shipped to Shenzhen or other cities to be sold in the markets or to be sold on the Internet.

One of our witnesses today has described to the committee, "whole factories set up in China just for counterfeiting" and counterfeit electronic parts are sold openly from shops in Chinese markets.

This morning, we will hear from Richard Hillman of the U.S. Government Accountability Office (GAO), about just how pervasive the presence of China-based counterfeiters is online. Mr. Hillman will share the preliminary results of the investigative work that we asked him to undertake. GAO's stunning results not only point directly to China as the source of the counterfeiting problem, they show just how far the counterfeiters are willing to go for money. GAO investigators went out to buy electronic parts that go into defense systems and found that not only would companies supply

counterfeit parts when the GAO sought legitimate parts, suppliers also sold GAO investigators, acting undercover, parts that had nonexistent part numbers, part numbers that were made up from whole cloth by committee staff. All of those sellers that sent those parts with nonexistent numbers were in China.

Now, I am going to go through very quickly a presentation of how one of these counterfeit parts made its way through the defense supply chain. The SH–60B is a Navy helicopter that conducts anti-submarine and anti-surface warfare surveillance and targeting support. The SH–60B deploys on Navy cruisers, destroyers, and frigates and has a forward-looking infrared (FLIR) system, which provides night vision capability. The FLIR also contains a laser used for targeting the SH–60B's Hellfire missiles.

On September 8, 2011, the Raytheon Company sent a letter to the U.S. Naval Supply Systems Command alerting the Navy that electronic parts suspected to be counterfeit had been installed on three electromagnetic interference filters installed on FLIR units delivered by Raytheon. Raytheon only became aware of the suspect counterfeit, by the way, after being alerted by our committee's investigation. According to the Navy, the failure of an electromagnetic interference filter could cause the FLIR to fail. The Navy also told the committee that an SH–60B could not conduct surface warfare missions involving Hellfire missiles without a reliable, functioning FLIR. One of the FLIRs was sent to the USS *Gridley* in the Pacific fleet.

So how did a suspect counterfeit part end up in a night vision and targeting system intended for a Navy helicopter in the Pacific fleet? These filters were sold to Raytheon by a company called Texas Spectrum Electronics. This is the map we are showing you about the path of these counterfeit parts. That is a defense subcontractor in Texas. Those three FLIRs contain transistors that Texas Spectrum bought in 2010 from a company called Technology Conservation Group (TCG). TCG, it turns out, is both an electronics recycling company and an electronics distributor. The transistors at issue were mixed in among 72 pounds of miscellaneous excess inventory that a Massachusetts company called Thomson Broadcast sent to TCG as, "e-scrap." According to TCG, the parts arrived in what appeared to be the original packaging. So TCG sold the transistors as new and unused parts.

Now, where did Thompson Broadcasting get the parts? They bought them from a company called E-Warehouse in California, and E-Warehouse? They bought them from Pivotal Electronics, an electronics distributor in the UK. We asked Pivotal where they bought them and their answer was Huajie Electronics Limited in Shenzhen, China.

The C–27J is a military aircraft used for tactical support and to support combat operations. The U.S. Air Force has ordered 38 C–27Js, 11 of which have been delivered. Two C–27Js are currently deployed now in Afghanistan. The C–27J is equipped with display units that provide the pilot with information on the health of the airplane, including engine status, fuel use, location, and warning messages. The display units are manufactured by L–3 Display Systems, a division of L–3 Communications, and they are manufactured for Alenia Aeronautica. Alenia is a subcontractor to L–3 Inte-

grated Systems, another division of L–3 Communications and the military's prime contractor for the C–27J.

In November 2010, after a part failed on a fielded aircraft, and in internal testing L–3 Display Systems discovered that a memory chip used on its display unit was counterfeit. L–3 Display Systems had already installed the parts on more than 500 of its display units, including those intended for the C–27J, as well as the Air Force's C–130J and C–17 aircraft and the CH–46 used by the Marines. Failure of the memory chip could cause a display unit to show a degraded image, lose data, or even go blank altogether. But L–3 Integrated Systems, the prime contractor to the Air Force, did not notify its customer, the Air Force, that the C–27Js were affected by the part until September 2011, nearly a year after it had been discovered.

Where did these counterfeit chips come from? The supply chain is somewhat shorter in this case, but it started off in the same place. L–3 Display Systems bought the parts from Global IC Trading Group, an electronics distributor in California, which in turn bought the chips from Hong Dark Electronic Trade, a company in Shenzhen, China.

That is not the end of it. In total the committee discovered that Hong Dark supplied more than 28,000 electronic parts to divisions within L–3 Communications, and at least 14,000 of those parts have already been identified as suspect counterfeit. Neither the committee nor L–3 Communications knows whether the remaining 14,000 parts are authentic, and the company has not yet identified what military systems they might be in.

Another example. The P–8A Poseidon is a Boeing 737 airplane modified to incorporate anti-submarine and anti-surface warfare capabilities. Three P–8A flight test aircraft currently are in test at the Naval Air Station at Patuxent River, Maryland, and the Navy intends to purchase 108 of the aircraft from Boeing.

On August 17, 2011, Boeing sent a message marked, quote, priority critical to the P–8 program office. The message said that an ice detection module installed on one of the P–8 test aircraft contained a, "reworked part that should not have been put on the airplane originally and should be replaced immediately." The part at issue is critical to the functioning, in other words, of the P–8's ice detection module.

Boeing first identified a problem with the part in December 2009 when an ice detection module failed on the company's flight line. In that case, the part had literally fallen out of its socket and was found rattling around inside the module on the airplane. BAE Systems, which manufactures the ice detection system for Boeing, investigated the failure. They discovered that the part that had fallen out of the socket and dozens of other parts from the same lot were not new parts at all. Rather, they were previously used parts counterfeited to make them appear new. On closer inspection, BAE discovered that the parts had likely been sanded down and remarked. The leads on many parts were bent and marking on the parts were inconsistent. Parts that should have been virtually identical to one another were actually found to be of different sizes.

In January 2010, BAE notified Boeing of suspect counterfeit parts on a P–8, calling the counterfeit parts, "unacceptable for use,"

and recommending that they be replaced. BAE engineers believed their use created a long-term reliability risk. But it took Boeing more than a year and a half to notify the Navy or its other customers about the suspect counterfeit parts. Those notifications only came after our committee asked about them. Why it took so long for Boeing to notify its customers is something which we will discuss with Mr. Dabundo, the Program Manager for Boeing Defense, Space, and Security Systems P–8 Program Office who is a witness on our third panel.

The Navy recently wrote Boeing that, "the Government's position is that any counterfeit material received is nonconforming material and shall be immediately reported."

So where did the counterfeit parts come from in that case? BAE purchased around 300 of the parts from a company called Tandex Test Labs in California. Tandex bought the parts from a company called Abacus Technologies in Florida. Abacus, in turn, purchased the parts from an affiliate of A Access Electronics in Shenzhen, China, and wired payment for the parts to A Access's account at a bank in Shenzhen, China.

The three cases I just described are a drop in the bucket. There is a flood of counterfeits and it is putting our military men and women at risk and costing us a fortune. In terms of the cost, just one example, to the Government now.

In September 2010, the Missile Defense Agency (MDA) learned that mission computers for Terminal High Altitude Area Defense (THAAD) missiles contained suspect counterfeit memory devices. According to the MDA, if the devices had failed, the THAAD missile itself would likely have failed. The cost of that fix was nearly $2.7 million, and who paid for it? The American taxpayer.

We must change our acquisition rules to ensure that the cost of replacing suspect counterfeit parts is paid by the contractor, not the taxpayer. No ifs, no ands, no buts, and regardless of the type of contract involved.

So let us be clear, though. The risk is not created by the contractors. The risk stems from the brazen actions of the counterfeiters. Mr. Kamath of Raytheon, another one of our witnesses, told the committee that "what keeps us up at night is the dynamic nature of this threat because by the time we figured out how to test for these counterfeits, they have figured out how to get around it."

Now, some have argued that even if a counterfeit is not identified right away, that a contractor's testing process will weed out counterfeit parts. If a system containing a counterfeit part passes that testing, they argue, then the counterfeit part should work just like a new part. But that is not what the manufacturers of these parts tell us, and it is also not what our military leaders tell us.

We wrote to Xilinx, a large semiconductor manufacturer, about the anomalies that BAE had identified on the counterfeit parts that were intended for ice detection modules in that P–8A. Again, the parts were counterfeits of original Xilinx devices. This is what Xilinx told us. "These cases pose a significant reliability risk. Some of these could be catastrophic. Though the devices may initially function, it may be next to impossible to predict what amount of life is remaining or what damage may have been caused to the circuitry."

In those cases, when DOD or a contractor in the defense industry needs a spare electronic part to fix a 10- or 20-year-old system, there is a good chance that that part may no longer be available from its original manufacturer and there may be little choice but to go to the open market to find the replacement part. In other words, the parts that we buy are still supposed to be new even if they are no longer being manufactured.

Now, too few contractors and distributors consistently file reports with the Government-Industry Data Exchange Program (GIDEP), a DOD-run system that provides a forum for industry and Government to report suspect counterfeit parts and the suppliers who sold them. That has to change too. Failing to report suspect counterfeits and suspect suppliers puts everybody at risk. We need to make sure our regulations require contractors who discover suspected counterfeit parts in a military system to report that discovery to the military right away.

We will hear today from three panels of witnesses. Our first panel has three witnesses, now four witnesses I believe. Mr. Brian Toohey is President of SIA. Mr. Tom Sharpe is Vice President of SMT Corporation, an independent distributor of electronic components, as well as I believe Vice President of its affiliated test lab, Liberty Component Services, and Mr. Richard Hillman, the Managing Director, Forensic Audits and Investigative Service at GAO. Mr. Hillman is accompanied by the chief scientist for the GAO, Dr. Timothy Persons.

The witness on our second panel is Lieutenant General Patrick O'Reilly. General O'Reilly is the Director of MDA.

Our final panel has three witnesses: Mr. Vivek Kamath, the Vice President for Supply Chain Operations at Raytheon; Mr. Ralph DeNino, Vice President of Corporate Procurement at L–3 Communications; and Charles Dabundo, Vice President and P–8 Poseidon Program Manager for Boeing Defense, Space and Security Systems.

We appreciate the attendance of our witnesses this morning. By the way—and this is an important point—all of the companies and agencies represented here today have cooperated with the committee's investigation. We and the companies and the industry here, as well as, obviously, our troops and their families, are all on the same side of this battle. The only people who benefit from counterfeits are people who are making money off those counterfeits, and we have to end that.

We also have to end the attitude of the Chinese who will not cooperate with this investigation and who will not act against the counterfeiters. We wrote the Chinese Ambassador last week, invited him to send a representative to testify today, but he declined.

[The prepared statement of Senator Levin follows:]

PREPARED STATEMENT BY SENATOR CARL LEVIN

Today's hearing is a product of the Armed Services Committee's ongoing investigation into counterfeit electronic parts in the Department of Defense's (DOD) supply chain. We will probably hold at least one additional hearing to discuss what DOD is doing to keep counterfeit electronic parts out of defense systems. We have three panels of witnesses today so I expect the hearing to continue into the afternoon, and I also expect that we will break for lunch. I want to thank Sen. McCain for his efforts in this investigation, and to recognize the hard work of our investigative staff.

The systems we rely on for national security and the protection of our military men and women depend on the performance and reliability of small, highly sophisticated electronic components. Our fighter pilots rely on night vision systems, enabled by transistors the size of paper clips, to identify targets. Our troops depend on radios and global positioning systems devices, and the microelectronics that make them work, to stay in contact with their units and get advance warning of threats that may be just around the next corner. The failure of a single electronic part can leave a soldier, sailor, airman, or marine vulnerable at the worst possible time. A flood of counterfeit electronic parts has made it a lot harder to have confidence that won't happen.

In some industries, the term "counterfeit" suggests an unauthorized fake, a knock-off of an original product. The definition of counterfeit, as it relates to electronic parts, which has been endorsed by DOD and defense contractors alike includes both fakes and previously used parts that are made to look new, and are sold as new. Previously used parts sold as new parts present a significant risk because, while they may pass initial screening, they are far more likely than new parts to exhibit reliability and performance problems later on when deployed in the field.

In January 2010, the Department of Commerce Bureau of Industry and Security published a report entitled "Defense Industrial Base Assessment: Counterfeit Electronics." The report was the result of a survey of 387 companies and organizations in DOD's supply chain, including electronic parts manufacturers, distributors, assemblers, defense contractors, and the Department itself. The report highlighted "an "increasing number of counterfeit incidents being detected, rising from 3,868 incidents in 2005 to 9,356 incidents in 2008." The Commerce survey asked respondents to identify particular countries suspected or confirmed to be sources of counterfeits. China was identified nearly five times more often than any other country.

In March of this year, we announced an Armed Services Committee investigation into counterfeit parts in the DOD supply chain. During the course of the committee's investigation, virtually every one of the dozens of people our investigators have spoken with—from defense contractors to semiconductor manufacturers to electronic component brokers—has pointed to China, specifically the city of Shenzhen in Guangdong Province, as the primary source of counterfeit electronic parts.

U.S. Government reports also identify Shenzhen as the epicenter of the global trade in counterfeit electronic parts. In April 2011 the United States Trade Representative (USTR) issued its "Notorious Markets List," which identified the worst of the worst markets that sell counterfeit goods. The report stated that Shenzhen and Guangzhou, in Guangdong province, are "reportedly home to dozens of markets offering counterfeit or pirated goods." Also in April USTR issued its "Special 301" report reviewing the global state of intellectual property rights. In it, USTR said that China's manufacturing "extends to all phases of the production and global distribution of counterfeit goods." USTR stated point blank: "Many of these activities can be traced back to Guangdong Province."

While this hearing is focused mainly on the national security implications of counterfeit electronic parts, the rampant theft of U.S. intellectual property by Chinese counterfeiters also severely impacts our economic security. According to the Semiconductor Industry Association (SIA), U.S. semiconductor manufacturers employ nearly 200,000 American workers. Counterfeiting puts those jobs at risk and robs us of American jobs yet to be created. SIA estimates that counterfeiting costs U.S. semiconductor manufacturers $7.5 billion a year in lost revenue and costs U.S. workers nearly 11,000 jobs. But the Chinese government is obviously unwilling to take the necessary steps to shut the counterfeiters down. Raytheon's Vice President of Supply Chain Operations Vivek Kamath, one of our witnesses today, told us about his experience in China stating: "the amazing thing about [counterfeiting] is it's very open. There is nothing discreet about it. And it's just almost as if it's just accepted as another business model in the country."

This spring, we attempted to send Armed Services Committee staff to mainland China to get a first-hand look at the counterfeiting industry. I wrote the Chinese Ambassador to the United States, informing him that that the trip was part of the committee's official duties. Shortly after my letter, an official at the Chinese Embassy told committee staff that the issues we were investigating were "sensitive" and that if the results of the investigation were not positive, it could be "damaging" to the U.S.-China relationship. That's exactly backwards. What is damaging to U.S.-China relations is China's refusal to act against brazen counterfeiting that is openly carried out in that country.

In June, we sent our staff to Hong Kong, where a visa is not required, and the staff again sought entry into mainland China. But appeals on our behalf, through our most senior diplomats in Hong Kong and Beijing, fell on deaf ears and our staff was refused entry. That refusal only highlighted the Chinese Government's total

lack of transparency and unwillingness to act to stem the tide of dangerous counterfeits produced in China that is swamping the market.

In the course of the investigation, the committee staff scoured more than 100,000 pages of documents, including purchase orders and invoices, test reports and failure analyses identifying counterfeit parts. Staff met with and interviewed dozens of individuals, from defense officials, to manufacturers of electronic parts, to defense contractors and subcontractors, independent testing laboratories, and electronic parts distributors.

Looking at just a slice of the defense contracting universe, committee staff asked a number of large defense contractors and some of their testing companies to identify cases in which they had found suspected counterfeit parts over a 2-year period. They reported 1,800 cases, covering a total of 1 million individual parts. Of those 1,800 or so cases, we selected about 100 to track backwards through the supply chain. In some instances, the trail was a short one. In others, we chased parts across the country and around the world, as they changed hands from one parts broker to another. So where did those trails ultimately lead? The overwhelming majority—more than 70 percent—led to China. With few exceptions, the rest came from known resale points for parts from China, in Canada and the U.K.

Counterfeit parts from China all too often end up in critical defense systems in the United States. To cite a few examples, the investigation uncovered suspected counterfeit parts on thermal weapons sights delivered to the Army, on mission computers for the Missile Defense Agency's Terminal High Altitude Area Defense (THAAD) missile, and on military airplanes including the C–17, C–130J, C–27J, and P–8A as well as on AH–64, SH–60B, and CH–46 helicopters. Today's hearing will explore three cases where suspect counterfeit parts from China were installed on military systems manufactured by Raytheon, L–3 Communications, and Boeing, respectively. They and other contractors have been cooperative with the committee's investigation. They recognize the threat that counterfeit electronic parts pose to national security and to their businesses. While they need to do a better job knowing where their parts come from and notifying the military when there's a problem, the source of the counterfeit problem is China. China must shut down the counterfeiters that operate with impunity in their country. If China will not act promptly, then we should treat all electronic parts from China as suspected counterfeits. That would mean requiring inspections at our ports of all shipments of Chinese electronic parts to ensure that they are legitimate. The costs of these inspections would be borne by shippers, as is the case with other types of border inspections.

Before I talk about those three cases, I want to describe how these counterfeits are made and why they are so dangerous.

FROM THE SCRAP HEAP TO THE INTERNET—THE MAKING AND SELLING OF COUNTERFEITS

Much of the material used to make counterfeit electronic parts is electronic waste (e-waste) shipped from the United States and the rest of the world to China. In its January 2010 study, the Department of Commerce's said that e-waste has "turned into an abundance of discrete electronic components and microcircuits for counterfeit parts."

In fact, e-waste is shipped into Chinese cities like Shantou in Guangdong Province where it is disassembled by hand. Tom Sharpe, who is one of our witnesses today, visited Shantou's counterfeiting district, where he saw first-hand electronic debris stacked in huge mounds and piles of components that had been burned off of old circuit boards. He witnessed electronic parts being washed in a dirty river and dried on city sidewalks in Shantou.

Once they have been washed, parts may be sanded down to remove the existing part number, the date code (which tells you when a part was made), and other marks on the part that indicate its quality or performance. In a process known as "black topping," the tops of the parts may be recoated to hide sanding marks. State-of-the-art printing equipment is used to put false markings on the parts, showing them to be new, of higher quality, faster speed, or able to withstand more extreme temperatures than those for which they were originally manufactured. When the process is complete, the parts are made to look brand new to the naked eye.

Once they have been through the counterfeiting process, the parts are packaged and shipped to Shenzhen or other cities to be sold in the markets or on the Internet.

While the counterfeiting process for electronic parts is shocking to us, it is no secret in China. Mr. Kamath of Raytheon described "whole factories, set up [in China] just for counterfeiting" and counterfeit electronic parts are sold openly from shops in Chinese markets. But the counterfeiters' target is much bigger than a Shenzhen bazaar. The internet puts the entire world at their doorstep. In fact, there are doz-

ens of internet sites that specialize in the trade of electronic parts, with a large number of China-based distributors posting parts for sale. While some of them may be legitimate businesses, many others are nothing more than fronts for counterfeiters. This morning we will hear from Mr. Richard Hillman, the Managing Director, Forensic Audits and Investigative Service at the U.S. Government Accountability Office (GAO) about some of those front companies and just how pervasive the presence of China-based counterfeiters is online. Mr. Hillman will share the preliminary results of the investigative work that we asked him to undertake. GAO's stunning results not only point directly to China as the source of the counterfeiting problem, but show just how far the counterfeiters are willing to go for money. GAO investigators went out to buy electronic parts that go into defense systems, and found that not only would companies supply counterfeit parts when GAO sought legitimate parts. Suppliers also sold GAO investigators parts with nonexistent part numbers. And all of those sellers are in China.

I would now like to move to three cases where counterfeit electronic parts that the committee traced back to Chinese suppliers made their way into defense systems sold to the U.S. military.

SUSPECT COUNTERFEIT PARTS IN THE U.S. NAVY SH–60B HELICOPTER

I am now going to run through a presentation of how one of these counterfeit parts made its way through the defense supply chain. The SH–60B is a Navy helicopter that conducts anti-submarine and anti-surface warfare, surveillance and targeting support. The SH–60B deploys on Navy cruisers, destroyers, and frigates and has a Forward Looking InfraRed (FLIR) System which provides night vision capability. The FLIR also contains a laser used for targeting the SH–60B's hellfire missiles.

On September 8, 2011, the Raytheon Company sent a letter to the U.S. Naval Supply Systems Command alerting the Navy that electronic parts suspected to be counterfeit had been installed on three Electromagnetic Interference Filters (EIF) installed on FLIR units delivered by Raytheon. Raytheon only became aware of the suspect counterfeit after being alerted by the committee's investigation. According to the Navy, the failure of an EIF could cause the FLIR to fail. The Navy also told the committee that an SH–60B could not conduct surface warfare missions involving hellfire missiles without a reliable, functioning FLIR. A FLIR failure would also compromise the pilot's ability to avoid hazards and identify targets at night, limiting the SH–60Bs ability to be deployed in night missions. One of the FLIRs was sent to the USS *Gridley* in the Pacific Fleet.

So, how did a suspect counterfeit part end up in a night vision and targeting system intended for a Navy helicopter in the Pacific Fleet?

The Electromagnetic Interference Filters were sold to Raytheon by a company called Texas Spectrum Electronics, a defense subcontractor in Texas. Those three FLIRs contained transistors that Texas Spectrum bought in July 2010 from a company called Technology Conservation Group or TCG.

TCG, it turns out, is both an electronics recycling company and an electronics distributor. The transistors at issue were mixed in among 72 pounds of miscellaneous excess inventory that a Massachusetts company called Thomson Broadcast sent to TCG as "E-scrap." According to TCG, the parts arrived in what appeared to be the original packaging so TCG sold the transistors as "new" and unused parts. Incidentally, after TCG sold the parts to Texas Spectrum, it tried to sell other parts from the same lot to two other customers. Both prospective customers rejected the parts because of concerns about their condition. An independent testing laboratory hired by one of the two companies identified the parts as suspect counterfeits and notified TCG. TCG did not share that information with Texas Spectrum. In an October 25, 2011 letter, Fairchild Semiconductor, the manufacturer identified on the parts, informed the committee that it believes the TCG parts are "not Fairchild Semiconductor devices."

Where did Thompson Broadcasting get the parts? They bought them in April 2008 from a company called E-Warehouse in California. And E-Warehouse? They bought them from Pivotal Electronics, an electronics distributor in the UK. We asked Pivotal where they bought them. Their answer? Huajie Electronics Ltd. in Shenzhen, China.

SUSPECT COUNTERFEIT PARTS IN THE U.S. AIR FORCE C–27J

The C–27J is military aircraft used for tactical transport and to support combat operations. The U.S. Air Force has ordered 38 C–27Js, 11 of which have been delivered. Two C27Js are currently deployed in Afghanistan. The C–27J is equipped with display units that provide the pilot with information on the health of the airplane,

including engine status, fuel use, location, and warning messages. The display units are manufactured by L–3 Display Systems, a division of L–3 Communications, for Alenia Aeronautica. Alenia is a subcontractor to L–3 Integrated Systems, another division of L–3 Communications and the military's prime contractor for the C–27J.

In November 2010, L–3 Display Systems detected that their failure rate for a chip installed on display units had more than tripled, from 8.5 percent to 27 percent. L–3 Display Systems also noticed that the same part, which was failing in house, had also failed on a fielded military airplane in June 2010. The company sent the chip that failed on the plane and other samples from the lot for testing. That testing identified "multiple abnormalities" with the chips, including a blacktopped surface. The tester concluded they were "suspect counterfeit." Unfortunately, L–3 Display Systems had already installed parts from the suspect lot on more than 500 of its display units, including those intended for the C–27J, as well as the Air Force's C–130J and C–17 aircraft, and the CH–46, a helicopter used by the Marine Corps for assault support. Failure of the memory chip could cause a display unit to show a degraded image, lose data, or even go blank altogether—again, these displays provide the pilot with warning messages and other information on the health of the airplane.

L–3 Display Systems had learned of the counterfeit chip in November 2010 and informed their customer, Alenia, shortly thereafter. Despite being a division of the same company as L–3 Display Systems, which identified the counterfeit part, L–3 Integrated Systems, the prime contractor to the Air Force, told the committee that it only learned of the problem as a result of the committee's investigation. As a result, L–3 Integrated Systems did not notify the Air Force that the C–27Js were affected by the part until September 19, 2011—nearly a year after it had been discovered and just one day before committee staff was scheduled to meet with the Air Force's C–27J program office on the issue.

We will ask Ralph DeNino, L–3's Vice President for Corporate Procurement, who is a witness on our third panel, about breakdowns that led to the company's failure to provide timely notification to the government.

Where did the counterfeit chips come from? The supply chain is somewhat shorter in this case, but it started off the same place. L–3 Display Systems bought the parts from Global IC Trading Group, an electronics distributor in California, which in turn, bought the chips from Hong Dark Electronic Trade, a company in Shenzhen, China.

It turns out that the chips destined for the C27J, C130J and other aircraft was not the only lot of counterfeit parts that divisions of L–3 received from Hong Dark through Global IC. Hong Dark was also the source of another lot of counterfeit parts discovered by L–3 Display Systems in October 2009.

Moreover, a year ago, Global IC notified L–3 Display Systems that they had also supplied the company with a third lot of parts from Hong Dark, some of which were installed on display units intended for EA–6B military aircraft. L–3 submitted them for testing only a few weeks ago, after committee staff asked about them. The testing has since identified them as "suspect counterfeit."

But that's not even the end of it. In total, the committee discovered that Hong Dark made nearly 30 shipments in 2009 and 2010, totaling more than 28,000 electronic parts, to Global IC Trading Group, that were then sold divisions within L–3. At least 14,000 of those parts have already been identified as suspect counterfeit. Neither the committee nor L–3 knows whether the remaining 14,000 parts are authentic and L–3 has not yet identified what military systems they might be in.

SUSPECT COUNTERFEIT PARTS IN THE NAVY P–8A POSEIDON

The P–8A Poseidon is a Boeing 737 airplane modified to incorporate antisubmarine and anti-surface warfare capabilities. Three P–8A flight test aircraft currently are in test at the Naval Air Station at Patuxent River, Maryland and the Navy intends to purchase 108 of the aircraft from Boeing.

On August 17, 2011, Boeing sent a message marked "Priority: Critical" to the P–8 program office. The message said that an ice detection module installed on one of the P–8 test aircraft contained a "reworked part that should not have been put on the airplane originally and should be replaced immediately." The part at issue is critical to the functioning of the P–8's ice detection module.

Boeing first identified a problem with the part in December 2009 when an ice detection module failed on the company's flight line. In that case, the part had literally fallen out of its socket and was found rattling around inside the module on the airplane.

BAE Systems, which manufactures the ice detection system for Boeing, investigated the failure. They discovered that the part that had fallen out of the socket,

and dozens of other parts from the same lot, were not new parts at all. Rather, they were previously used parts counterfeited to make them appear new. On closer inspection, BAE discovered that the parts had likely been sanded down and remarked. The leads on many parts were bent and markings on the parts were inconsistent. Parts that should have been virtually identical to one another were actually found to be of different sizes. In January 2010, BAE notified Boeing of their findings, calling the counterfeit parts "unacceptable for use" and recommending they be replaced. BAE engineers believed their use created a long-term reliability risk.

It took Boeing more than a year and a half to notify the Navy or its other customers about the suspect counterfeit parts. Those notifications only came after the committee asked about them. Why it took so long for Boeing to notify its customers is something we will discuss with Mr. Dabundo, the Program Manager for Boeing Defense and Security Systems' P–8 Program office, who is a witness on our third panel. The Navy recently wrote Boeing that "The Government's position is that any 'counterfeit' material received . is nonconforming material and shall be immediately reported."

So where did the counterfeit parts come from? Over a period of several months from the fall of 2008 until the spring of 2009, BAE purchased around 300 of the parts from a company called Tandex Test Labs in California. BAE hired Tandex to source the parts and screen them for signs of counterfeiting. Tandex, it turns out, only screened the first 50. The company sent the remainder—around 250 parts—to BAE without inspecting them at all.

Tandex bought the parts from a company called Abacus Technologies in Florida. Abacus, in turn, purchased the parts from an affiliate of A Access Electronics in Shenzhen, China and wired payment for the parts to A Access's account at the Chartered Bank Shenzhen, China.

COUNTERFEIT PARTS ARE COSTING DOD AND THE DEFENSE INDUSTRY MILLIONS

The three cases I just described are a drop in the bucket. There is a flood of counterfeits and it is putting our military men and women at risk and costing us a fortune.

To cite just one example, in September 2010, the Missile Defense Agency learned that mission computers for THAAD missiles contained suspect counterfeit memory devices. According to MDA, if the devices had failed, the THAAD missile itself would likely have failed. The memory devices were purchased by Honeywell, a MDA subcontractor, from an independent distributor. Honeywell installed them on mission computers which it sold to Lockheed Martin. Lockheed, in turn, supplied them to MDA. To their credit, Honeywell and Lockheed notified MDA when they figured out the parts were suspect and put together a plan to fix the problem. But the cost of that fix was nearly $2.7 million. And who do you think paid for it? The American taxpayer. That's an area where we need reform. There is no reason on earth that the replacement of a counterfeit part should be paid for by American taxpayers, instead of by the contractor who put it in a military system. We must clarify our acquisition rules to ensure that the cost of replacing suspect counterfeit parts is paid by the contractor, not the taxpayer—no ifs, ands, or buts.

HOW COUNTERFEITS FIND THEIR WAY INTO DEFENSE SYSTEMS

One might ask, how do all these counterfeit parts make it through the system? The answer, in part, is that counterfeiters are shrewd, and they are getting shrewder. That is not only true about how they produce counterfeits but how they package and sell them. Sophisticated counterfeiters may mix counterfeit parts with authentic parts, in a method called "sprinkling," to increase the chance that the counterfeits will avoid detection. For example, some electronic components are purchased in reels. A counterfeiter might buy a reel of good parts, cut that reel up, and splice authentic parts into the beginning, middle, and end of several reels of counterfeit parts. The counterfeiters know that companies often test components from the beginning, middle and end of a reel to validate the authenticity of the entire reel.

In the case of L–3's counterfeit memory chip, the suppliers in China selected and sent the distributor a sample of 18 parts to test. Once those few parts were tested and validated as authentic, the supplier sold another 10,000 of those memory chips for use by L–3. L–3's process at the time allowed the company to accept the chips without additional testing.

It is a constant battle to stay ahead of the counterfeiters. Mr. Sharpe, the Vice President of an independent test laboratory and one of our witnesses today, is confronted every day with new counterfeiting techniques. Mr. Kamath of Raytheon, another one of our witnesses, told the committee that "what keeps us up at night is

the dynamic nature of this threat because by the time we've figured out how to test for these counterfeits, they've figured out how to get around it. And it's literally on almost a daily basis they change and the sophistication of the counterfeiting is amazing to us. We're finding that you have to go down to the microns to be able to figure out that [a part is] actually a counterfeit."

Some have argued that, even if a counterfeit is not identified right away, a contractor's testing process—where systems may be subjected to heat, vibration and other stresses—will weed out counterfeit parts. If a system containing a counterfeit part passes that testing, they argue, then the counterfeit part should work just like a new part.

The Boeing Service Engineer responsible for determining the company's handling of counterfeit parts on the P–8 told the committee that "[m]any used parts tend to have the same reliability as a new part." And the Chief Engineer for L–3 Integrated Systems' C–27J program stated that L–3's process for testing its systems "would show whether [a part in an L–3 system] was functional or not."

But that's not what the manufacturers of these parts tell us. And it is also not what our military experts say either.

We wrote to Samsung, the manufacturer of the original parts that were counterfeited on the L–3 display units, to ask them about the reliability and performance risks associated with using parts with the identified anomalies. Samsung said simply, "one cannot expect such parts to function properly, or at all."

We wrote to Xilinx, a large semiconductor manufacturer, about the anomalies that BAE had identified on the counterfeit parts that were intended for the ice detection modules in the P–8A. (The parts were counterfeits of original Xilinx devices.) Listen to what Xilinx told us:

The devices may have been reclaimed and potentially exposed to excessive heat in order to dismount them from a circuit board. These cases pose a significant reliability risk. there are many potential damage mechanisms that could have affected the devices. Some of these could be catastrophic; others may create a damage mechanism that is latent for an undetermined amount of time. Though the devices may initially function, it would be next to impossible to predict what amount of life is remaining, or what damage may have been caused to the circuitry.

As to the belief that parts in a system which pass a contractor's acceptance testing should work just fine, here's what the Director of the Missile Defense Agency, General Patrick O'Reilly told the committee:

A counterfeit part may pass all production testing. However, it is possible that the part was damaged during unauthorized processing (e.g., removing the part from a previous assembly, or sanding the surface in order to place a new part number) causing the deployed system to fail. Similarly, reliability may be affected because a counterfeit part may be near the end of its useful life when it is installed. Should any mission critical component fail, that system fails and national security is impacted.

That is a risk we cannot tolerate. General O'Reilly will be testifying today.

WHY DOD IS VULNERABLE TO COUNTERFEITS

Given the risk, one might ask, why are we buying parts for defense systems from Hong Dark Electronic Trade, Huajie Electronics and other Chinese companies? Why don't we buy our parts from Intel and Freescale and Texas Instruments?

Part of the reason is that when an electronic part is no longer economical to produce due to declining demand, manufacturers stop making it. In many cases, the demand from the defense industry just is not enough to keep a manufacturing line up and running. Ted Glum, who is the Director of DOD's Microelectronics Activity Unit, the government's official authority on this issue, put it this way: "The defense community is critically reliant on a technology that obsoletes itself every 18 months, is made in unsecure locations and over which we have absolutely no market share influence." An electronic part may be manufactured for 18 months, while the defense systems it is used on may be in service for 18 years—or longer.

In those cases when DOD or a contractor in the defense industry needs a spare electronic part to fix a 10- or 20-year-old system, there is a good chance that part may be obsolete and there may be little choice but to go to the open market to find the replacement part. But the parts we buy are still supposed to be new, they are just obsolete. The open market is where the risk is the highest. That is also where DOD and its contractors must be most vigilant. Defense contractors and DOD simply have to do a better job finding out where their parts come from and in validating the authenticity of parts not sourced from the original manufacturer or a franchised distributor. But we must also confront the issue of counterfeit parts from China

head-on. As I stated earlier, if China does not act against the counterfeiters then we will have no choice but to treat all electronic parts from China as suspect.

THE IMPORTANCE OF TRANSPARENCY

Another place where the defense industry is coming up short is in reporting cases of counterfeit parts. Our investigation uncovered approximately 1,800 cases where parts suspected to be counterfeits have been identified by companies in the defense supply chain. However, the vast majority of those cases appear to have gone unreported to DOD or criminal authorities. In addition, too few contractors and distributors consistently file reports with the Government Industry Data Exchange Program (GIDEP), a DOD-run system that provides a forum for industry and government to report suspect counterfeit parts and the suppliers who sold them. That has to change. Failing to report suspect counterfeits and suspect suppliers puts everyone at risk. We need to make sure our regulations require contractors who discover suspected counterfeit parts in a military system to report that discovery to the military right away. We should also require DOD and contractors to report cases of suspected counterfeits found in the supply chain into GIDEP, so that others are alerted.

On September 30, 2011, the U.S. Attorney for the District of Columbia submitted a filing to the U.S. District Court relating to the sentencing of the former Administrative Manager of VisionTech Components. Between 2006 and 2010, VisionTech sold counterfeit electronic components, imported from China, to more than 1,000 buyers in the United States and abroad. Among those customers were several major defense contractors. There are other VisionTechs out there and we cannot afford to let them operate with impunity.

WITNESSES

We will hear from three panels of witnesses today. Our first panel has three witnesses: Mr. Brian Toohey is the President of the Semiconductor Industry Association; Mr. Tom Sharpe is the Vice President of SMT Corporation, an independent distributor of electronic components, and its affiliated test lab, Liberty Component Services; and Mr. Richard Hillman, the Managing Director, Forensic Audits and Investigative Service at the U.S. Government Accountability Office (GAO). Mr. Hillman is accompanied by the Chief Scientist for GAO, Mr. Timothy Persons. The witness on our second panel is Lieutenant General Patrick O'Reilly. General O'Reilly is the Director of the Missile Defense Agency. Our final panel has three witnesses: Mr. Vivek Kamath, the Vice President for Supply Chain Operations at Raytheon Company; Mr. Ralph DeNino, Vice President of Corporate Procurement at L–3 Communications; and Mr. Charles Dabundo, Vice President and P–8 Poseidon Program Manager for Boeing Defense, Space & Security Systems.

We appreciate the attendance of our witnesses this morning. All of the companies and agencies represented here today have cooperated with the committee's investigation. Last week, we wrote the Chinese Ambassador and invited him to send a representative to testify today, but he declined.

Chairman LEVIN. Again, with my thanks, Senator McCain.

STATEMENT OF SENATOR JOHN MCCAIN

Senator MCCAIN. Thank you, Mr. Chairman, and I thank the witnesses for being here.

We are talking about an issue that is a risk to national security. These counterfeit electronic parts in our supply chain result, as we all know, in reduced reliability, availability, and frankly our ability to defend this Nation's national security interests.

As the chairman has pointed out, much of the raw material for counterfeit electronic parts is salvaged electronic waste, e-waste, shipped from the United States and other countries to China where old computers and other electronic products are disassembled by hand. There is an article in Business Week magazine entitled "Dangerous Fakes," which I would like to quote from. It says, much of that pollution emanates from the Chinese hinterlands. Business Week tracked counterfeit military components used in gear made by BAE Systems to traders in Shenzhen, China. The traders typically obtain supplies from recycled chip emporiums such as the

Guiyu Electronics Market outside the City of Shantou in southeastern China. The garbage-strewn streets of Guiyu reek of burning plastic as workers in back rooms and open yards strip chips from old PC circuit boards. The components, typically less than an inch long, are cleaned in the nearby Lianjiang River and then sold from the cramped premises of businesses such as the Jinlong Electronics Trade Center.

A sign for Jinlong Electronics advertises in Chinese that it sells, quote, military circuitry, meaning chips that are more durable than commercial components and able to function at extreme temperatures. But proprietor Lu Weilong admits that his wares are counterfeit. His employees sand off the markings on used commercial chips and relabel them as military. Everyone in Guiyu does this, he says. The dates on the chips are 100 percent fake because the products pulled off the computer boards are from the 1980s and 1990s, while customers demand products from after 2000.

The chairman has described the situation in detail, and I will not go on at length because we need to hear from the witnesses. But this is a serious issue. The Chinese Government can stop it. If the Chinese Government does not stop it, then it continues to pose a national security risk.

There are other problems associated with that which the chairman has outlined about how defense contractors are often forced to purchase parts from independent distributors or brokers who may stock or have access to obsolete parts. There is risk, which I hope the witnesses will explore a little bit, in obtaining parts in the "independent market." We know that some of these people that are advertised as small business people are simply conduits with a phone and a desk for some of these parts. The chairman outlined the various layers and places that these parts go through. We have to address that side of the issue. We all want the small business people to be able to obtain DOD contracts, but not the kind of abuse that apparently also is practiced here.

I want to thank you, Mr. Chairman, and the staff for their many hours of long, hard work. I look forward to hearing from the witnesses. Thank you, Mr. Chairman.

Chairman LEVIN. Thank you, Senator McCain.

Let us start with Mr. Sharpe. Ordinarily we probably would call on the GAO witness first, but I think today we are going to start with the problem and kind of a very vivid description of the problem, and then, Mr. Hillman, you can give us the GAO investigation here that you undertook. So we are going to start, though, with Mr. Sharpe.

STATEMENT OF THOMAS R. SHARPE, VICE PRESIDENT, SMT CORPORATION AND LIBERTY COMPONENT SERVICES

Mr. SHARPE. Mr. Chairman, Senator McCain, and members of this committee, first I want to thank you for allowing me to come in and provide this testimony.

The issues with counterfeit parts in DOD is a big problem, obviously, and it is a big focus of our job at SMT Corporation. My company's job is to authenticate, source, and supply parts to the defense and aerospace industry. We take this quite seriously.

I will explain to you what exactly I saw while I was in the City of Shenzhen and then into the City of Shantou, as well as some of the counterfeits that we are seeing out there today.

In July 2008, I had an opportunity, while traveling into the City of Hong Kong on business, to go into the nearby City of Shenzhen. The reason why I wanted to go in was to visit the marketplace that has been mentioned here. The photos are up there on the screen. I had an interpreter go with me. We walked through the marketplace for the day. While I was touring the marketplace, the interpreter told me that the marketplace district was the largest in the world of its kind, that 30 to 40 percent of all parts sold here were counterfeit, that many of the booths that we passed were owned by counterfeiters who owned off-site locations that actually did the counterfeiting and brought the product into the marketplace to sell, that the local brokers and manufacturers shop here openly to receive the 70 percent cost savings on buying parts that are counterfeit as opposed to buying brand new parts, knowing full well that the fall-out on these parts is up to 15 percent will not work.

Products sold to brokers outside of China are represented to be "new and unused at the time that they are sold," into the United States and elsewhere.

Also, that most of the component counterfeiting was performed in the nearby City of Shantou. Now, I had never heard of Shantou prior to going to Shenzhen. So this was new to me.

The next morning, we traveled to Shantou. We spent the day touring this area, and we visited select businesses that were known to the driver that was with us. While there, I witnessed e-scrap piled outside of buildings throughout large areas of the town, throughout the outskirts of the town, used electronic parts being washed in a river, and laid on the riverbank to dry, nylon sacks with harvested components being dumped onto sidewalks and sorted by women and children, laid out there for the monsoon rains of July to wash them naturally, cardboard and plastic bins filled with expensive brand name components and harvested from scrap printed circuit boards ready for processing. The actual counterfeiting process of electronic components actually taking place while I was there within some of the buildings. A wide variety of counterfeit parts for sale within the counterfeiting facility sales areas. So materials that come from most manufacturers that we know of for sale. Overall, a huge infrastructure of similar or supporting businesses in and around Shantou for harvesting components from e-scrap and processing into counterfeit electronic parts.

It is interesting to note that counterfeiting performed in Shantou, from speaking to the people there, was not regarded as intellectual property theft or wrong in any way whatsoever. It was seen more as a positive green initiative for the repurposing and reuse of perfectly good used product.

In the past several years, SMT has identified and documented several new counterfeit processes and threats specifically designed to evade the current inspection processes known to be in use by our industry at the time. These include a new surface recoating material that is immune to acetone surface-permanency tests that has a surface that looks just like the manufacturer's top coat. SMT released this to DOD and prime contractors in August 2009. A proc-

ess to remove manufacturer part markings without requiring surface recoatings. We released this to DOD and primes in June 2011. A process to remove and recondition the top surfaces of ceramic components which was released just yesterday to DOD, prime contractors, and others.

The counterfeiters are most certainly monitoring our level of detection expertise and quickly evolving newer processes to introduce into the global supply chains. Many of the current counterfeit techniques are already beyond the in-house capabilities of most open-market suppliers.

Over the last several years, the defense and aerospace industry has made steady progress in laying the foundational groundwork for an effective counterfeit avoidance plan. We hope to begin to see the fruits of this labor in 2012.

Lastly, I personally believe that the work of this committee is playing a significant role in the industry transformation needed to effectively mitigate the counterfeit threat within DOD.

Thank you.

[The prepared statement of Mr. Sharpe follows:]

PREPARED STATEMENT BY THOMAS SHARPE

Mr. Chairman, Senator McCain, and members of this committee, I am honored to have been requested to provide testimony on the counterfeit issue and its effect on the supply-chain of the Department of Defense (DOD).

My company, SMT Corporation, is an independent stocking distributor of board-level electronic components. We specialize in the sourcing, authentication testing and supply of obsolete components to the Defense & Aerospace Industry.

CITY OF SHENZHEN, GUANGDONG PROVIDENCE CHINA

In July 2008, while on business in Hong Kong, I had made it a point to visit the Electronic component marketplace in the nearby city of Shenzhen China.

While touring the Shenzhen marketplace with a local interpreter I was told:

(1) The electronic marketplace district was the largest wholesale component distribution area of its type in the world.
(2) 30–40 percent of all broker-sold products at this marketplace are counterfeit.
(3) Many of the booths we passed contained companies that own counterfeiting operations elsewhere within China.
(4) Local brokers and manufacturers purposely buy counterfeits for a 70 percent savings off authentic component prices—fully aware that up to 15 percent may not function at all.
(5) Products sold to brokers outside of China are represented to be new, original factory product at time of sale.
(6) Most component counterfeiting was performed in the nearby city of Shantou.

CITY OF SHANTOU, GUANGDONG PROVIDENCE CHINA

The next morning we traveled to Shantou and spent the day touring the area and visiting selected businesses known to the driver.

While in Shantou I witnessed:

(1) E-scrap piled outside buildings throughout large areas of the town.
(2) Used electronic components being washed in a river and dried on the riverbank.
(3) Nylon sacks filled with harvested components being dumped onto sidewalks, sorted and naturally washed in the daily monsoon rains.
(4) Piles of sorted scrap circuit boards that supposedly had just arrived from the United States.
(5) Cardboard and plastic bins filled with expensive brand-name components harvested from scrap PCBs ready for processing.
(6) The actual counterfeit processing of electronic components taking place.
(7) A wide variety of counterfeit parts for sale within the counterfeiting facility sales area.

(8) A huge infrastructure of similar or supporting businesses in and around Shantou for harvesting components from e-scrap and processing into counterfeit electronic parts.

Counterfeiting performed in Shantou was not regarded as intellectual property theft or improper in any way. It was seen more as a positive "green initiative" for the repurposing of discarded electronic component material.

COUNTERFEIT PROCESSES ARE CONSTANTLY EVOLVING TO EVADE DETECTION

In the past several years SMT has identified and documented many new counterfeit process threats specifically designed to evade the current inspection processes known to be in use by our industry at the time.

These include:

(1) A new surface recoating material that is immune to acetone surface-permanency tests. (released by SMT in August 2009)
(2) A process to remove manufacturer part markings without requiring surface recoatings. (released by SMT in June 2011)
(3) A process to remove and recondition the top surfaces of ceramic components. (released by SMT in November 2011)

The counterfeiters are most certainly monitoring our level of detection expertise and quickly evolving newer processes to introduce into the global supply chains. Many of the current counterfeiting techniques are already beyond the in-house detection capabilities of most open-market suppliers.

MUCH IS BEING ACCOMPLISHED ON THE COUNTERFEIT THREAT

Over the last several years the Defense & Aerospace Industry has made steady progress in laying the foundational ground-work for an effective counterfeit avoidance plan. We will begin to see the fruits of this labor in 2012.

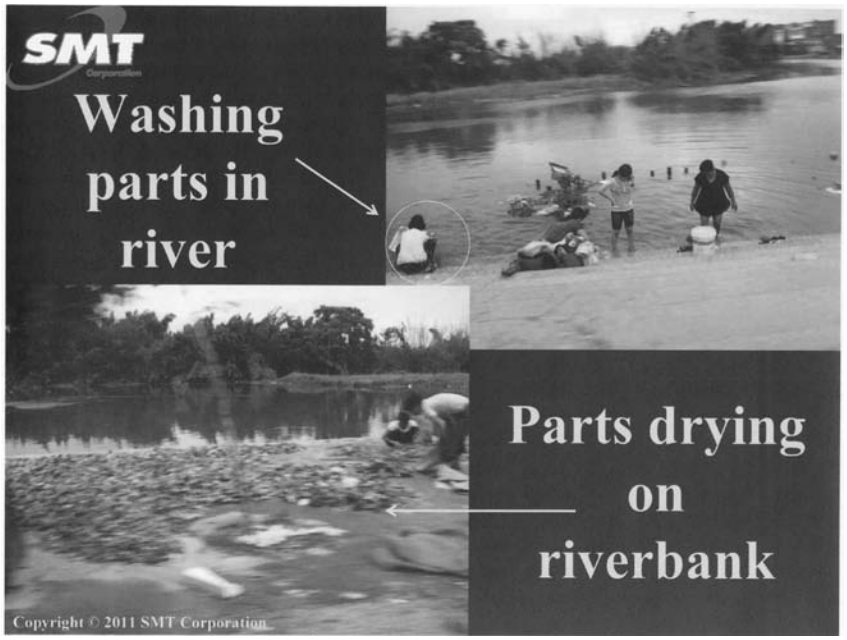
(1) New quality standards have been released and/or nearing release which focus on counterfeit mitigation: (Much thanks and recognition go to NASA and JPL for these—among many others as well.)
    a. AS5553—Counterfeit avoidance standard for manufacturers.
    b. AS6081—Counterfeit avoidance standard for distributors.
    c. AS6171—Test methods standard for the identification of counterfeit electronic parts.
(2) There have been very significant test and inspection additions to counterfeit mitigation flow-down requirements from the Defense contractors to open-market suppliers.
(3) The total approved vendor list (AVL) of open-market suppliers to Defense contractors has been/is being reduced to three or four total in all cases I am aware of. This small group of extensively audited suppliers must meet stringent customer requirements that include:
    a. Significant counterfeit mitigation capability and quality processes
    b. Certification to Aerospace & Industry standards
    c. Performance, training and constant improvement metrics
    d. Fair pricing and on-time delivery track records
    e. Product "pedigree" documentation supplied in all cases possible
    f. Documented proof of supplier due-diligence to perform quality and authentication test flow-down requirements from contractors
(4) In the past year, I have seen significant effort on the part of the component manufacturers to provide component authentication help to government agencies for the purpose of counterfeit detection.

IMPORTANT TOOLS NEEDED FROM GOVERNMENT TO HELP FIGHT COUNTERFEITS

(1) Federal funding for the creation and ongoing concern of a "Counterfeit Repository" where suspect-counterfeit components can be sent for final authenticity determination, disposition to intellectual property holders or Federal law enforcement agencies.
(2) In an effort to curtail the export of e-scrap material containing PCBs which become the counterfeiter's feedstock, legislation must be passed banning the export of this material. This legislation should require the complete destruction and green-processing of PCB scrap within the United States only.
(3) Provide significant funding for new PCB designs within DOD systems in an effort to reduce obsolescence issues and the need to procure open-market product from non-authorized sources when maintaining older electronic systems.

I personally believe the work of this committee is playing a significant role in the industry transformation needed to effectively mitigate the counterfeit threat within the DOD.

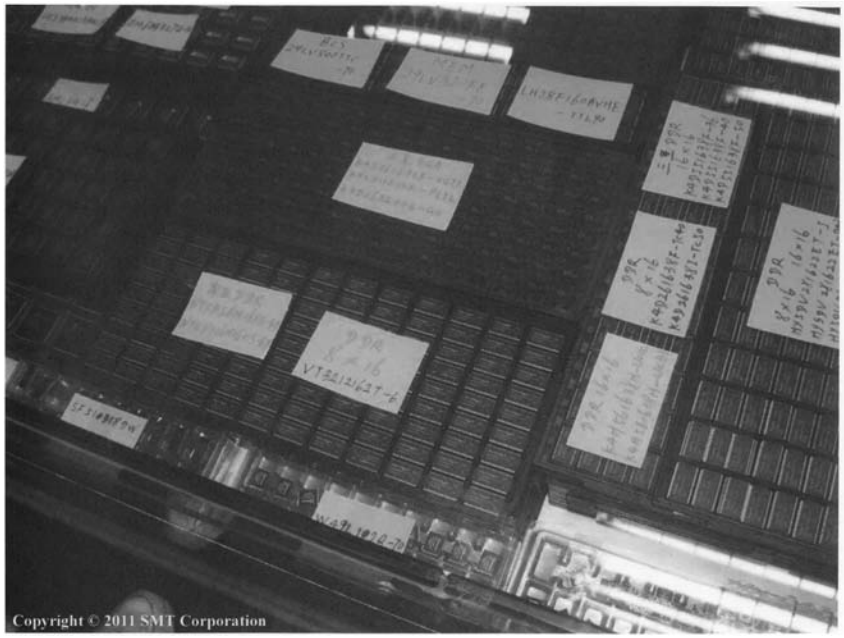
Copyright © 2011 SMT Corporation

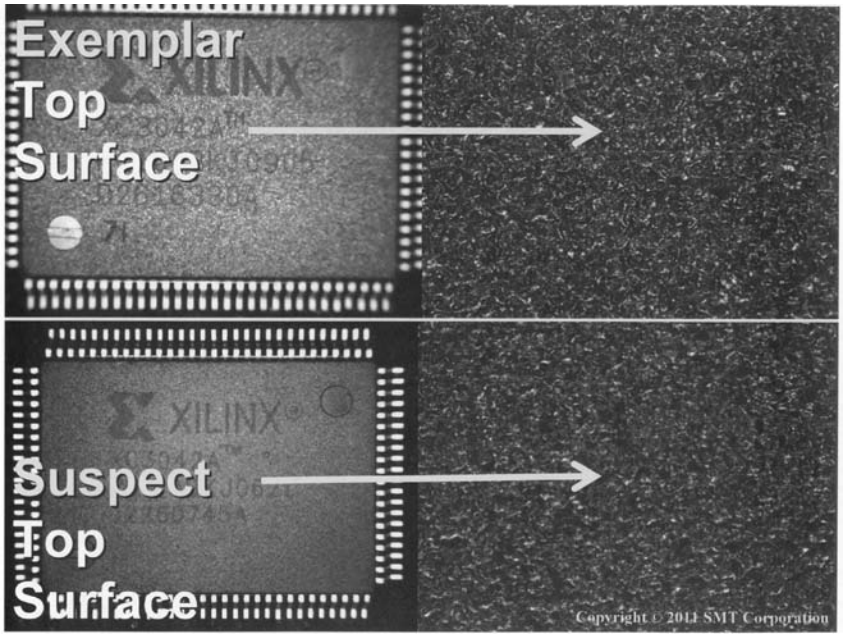

SMT
Washing parts in river
Parts drying on riverbank
Copyright © 2011 SMT Corporation

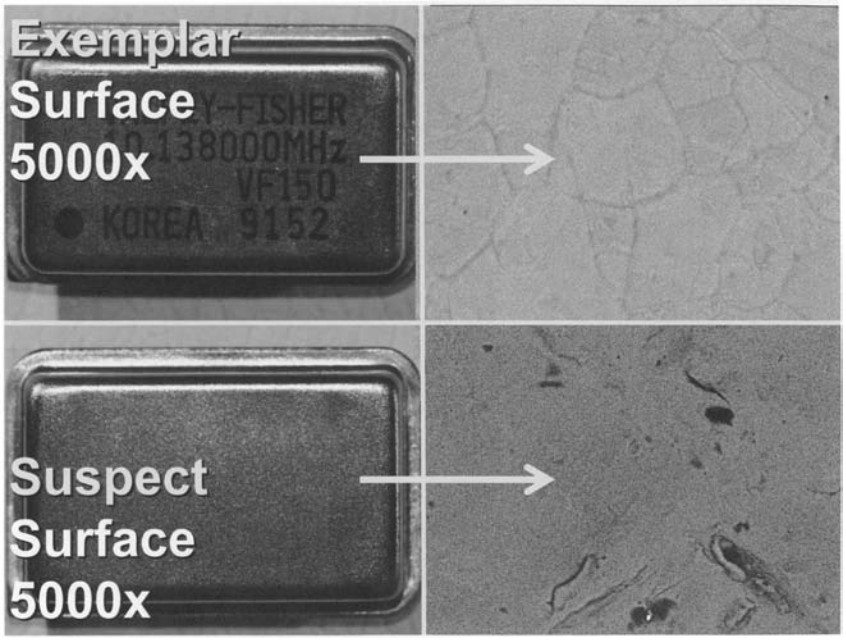
Cost 0.25¢
new
Copyright © 2011 SMT Corporation

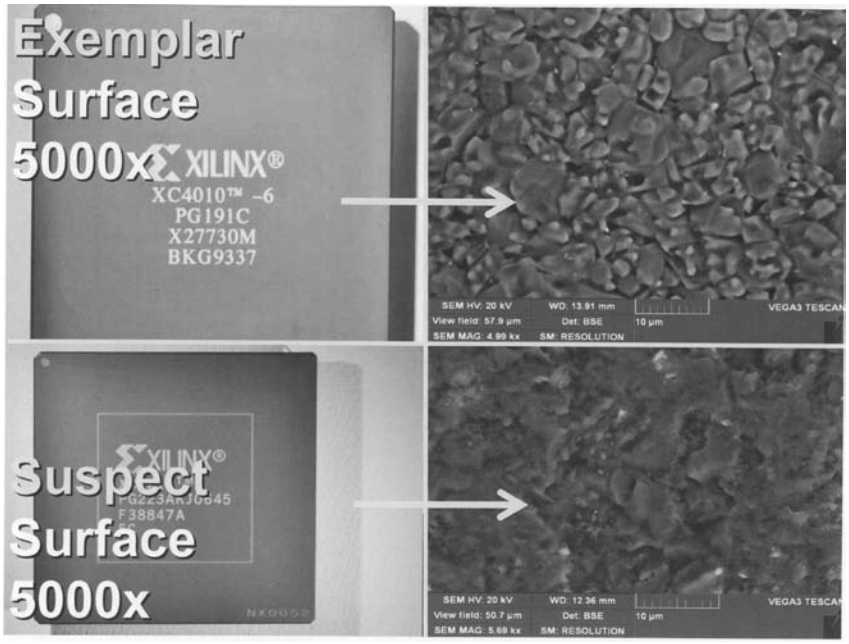
SMT
E-Waste
feedstock
for counterfeits
Copyright © 2011 SMT Corporation

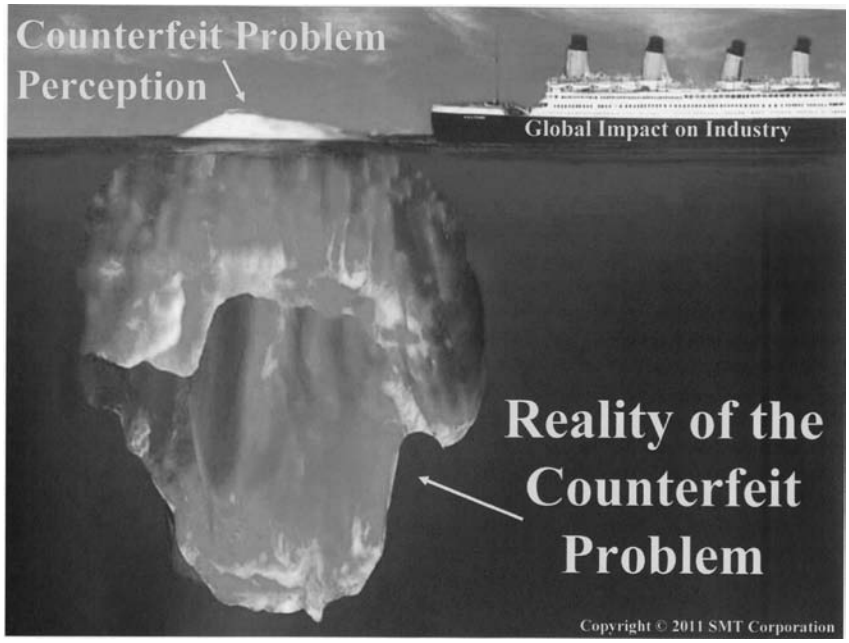
Copyright © 2011 SMT Corporation


Copyright © 2011 SMT Corporation


Exemplar
Top
Surface
XILINX
Suspect
Top
Surface
XILINX
Copyright © 2013 SMT Corporation


Exemplar
Surface
5000x
Y-FISHER
0.138000MHz
VF150
KOREA 9152
Suspect
Surface
5000x





Chairman LEVIN. Thank you very much, Mr. Sharpe. Your entire statement, if you did not give it, will be made part of the record, and that would be true with all the statements of all of our wit-

nesses because we know in some cases they are reducing the length of that statement for time purposes.

Mr. Hillman.

STATEMENT OF RICHARD J. HILLMAN, MANAGING DIRECTOR, FORENSIC AUDITS AND INVESTIGATIVE SERVICE, GOVERNMENT ACCOUNTABILITY OFFICE; ACCOMPANIED BY DR. TIMOTHY PERSONS, CHIEF SCIENTIST, CENTER FOR SCIENCE, TECHNOLOGY, AND ENGINEERING, GOVERNMENT ACCOUNTABILITY OFFICE

Mr. HILLMAN. Chairman Levin, Ranking Member McCain, and members of the committee, thank you for the opportunity to discuss the preliminary observations of our ongoing investigation into the availability of counterfeit parts on Internet trading platforms.

Counterfeit parts have the potential to seriously disrupt DOD supply chain, affect the integrity of weapons systems, and ultimately endanger the safety of our military personnel.

This committee cited concerns about the availability of counterfeit parts on Internet platforms and asked us to purchase certain electronic parts and have their authenticity tested. I would like to briefly summarize how we are conducting this ongoing investigation and our results to date.

In conducting this work, we created a fictitious company to gain access to Internet platforms that sell military-grade electronic parts. Our company included a fictitious owner and employees, mailing and e-mailing addresses, a Web site, and a listing on the central contractor registration. We attempted to purchase membership to three Internet platforms that were of interest to this committee and were granted membership to two platforms.

We then requested quotes from vendors on both platforms to purchase a total of 13 parts from a list of parts this committee provided that fell into one of three categories: one, authentic part numbers for obsolete and rare parts; two, authentic part numbers with post-production date codes or date codes after the last date the part was manufactured; and three, bogus part numbers.

We independently verified with the Defense Logistics Agency (DLA) that the authentic part numbers were used for military applications. We also confirmed with DLA and selected part manufacturers that the bogus part numbers were not associated with actual parts. We requested parts from vendors that were new in original packaging, not refurbished, and not with mixed date codes. We selected the first vendor amongst those offering the lowest prices that provided enough information such as name, addresses, and payment method to make a purchase. We then contracted with SMT Corporation for component authentication analyses of the parts that we received. We are not disclosing the names of the Internet trading platforms we are using and we altered all part numbers in this testimony due to the ongoing nature of our investigation.

Regarding our preliminary results, as shown in figure 1 of my prepared statement, as of today we have purchased 13 parts, and none of the seven parts we have complete test results for are authentic. Specifically, according to SMT Corp., all three parts tested, after we requested legitimate but rare or obsolete parts, failed at least three of seven authentication analyses and were suspected

counterfeits. These parts included two voltage regulators and one operational amplifier, the failure of which could pose risk to the functioning of the electronic systems where the parts reside.

SMT Corp. also made the same determination for another operational amplifier we received after requesting a legitimate part number with a post-production date code. In this instance, the part failed four of seven authentication analyses and the vendor also misrepresented the part as 9 years newer than the date it was last produced.

In addition, we received three bogus parts after submitting orders using invalid part numbers. Because no legitimate parts in this final category exist, we did not send them for authentication testing.

We are also awaiting testing results on two additional parts and have not yet received another four purchases. We will report the results for these and additional parts we plan to purchase in a future product.

While we sent requests to both domestic and international companies, all of the parts we have purchased and received to date were provided by vendors in China. More specifically, all four of the parts that SMT Corp. tested were suspected counterfeits. The parts were subject to a component authentication analysis which included visual, chemical, x-ray, and microscopic testing. Figures 2 and 3 on pages 6 and 10 of my prepared statement provide photos and detailed test results for each part. Overall, each was a suspect counterfeit because the results of the tests indicated that the parts were likely used parts that were harvested from older equipment and then altered to appear as new.

For example, SMT Corp. found that some parts were found to have scratches similar to suspect counterfeit devices that had been remarked and confirmed by both visual inspection and scanning electronic microscopic analysis. Tooling marks were also found on the bottom of some components suggesting the components were pulled from a working environment. Further testing between the top and bottom of leads revealed inconsistencies in chemical composition, leading SMT Corp. to conclude that the leads were extended with the intention to deceive. Microscopic inspection also revealed that different revision numbers of the die and differences in various die markings were found in some parts even though the samples were advertised to be from the same part number and production date. Commonly components manufactured with the same date and lot code have the same die revisions.

Finally, the manufacturer of certain parts confirmed their end-of-life designation leading SMT Corp. to conclude that certain parts were misrepresented as being newer than the actual parts could possibly be.

As previously stated, as of today, we have also received three bogus parts after submitting requests using invalid part numbers. The fact that vendors fulfilled our requests indicate that they were willing to sell parts stamped with nonexistent part numbers essentially taking money in exchange for bogus parts. Figure 4 of my prepared statement provides photos of the fictitious parts we received to date.

In conclusion, preliminary observations from our ongoing investigation indicate that counterfeit electronic parts can be found on Internet purchasing platforms.

I will be pleased to report to you the full results of our work once our investigation is complete.

I would also like to extend my appreciation to the entire investigation team for their dedication and commitment in delivering this interim report. With the combined assistance of investigators, analysts, and methodologists, we are pleased to provide these investigative services to Congress.

Chairman Levin and Ranking Member McCain and members of the committee, this concludes my prepared remarks and I would be happy to respond to any questions you may have.

[The prepared statement of Mr. Hillman follows:]

PREPARED STATEMENT BY RICHARD J. HILLMAN

Chairman Levin, Ranking Member McCain, and members of the committee:

Thank you for the opportunity to discuss the preliminary observations of our ongoing investigation into the availability of counterfeit military-grade electronic parts on Internet purchasing platforms. Counterfeit parts—generally those whose sources knowingly misrepresent the parts' identity or pedigree—have the potential to seriously disrupt the Department of Defense (DOD) supply chain, delay missions, affect the integrity of weapon systems, and ultimately endanger the lives of our troops. Almost anything is at risk of being counterfeited, from fasteners used on aircraft to electronics used on missile guidance systems. There can be many sources of counterfeit parts as DOD draws from a large network of global suppliers.[1]

We recently reported that the increase in counterfeit electronic parts is one of several potential barriers DOD faces in addressing parts quality problems.[2] In your request letter, you cited specific questions about the availability of counterfeit parts on Internet platforms commonly used to buy hard-to-find military-grade electronic parts, including those used in weapon systems. My statement today summarizes preliminary observations from our ongoing investigation into the purchase and authenticity testing of selected, military-grade electronic parts that may enter the DOD supply chain. We will issue our final report when our investigation is complete.

In conducting this investigation, we created a fictitious company to gain access to Internet platforms that sell military-grade electronic parts. Our company included a fictitious owner and employees, mailing and e-mail addresses, a Web site, and a listing on the Central Contractor Registration.[3] We attempted to purchase memberships to three Internet platforms that were of interest to this committee. We were granted memberships to two platforms but denied by the third. We then requested quotes from vendors on both platforms to purchase a total of 13 parts from a list of parts this committee provided that fell into one of three categories: (1) authentic part numbers for obsolete and rare parts, (2) authentic part numbers with post production date codes (date codes after the last date the part was manufactured), and (3) bogus part numbers. We independently verified with the Defense Logistics Agency (DLA) that the authentic part numbers were used for military applications using DLA's Federal Logistics Information System and by interviewing DLA officials.[4] We also confirmed with DLA and selected part manufacturers that the bogus part numbers were not associated with actual parts. We altered all part numbers in this testimony due to the ongoing nature of our investigation. We requested parts from vendors that were new in original packaging, not refurbished, and had no mixed date codes. We selected the first vendor among those offering the lowest

[1] Government Accountability Office (GAO), Defense Supplier Base: DOD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Counterfeit Parts, GAO–10–389 (Washington, DC: Mar. 29, 2010).

[2] GAO, Space and Missile Defense Acquisitions: Periodic Assessment Needed to Correct Parts Quality Problems in Major Programs, GAO–11–404 (Washington, D.C.: June 24, 2011).

[3] The Central Contractor Registration is the primary contractor registrant database for the U.S. Federal Government. The Central Contractor Registration collects, validates, stores, and disseminates data in support of agency acquisition missions.

[4] DLA's Federal Logistics Information Service via the World Wide Web provides general information about more than 8 million supply items used by the U.S. Government and North Atlantic Treaty Organization (NATO) allies.

prices that provided enough information, such as name, addresses, and payment method, to make a purchase. We attempted to avoid using the same vendor more than once unless no other vendor responded to our request; however, vendors may operate under more than one name. We did not attempt to verify the independence of any vendor before we made our purchases. Finally, we contracted with the SMT Corp. for full component authentication analysis. For details on this analysis, see appendix I. The results of this investigation are based on the use of a nongeneralizable sample, and these results cannot be used to make inferences about the extent that parts are being counterfeited. We began this investigation in August 2011 and are conducting it in accordance with standards prescribed by the Council of the Inspectors General on Integrity and Efficiency.

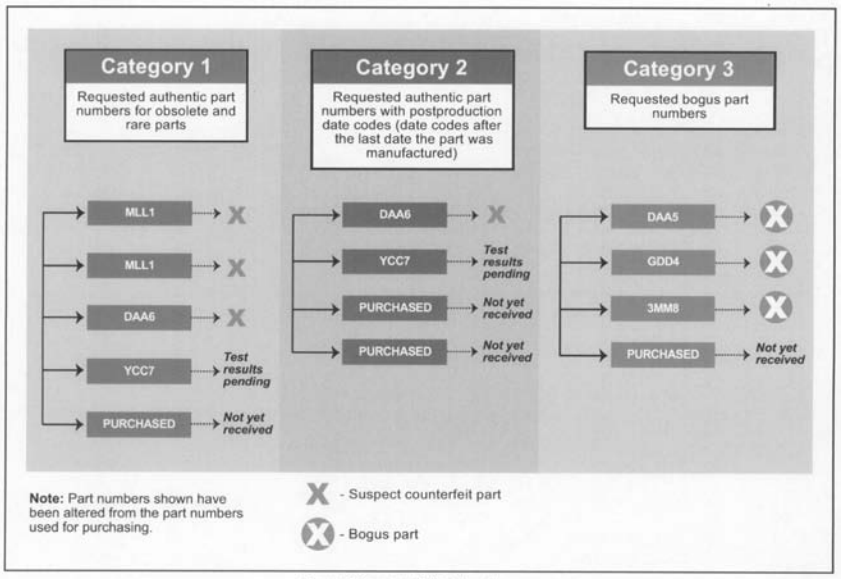
In summary, as of November 8, 2011, we have purchased 13 parts. None of the seven parts we have complete results for are authentic. Specifically, according to SMT Corp., all three parts tested after we requested legitimate but rare or obsolete parts failed at least three of seven authentication analyses and were "suspect counterfeit."[5] These parts included two voltage regulators and one operational amplifier, the failure of which could pose risks to the functioning of the electronic system where the parts reside. SMT Corp. also made the same determination for the other operational amplifier we received after requesting a legitimate part number with a post production date code. In this instance, the part failed four of seven authentication analyses, and the vendor also misrepresented the part as 9 years newer than the date it was last produced. In addition, we received three bogus parts after submitting orders using invalid part numbers. Because no legitimate parts in this final category exist—the part numbers are not in DLA's Federal Logistics Information System and selected manufacturers confirmed they have never been produced—we did not send them for authenticity testing. We are awaiting authentication analysis results for two additional parts, and have not yet received another four purchases. We will report the results for these and additional parts we plan to purchase in a future product. While we sent requests to both domestic and international companies, all of the parts we purchased and received to date were provided by vendors in China. We will issue our final report when our investigation is complete.

PRELIMINARY OBSERVATIONS POINT TO AVAILABILITY OF COUNTERFEIT AND NONEXISTENT PARTS

Figure 1 shows the preliminary status of the 13 parts we have purchased as of November 8, 2011. The text below details our preliminary findings for each of the three categories of parts.

[5] According to SMT Corporation, industry standards dictate that the term "counterfeit" cannot be used by an independent test lab; only the product manufacturer can deem a product counterfeit. Therefore, the term "suspect counterfeit" is defined as items that are produced or distributed in violation of intellectual property rights, copyrights, or trademark laws, as well as any items that are deliberately altered in such a way as to misrepresent the actual quality of the item with intent to defraud or deceive the purchaser.

Figure 1: Preliminary Status of Parts Purchased and Tested

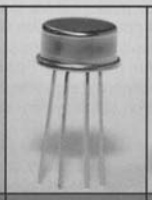
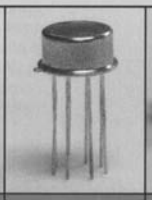
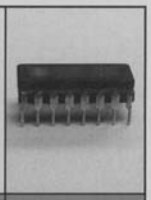


Source: GAO analysis of SMT test results.

Authentic Part Numbers for Obsolete or Rare Parts

All three of the obsolete or rare parts that SMT Corp. tested were suspected counterfeits. The parts were subject to a component authentication analysis, which included visual, chemical, x-ray, and microscopic testing. Figure 2 provides photos and detailed test results for each part. We purchased two additional parts; one is currently being tested by SMT Corp., while we have not yet received the other. All five parts were purchased through the same Internet platform.

Figure 2: Preliminary Authentication Analysis Results of Obsolete or Rare Parts

Category 1 Requested authentic part numbers for obsolete and rare parts				
Analysis performed	**MLL1**	**MLL1**	**DAA6**	**YCC7**
Visual inspection	Fail ☒	Fail ☒	Fail ☒	*Test results pending*
Package configuration and dimensions	Pass ☑	Pass ☑	Pass ☑	*Test results pending*
XRF elemental analysis	Fail ☒	Fail ☒	Fail ☒	*Test results pending*
Real-time x-ray analysis	Pass ☑	Pass ☑	Pass ☑	*Test results pending*
Scanning electron microscopy (SEM) analysis	Pass ☑	Pass ☑	Fail ☒	*Test results pending*
Solderability test	Pass ☑	Pass ☑	Pass ☑	*Test results pending*
Delidding and die microscopy	Fail ☒	Fail ☒	Fail ☒	*Test results pending*
Suspect counterfeit	**Yes**	**Yes**	**Yes**	***Test results pending***

Note: Part numbers shown have been altered from the part numbers used for purchasing.

Source: GAO analysis of SMT test results.

For two of the tested parts, purchased with part number MLL1, evidence lots contained a number of samples that failed three of seven analyses leading SMT Corp. to conclude that they are suspect counterfeit. Both parts were purchased from different vendors using the same part number, as pictured in figure 2. An authentic part with this number is a voltage regulator that may be commonly found in military systems such as the Air Force's KC–130 Hercules aircraft, the Navy's F/A–18E Super Hornet fighter plane, the Marine Corps' V–22 Osprey aircraft, and the Navy's SSN–688 Los Angeles Class nuclear-powered attack submarine. If authentic, these parts provide accurate power voltage to segments of the system they serve. Failure can lead to unreliable operation of several components (e.g., integrated circuits) in the system and poses risks to the function of the system where the parts reside.

Visual inspection was performed on all evidence samples for both parts. Different color epoxy seals were noted within both lots according to SMT Corp., which is common in suspect counterfeit devices because many date and lot codes are remarked to create a uniform appearance. Moreover, according to SMT Corp., x-ray fluorescence (XRF) testing of the samples revealed that the leads contain no lead (Pb), which, according to military performance standards defined in section A.3.5.6.3 of the MIL–PRF–38535J DOD Performance Specification for Integrated Circuits (Microcircuits) Manufacturing, should be alloyed with at least 3 percent of lead (Pb).[6,7] Further, XRF data between the top and bottom of the lead revealed inconsistencies in chemical composition, leading SMT Corp. to conclude that the leads were extended with the intention to deceive. Microscopic inspection revealed that different revision numbers of the die and differences in various die markings were

[6] XRF analyzers quickly and nondestructively determine the elemental composition of materials commonly found in microelectronic devices. Each of the elements present in a sample produces a unique set of characteristic x-rays that reveals the chemistry of the sample in an analogous manner to a fingerprint. A lead is an electrical connection consisting of a length of wire or soldering pad that comes from a device. Leads are used for physical support, to transfer power, to probe circuits, and to transmit information.

[7] Department of Defense, MIL–PRF–38535J (Dec. 28, 2010).

found even though the samples were advertised to be from the same lot and date code.[8] Commonly, components manufactured within the same date and lot code will have the same die revisions. According to SMT Corp.'s report, the manufacturer also stated that "it is very unusual to have two die runs in a common assembly lot. This is suspicious." Finally, the devices found in the first lot tested went into "last time buy" status—an end-of-life designation—on September 4, 2001, meaning that the parts were misrepresented as newer than they actually were. The manufacturer confirmed this status and added that the part marking did not match its marking scheme, meaning that the date code marked on the samples would not be possible.

For the third tested part, purchased as part number DAA6, evidence lots contained many samples that failed four authentication analyses, leading SMT Corp. to conclude that they are suspect counterfeit. An authentic part with this part number is an operational amplifier that may be commonly found in the Army and Air Force's Joint Surveillance and Target Attack Radar System (JSTARS); the Air Force's F–15 Eagle fighter plane; and the Air Force, Navy, and Marine Corps' Maverick AGM–65A missile. If authentic, this part converts input voltages into output voltages that can be hundreds to thousands of times larger. Failure can lead to unreliable operation of several components (e.g., integrated circuits) in the system and poses risks to the function of the system where the parts reside.

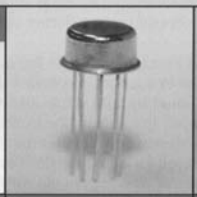
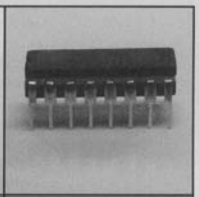
Visual inspection for DAA6 found inconsistencies, including different or missing markings and scratches, which suggested that samples were remarked. Scanning electron microscopy analysis revealed further evidence of remarking. Similarly to parts MLL1, XRF testing of the DAA6 samples revealed that the leads contain no lead (Pb) instead of the 3 percent lead (Pb) required by military specifications.[9] Five samples were chosen for delidding because of their side marking inconsistencies. While all five samples had the same die, the die markings were inconsistent. According to SMT Corp., die markings in components manufactured within the same date and lot code should be consistent. Finally, the devices found in the first lot tested went into "last time buy" status in 2001, meaning that the parts were misrepresented as newer than they actually were. The manufacturer confirmed this status and added that the part marking did not match its marking scheme, meaning that the date code marked on the samples would not be possible.

Authentic Part Numbers with Postproduction Date Codes

As of November 8, 2011, the part we received and tested after requesting a legitimate part number but specifying a postproduction date code was also suspected counterfeit, according to SMT Corp. Figure 3 provides a photo and detailed test results. We have purchased three additional parts with postproduction date codes; one is with SMT Corp. for testing, while we have not yet received the other two. By fulfilling our requests, the vendors agreed to provide parts that they represented as several years newer than when they were last manufactured. We verified the last date the parts were produced with the part manufacturers. Nonetheless, the parts will be subject to a full component authentication analysis.

[8] A die is a small wafer of semiconducting material on which a functional circuit is fabricated.
[9] Department of Defense, MIL–PRF–38535J.

Figure 3: Preliminary Authentication Analysis Results of Part with Invalid Date Codes

Category 2 Requested authentic part numbers with postproduction date codes (date codes after the last date the part was manufactured)		
Analysis performed	**DAA6**	**YCC7**
Visual inspection	Fail ☒	*Test results pending*
Package configuration and dimensions	Pass ☑	*Test results pending*
XRF elemental analysis	Fail ☒	*Test results pending*
Real-time x-ray analysis	Pass ☑	*Test results pending*
Scanning electron microscopy (SEM) analysis	Fail ☒	*Test results pending*
Solderability test	Pass ☑	*Test results pending*
Delidding and die microscopy	Fail ☒	*Test results pending*
Suspect counterfeit	**Yes**	*Test results pending*

Note: Part numbers shown have been altered from the part numbers used for purchasing.

Source: GAO analysis of SMT test results.

For the part purchased with part number DAA6, evidence lots contained many samples that failed four of seven analyses, leading SMT Corp. to conclude that they are suspect counterfeit. This is the same part number used to purchase the DAA6 part tested under category one, which was also suspected counterfeit. However, for this part our order included a postproduction date code in place of a valid one, and the part we received was supplied by a different vendor.

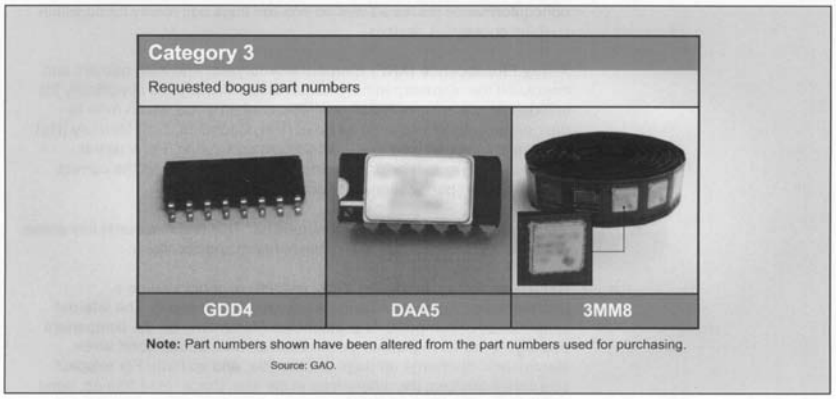
Surfaces on the parts in the evidence lots were found to have scratches similar to suspect counterfeit devices that have been remarked, as confirmed by both visual inspection and scanning electron microscopy analysis. In addition, the quality of exterior markings, including a lack of consistency between the manufacturer's logo, was lower than would be expected for authentic devices. Tooling marks were also found on the bottom of all components within the evidence lot; these marks suggest the components were pulled from a working environment. Further inspection led SMT Corp. to conclude that many samples with refurbished leads were extended with the intention to deceive. Moreover, XRF analysis revealed the leads contain no lead (Pb), which according to military performance standards defined in section A.3.5.6.3 of the MIL–PRF–38535J DOD Performance Specification for Integrated Circuits (Microcircuits) Manufacturing, should be alloyed with at least 3 percent of lead (Pb).[10] Delidding, which exposes parts' die, revealed that the die, while correct for this device, were inconsistent. As previously stated, multiple die runs are considered suspicious. Finally, some of the samples went into "last time buy" status in 2001, despite the fact that we requested 2005 or later and the vendor agreed to provide 2010 or later.

[10] Department of Defense, MIL–PRF–38535J.

Bogus Part Numbers

As of November 8, 2011, we have received three bogus parts after submitting requests using invalid part numbers. The fact that vendors fulfilled our requests indicates that they were willing to sell parts stamped with nonexistent part numbers essentially taking money in exchange for bogus parts. According to selected manufacturers, the part numbers we requested and received parts for, GDD4, DAA5, and 3MM8, are not associated with parts that have ever been manufactured. In addition, the parts were not listed in DLA's Federal Logistics Information Service. As such, we did not send the parts to SMT Corp. for authentication analysis. Figure 4 provides photos of the fictitious parts we received. We purchased a fourth part with an invalid part number but have not yet received it.

Figure 4: Photos of Parts Received Despite Requesting Invalid Part Numbers



Note: Part numbers shown have been altered from the part numbers used for purchasing.

Source: GAO.

Chairman Levin, Ranking Member McCain, and members of the committee, this concludes my prepared statement. I would be happy to respond to any questions you may have.

APPENDIX I: DETAILS OF AUTHENTICATION ANALYSIS TESTS

This appendix provides details on each of the tests that constitute the authentication analysis SMT Corp. conducted for the parts we purchased.

Visual Inspection:

Visual inspection is performed on a predetermined number of samples (usually 100 percent) to look for legitimate nonconformance issues as well as any red flags commonly found within suspect counterfeit devices.

X-Ray Florescence (XRF) Elemental Analysis:

The XRF gathers and measures the elements within a target area. This is used specifically for testing components for RoHS or Hi-Rel conformance, which refer to dangerous substances such as Lead (Pb), Cadmium (Cd), Mercury (Hg) that are commonly used in electronics manufacturing. For suspect counterfeit devices, it helps determine if a component has the correct plating for the specification it supposed to adhere to.

Package Configuration and Dimensions:

This test measures key areas of the device to see if they fall within industry specifications.

Real-Time X-Ray Analysis:

X-ray analysis is performed on a predetermined number of samples (usually 100 percent). The internal construction of components is inspected (depending on the component package type) for legitimate issues such as broken/taut bond wires, electrostatic discharge damage, broken die, and so forth. For suspect counterfeit devices, the differences in die size/shape, lead frames, bond wire layout, etc. are inspected.

Scanning Electron Microscopy:

A scanning electron microscope is used to perform an exterior visual inspection—more in-depth than the previous visual inspection. This is usually performed on a two-piece sample from the evidence lot. Depending on the package type, indications of suspect counterfeit devices are sought, including surface lapping, sandblasting, and sanding with regards to part marking removal.

Solderability:

This test is usually for legitimate components to determine if they will solder properly when going to be used in production.

Decapsulation/Delidding and Die Verification:

The die of a component is exposed with either corrosive materials or a cutting apparatus. This is done to inspect the die or "brain" of a component to determine its legitimacy. This process is performed on numerous samples to look for differences between samples such as die metallization layout, revisions, part numbers, and so forth—all of which are red flags for suspect counterfeits.

Chairman LEVIN. Thank you so much, Mr. Hillman, for your investigation here and for all the other great work that GAO does.

Mr. Toohey.

STATEMENT OF BRIAN C. TOOHEY, PRESIDENT, SEMICONDUCTOR INDUSTRY ASSOCIATION

Mr. TOOHEY. Chairman Levin, Ranking Member McCain, and members of the committee, I greatly appreciate the opportunity to testify today to aid in your investigation into counterfeit electronic parts in the DOD supply chain and about the dangers that counterfeit semiconductors pose to U.S. national security and public safety.

The issue is of more and more importance as semiconductors are key components to an increasing number of mission-critical civilian applications such as lifesaving medical devices, automotive safety systems, airplanes, but even more alarmingly, counterfeit semiconductors have infiltrated the tools, systems, and communications equipment that our military is using today.

By way of brief background, a semiconductor is the foundation or brains of any electronic device. The popular terms, "microelectronics," "integrated circuits," and "computer chips," are synonymous with semiconductors.

Our industry is America's largest exporter, and semiconductor innovations form the foundation for America's $1.1 trillion technology industry that supports a workforce of nearly 6 million. The semiconductor industry is a great American innovation story, and our companies still lead the world in the rapid pace of innovation and global market share. We consider our industry a model for the innovation economy of the future, and our companies still do the vast majority of advance design and manufacturing here in the United States and sell nearly 85 percent of our products internationally.

First, a note on how legitimate semiconductors are manufactured versus counterfeits. Our members, which include the largest U.S. headquartered semiconductor companies, invest billions of dollars in state-of-the-art facilities in order to manufacture semiconductors in ultra-clean rooms. The highly sensitive chips are then tested to ensure they function to exacting specifications and standards. In the case of military-grade chips, these specific semiconductors are designed and tested to withstand intense temperature and movement variables to meet the performance standards necessary for combat and military situations.

In contrast, as the chairman and ranking member noted, counterfeiters abroad rummage through piles of e-waste—in some instances, this includes old computers and circuit boards from the 1980s and 1990s—and use crude techniques like surface sanding, acid washes, and open flames to conceal the true origin and purpose of the chip. These chips, already weakened from their original state and at great risk of failure, are then relabeled sometimes as military-grade using digital printing and laser etching and packaged for sale to international brokers. Recently counterfeiters have begun acquiring more sophisticated equipment and advanced labeling techniques making it increasingly difficult to identify fake semiconductors.

Our members have also found factories that manufacture blank chips on which counterfeit markings are added later in a made-to-order fashion even if the chip's functionality does not match the order specifications.

As a result, more and more counterfeit chips make it through our borders into a wide range of products. Given the high failure risk, this places our citizens and our military personnel in unreasonable peril. A counterfeit semiconductor is a ticking time bomb.

A prime example of counterfeits making their way into the military supply chain is the VisionTech case which recently resulted in the first felony conviction for counterfeit IC trafficking. The counterfeit semiconductor sold by VisionTech included chips destined for naval vessel and land-based identification friend or foe systems, memory chips for the Harm Testing System used by F–16s to track hostile radar systems, chips intended for an application the U.S. Navy Cobra Judy Replacement Program, and chips that control the braking system in high-speed trains. This is a very real and very alarming problem. Americans' lives are at risk every time a counterfeit semiconductor makes its way into one of these highly complex and mission-critical systems.

Experts have estimated that as many as 15 percent of all spare and replacement parts purchased by the Pentagon are counterfeit.

Overall, as the chairman noted, we estimate that counterfeiting costs U.S.-based semiconductor companies more than $7.5 billion per year, which translates into nearly 11,000 lost American jobs.

Our industry takes this threat very seriously and we are committed to doing everything within our power to stop counterfeits from entering the United States and being used in our military and civilian supply chains. We believe this is a multi-faceted problem that will require a multi-pronged approach with a coordinated effort from Government and industry.

While I understand this is primarily an investigative hearing, I would like to offer five steps that we view as critical to combating this clear and present danger.

First, we should continue our successful partnerships with DOD and the Department of Justice and the semiconductor industry and others to develop a more robust and effective authentication system.

Second, DOD should implement strengthened procurement procedures for mission-critical components, including purchasing exclusively from authorized distributors or DOD-certified resellers.

Third, we should strengthen our ability, the industry's ability, to partner with customs officials to stop counterfeit semiconductors at the border. In 2008, Customs and Border Protection (CBP) stopped the successful practice of sharing key information regarding suspect counterfeit chips with manufacturers and began redacting or crossing out critical manufacturing codes making it virtually impossible to determine if the suspect chips are authentic or counterfeit. Returning to the pre-2008 practice would significantly improve our Nation's ability to stop counterfeits at our border.

Fourth, we should continue to aggressively prosecute counterfeit traffickers.

Finally, we should leverage every trade tool at our disposal to encourage stronger enforcement of intellectual property rights, especially trademarks, internationally.

Thank you for this opportunity to testify, and I would welcome any questions.

[The prepared statement of Mr. Toohey follows:]

PREPARED STATEMENT BY BRIAN TOOHEY

EXECUTIVE SUMMARY

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

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

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

To address the threat with military applications, SIA and the Department of Defense (DOD) have been working closely to develop a new product authentication process to increase the ability of our industry, with DOD and other agencies to work more cooperatively to identify counterfeit products and potentially their sellers or importers. Our goal is to develop a process that will make both industry and government more effective and timely in fighting counterfeiters. The SIA Anti-Counterfeiting Task Force (ACTF), DOD, as well as the National Aeronautics and Space Administration (NASA), Jet Propulsion Laboratory, and other trade associations and companies formed the DOD Working Group. The Working Group has created a Product Identification/Authentication Request Form that will assist government agencies in requesting authentication services, from the manufacturer, for suspect products found during acquisition or already in the government supply chain. That form and authentication process are in the final review stage. The next Working Group project will be to draft recommendations for better procurement procedures for mission-critical and life/safety products to avoid procuring counterfeit products or products with embedded malware and back doors. Finally, SIA's Anti-Counterfeit Task Force, DOD and other government agencies are participating in the Department of Justice's (DOJ) DC Counterfeit Microelectronics Working Group where gov-

ernment agencies and industry exchange information on counterfeiting and anti-counterfeiting activities with a focus on identifying, investigating and prosecuting people that make or sell counterfeits in the United States.

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

Prior to 2000 when port officers suspected a shipment contained counterfeit chips, they would contact the trademark owner and share one of the products. After 2000, but before 2008, Port Officers photographed the outside of a suspect chip and sent the publicly viewable information to the chip manufacturer whose trademark appeared on the surface of the chip to determine whether the chip was counterfeit. Using a highly confidential database, the trademark owner could then determine very quickly, for almost 85 percent of the requests, whether or not the chips were counterfeits by analyzing the codes on the surface of the chip.

In mid-2008, however, CBP officers were instructed to redact any identifying marks in the photographs, except the trademark, before sending them to manufacturers, thereby scuttling the cooperative system that worked so well for 8 years. The current redaction practice makes it impossible for the industry, much less CBP, to authenticate suspected counterfeit semiconductors. CBP officials argue this change in practice is intended to shield port officers from criminal liability for the disclosure of confidential information. However, to the extent the codes on the surface of semiconductors—which are publicly-viewable by anybody who picks up a chip or looks at a chip's packaging label—are confidential; they belong to the manufacturers to whom photographs would be sent and not the importer.

SIA simply asks CBP to revert to its historical pre-2008 practice and share unredacted photographs, and where necessary physical products, of suspected counterfeit semiconductors with their original manufacturers. Such a policy is clearly in the Nation's interest to continuously improve our security. Preventing counterfeit semiconductors from entering the United States will safeguard the military supply chain and protect public health and safety.

BACKGROUND ON SEMICONDUCTORS

Semiconductor "chips" are used in everything that is computerized or uses radio waves. Indeed, semiconductors are components in a staggering variety of products, from computers and smart phones to medical devices, LEDs and smart meters, automobiles and military equipment, including missiles, radar, navigation systems and jets. They are making the world around us smarter, greener, safer, and more efficient. They form that backbone of our critical infrastructure and are economically vital to the Nation's growth and productivity.

In 2010, U.S. semiconductor companies generated over $140 billion in sales—representing nearly half the worldwide market, and making semiconductors the Nation's largest export industry on a 5-year average. Our industry directly employs nearly 200,000 workers in the U.S. Studies show that semiconductors, and the information technologies they enable, represent 3 percent of the economy, but drive 25 percent of economic growth.

BACKGROUND ON THE SIA

SIA is the voice of the U.S. semiconductor industry, America's largest export industry since 2005 and a bellwether of the U.S. economy. Semiconductor innovations form the foundation for America's $1.1 trillion technology industry affecting a U.S. workforce of nearly 6 million. Founded in 1977 by five microelectronics pioneers, SIA unites more than 60 companies from across the United States that account for 80 percent of the Nation's semiconductor production. Our industry has an especially robust presence in Arizona, California, Colorado, Idaho, Maine, Massachusetts, New York, New Hampshire, North Carolina, South Carolina, Oregon, Rhode Island, Texas and Virginia.

SIA seeks to strengthen U.S. leadership in semiconductor design and manufacture by working with Congress, the administration, and other industry groups to enable the right ecosystem for technology development and commercialization. Specifically, SIA encourages policies and regulations that fuel innovation, propel business and drive international competition in order to maintain a thriving semiconductor industry in the United States.

INCREASING PREVALENCE OF COUNTERFEITS

Due to the increasing availability and decreasing price of equipment needed to counterfeit semiconductors, unscrupulous brokers looking to garner illicit profits are importing ever greater numbers of counterfeit chips into the United States. In fact, the Department of Commerce has reported that counterfeit incidents discovered by the military and military suppliers more than doubled between 2005 and 2008, from 3,868 to more than 9,356 cases.[1]

In July of this year Greg Schaffer, the Acting Deputy Under Secretary for the Department of Homeland Security National (DHS) Protection and Programs Directorate, provided testimony to the House Oversight and Government Reform Committee. During the hearing, Mr. Schaffer was asked, and admitted that DOD had purchased counterfeit electronic products with embedded security risks that were found in the DOD supply chain.[2]

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

Alarmingly, counterfeit chips can be found in automobile airbag systems, defibrillators, and even highly-sensitive military equipment. As a 2008 Business Week article explains:

> The American military faces a growing threat of potentially fatal equipment failure—and even foreign espionage—because of counterfeit computer components used in warplanes, ships, and communications networks. Fake microchips flow from unruly bazaars in rural China to dubious kitchen-table brokers in the United States and into complex weapons. Senior Pentagon officials publicly play down the danger, but government documents, as well as interviews with insiders, suggest possible connections between phony parts and breakdowns. In November 2005, a confidential Pentagon-industry program that tracks counterfeits issued an alert that "BAE Systems experienced field failures," meaning military equipment malfunctions, which the large defense contractor traced to fake microchips . . . . In a separate incident last January, a chip falsely identified as having been made by Xicor . . . was discovered in the flight computer of an F–15 fighter jet at Robins Air Force Base . . . . Special Agent Terry Mosher of the Air Force Office of Special Investigations confirms that the 409th Supply Chain Management Squadron eventually found four counterfeit Xicor chips.[4]

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

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

> The traders typically obtain supplies from recycled-chip emporiums such as the Guiyu electronics Market outside the city of Shantou in southeastern China. The garbage-strewn streets of Guiyu reek of burning plastic as workers in back rooms and open yards strip chips from old PC circuit boards. The components, typically less than an inch long, are cleaned in the nearby Lianjiang River and then sold from the cramped premises of businesses such as Jinlong Electronics Trade Center. A sign for Jinlong Electronics advertises in Chinese that it sells "military" circuitry, meaning chips that are more durable than commercial components and able to function at extreme temperatures. But proprietor Lu Weilong admits that his

---

[1] U.S. Department of Commerce, Defense Industrial Base Assessment: Counterfeit Electronics available at http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final—counterfeit—electronics—report.pdf; see also Michele Moss, Systems Assurance, The Global Supply Chain, and Efforts to Increase Communication Between Acquisition and Development, available at http://www.dtic.mil/ndia/2010CMMI/WednesdayTrack4—11328Moss.pdf; Surge in counterfeit items in Pentagon's supplies, Homeland Security Newswire, Aug. 10, 2010, available at http://www.homelandsecuritynewswire.com/surge-counterfeit-items-pentagons-supplies.

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

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

[4] Brian Grow et al., Dangerous Fakes: How counterfeit, defective computer components from China are getting into U.S. warplanes and ships, BusinessWeek, Oct. 2, 2008, available at http://www.businessweek.com/magazine/content/08—41/b4103034193886.htm.

[5] Id.

wares are counterfeit. His employees sand off the markings on used commercial chips and relabel them as military. Everyone in Guiyu does this, he says:

> "The dates [on the chips] are 100 percent fake, because the products pulled off the computer boards are from the 1980s and 1990s, [while] consumers demand products from after 2000."[6]

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

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

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

ADMINISTRATION RESOLVE TO COMBAT COUNTERFEITS

Mr. Chao is correct—it is difficult to differentiate between a legitimate semiconductor and a fake. It is precisely because of the difficulties inherent in differentiating between a legitimate and counterfeit semiconductor that the government must place a single-minded emphasis on preventing the importation of counterfeit chips.[9]

The Obama administration—like the previous Bush and Clinton administrations—has shown an admirable resolve to combat counterfeiting and other forms of intellectual property theft. Indeed, President Obama himself has promised:

> We're going to aggressively protect our intellectual property. Our single greatest asset is the innovation and the ingenuity and creativity of the American people. It is essential to our prosperity and it will only become more so in this century.[10]

Last year, Department of Justice (DOJ), Immigration and Customs Enforcement (ICE), the Office of Homeland Security Investigations, Naval Criminal Investigative Service (NCIS), Postal Inspection Service, Internal Revenue Service, Department of Transportation and General Services Administration worked together with the semiconductor industry on an investigation that led to the indictments of the principals of a Florida-based company that generated nearly $16 million in gross receipts between 2007 and 2009 by importing nearly 60,000 counterfeit semiconductors from China and selling them to the military as "military grade."[11] As the U.S. Attorney in charge of the investigation explained:

---

[6] Id.

[7] Attachment 1.

[8] Id.

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

[10] Victoria Espinel, 2010 Joint Strategic Plan on Intellectual Property Enforcement 3, available at http://www.whitehouse.gov/sites/default/files/omb/assets/intellectualproperty/intellectualproperty—strategic—plan.pdf ("IPEC Report").

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

> Product counterfeiting, particularly of the sophisticated kind of equipment used by our Armed Forces, puts lives and property at risk. This case shows our determination to work in coordination with our law enforcement partners and the private sector to aggressively prosecute those who traffic in counterfeit parts.[12]

From 2006 to 2010, VisionTech Components knowingly sold counterfeit integrated circuits to approximately 1,101 buyers in the United States and abroad, including counterfeit integrated circuits destined for military applications. VisionTech shipped 75 counterfeit chips destined for naval vessel and land-based Identification Friend or Foe system. As the U.S. Attorney noted, "if the system failed during an engagement and could not identify an approaching threat aircraft 25 miles away, a missile fired from the threat aircraft could hit a ship 1 minute later."[13] Other shipments included 1,500 counterfeit memory chips destined for the Harm Testing System installed on F–16s to track hostile radar systems,[14] 350 counterfeit ICs intended for an application in the Beam Steering Control Module board within Multiple Sub-Array of Testable Antenna for the U.S. Navy Cobra Judy Replacement Program,[15] 1,500 counterfeit chips to control the braking system in a high speed train,[16] and 196 counterfeit chips to be used in a hand-held portable nuclear identification tool, a device offered for sale on the Federal Emergency Management Agency (FEMA) Web site as suggested emergency equipment for first responders.[17] For her part in the scheme, VisionTech's administrator, Stephanie McCloskey, was sentenced to 38 months imprisonment and $166,141 in fines.

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

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

> Violations of intellectual property rights, ambiguities in law and lack of enforcement create uncertainty in the marketplace, in the legal system and undermine consumer trust. Supply chains become polluted with counterfeit goods. Consumers are uncertain about what types of behavior are appropriate and whether the goods they are buying are legal and safe. Counterfeit products can pose a significant risk to public health, such as . . . military systems with untested and ineffective components to protect U.S. and allied soldiers, auto parts of unknown quality that play critical roles in securing passengers and suspect semiconductors used in lifesaving defibrillators . . . . Intellectual property infringement [also] can undermine our national and economic security. This includes counterfeit products entering the supply chain of the U.S. military, and economic espionage and theft of trade secrets by foreign citizens and companies.[18]

COOPERATION BETWEEN DOD AND THE SEMICONDUCTOR INDUSTRY

The SIA Anti-Counterfeiting Task Force (ACTF) and DOD have been collaborating to develop a new product authentication process to increase the ability of our industry and the U.S. Government to work more cooperatively to identify counterfeit products and potentially their sellers or importers. Our goal is to develop a process that will make both industry and government more effective and timely in fighting counterfeiters. The SIA ACTF, DOD, as well as NASA, Jet Propulsion Laboratory, and other trade associations and companies formed the DOD Working Group. The Working Group has created a Product Identification/Authentication Request Form that will assist DOD and other government agencies in authenticating suspect prod-

[12] Id.
[13] Government's Consolidated Memorandum In Aid Of Sentencing and Motion for Downward Departure Pursuant to U.S.S.G. § 5K1.1, September 9, 2011 at 50.
[14] Id. at 51.
[15] Id. at 54.
[16] Id. at 55.
[17] Id at 56–57.
[18] IPEC Report at 4.

ucts during acquisition or already in the government supply chain. That form and authentication process is in the final review stage.

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

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

CURRENT GOVERNMENT PURCHASING PRACTICES INCREASE COUNTERFEITS IN THE DOD SUPPLY CHAIN

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

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

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

The SIA respectfully recommends that the U.S. Government, and in particular DOD, should change its purchasing policies to ensure that products critical to life, health, safety, mission-critical applications and critical infrastructure are purchased from the manufacturer's authorized distributors when available. When those products are no longer available, such as legacy hardware 5 to 30 years old, then the government should implement new purchasing and product security processes. Buying critical components at low prices only saves money upfront and in the end could cost DOD far more in lives, failed missions, and replacement costs.

CBP ACTION HALTS INDUSTRY ASSISTANCE IN COMBATING COUNTERFEITING

Unfortunately, despite the Obama administration's understanding of the dangers posed by counterfeit semiconductors, and the excellent working relationship on anticounterfeiting between SIA, DOD, DOJ, NCIS, ICE, FBI and other Federal agencies, a 2008 CBP action is frustrating the efforts of those government agencies to combat the importation of counterfeit chips.

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

numerous successful raids of counterfeit manufacturers in China and brokers in the United States.[19]

However, in August 2008 manufacturers discovered Customs Officers had been ordered to stop sending photographs (or samples) of suspect chips showing the information required by a manufacturer to authenticate a chip—even though CBP had been sending such photographs for nearly 8 years. Instead, CBP began sending redacted photos that obscured identifying information and left only the manufacturer's trademark visible. Given the advanced labeling technology now available to counterfeiters, manufacturers cannot determine whether chips are counterfeit based on these logo-only pictures. Not surprisingly, before August 2008, seizures of counterfeit semiconductors were increasing year after year.

Since CBP changed its practice, interdictions at the border have been down and SIA members have reported receiving an increased number of complaints about counterfeits from end customers when the chip fails. Semiconductor manufacturers were not notified or provided an opportunity to comment before CBP began implementing the new practice; one day in August 2008, the identifying markings on photographs sent to manufacturers were simply redacted.

The CBP's new post-2008 redaction practice is based on an April 2000 Customs Directive which instructed Customs Officers to "remove or obliterate any information indicating the name and/or address of the manufacturer, exporter, and/or importer, including all bar codes or other identifying marks" before providing samples of chips suspected to bear "confusingly similar" trademarks to semiconductor manufacturers.[20] Of course, Customs Officers understood that this policy could not effectively prevent the importation of counterfeit semiconductors. The Officers did not interpret the restrictive Directive to apply to photographs until August 2008; when, we have been told, CBP Port Officers were "reminded" by Treasury officials that the April 2000 Directive applies to photographs.

CUSTOMS NEEDS MANUFACTURERS' SUPPORT TO PREVENT THE IMPORTATION OF COUNTERFEIT SEMICONDUCTORS

CBP cannot effectively prevent the importation of counterfeit semiconductors without the manufacturers/trademark owners' assistance. A semiconductor is very different from apparel, for example, where a photograph of a fake luxury handbag redacted per the Customs Directive's instructions likely still provides sufficient information for an intellectual property rights holder to determine the authenticity of merchandise. In contrast, semiconductor manufacturers use common exterior packages (which fit in common board designs) for their semiconductors. Moreover, counterfeiters have obtained professional and up-to-date laser etching equipment to place fake codes on counterfeit chips. Thus, it is almost always impossible to determine whether a given chip is legitimate or counterfeit based on the redacted photographs.[21]

Semiconductor manufacturers can only assist CBP in preventing importation of counterfeit merchandise if CBP provides manufacturers with sufficient information to determine whether suspect chips are authentic. An unredacted photograph of a suspect chip would ordinarily be sufficient to provide the manufacturing codes (that usually represent lot numbers, dates and locations of assembly) a manufacturer needs to authenticate a chip. Alternatively, CBP could provide manufacturers with these numbers or a sample chip.

However, a photograph that has been redacted to remove these numbers does not provide sufficient information to determine the authenticity of a chip. Unless CBP provides manufacturers unredacted photographs of suspect chips (or provides the manufacturing codes and dates and locations of assembly reflected on the face of the suspect chips that only manufacturers can decipher), CBP cannot discharge its statutory obligation to ensure that imports comply with U.S. intellectual property laws. In such circumstances, the risk increases that counterfeit chips will enter U.S. commerce and ultimately end up as components in commercial, industrial and military systems, as we have witnessed since Treasury's policy shift.

---

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

[20] Customs Directive No. 2310–008A (April 7, 2000), available at http://www.cbp.gov/linkhandler/cgov/trade/legal/directives/2310–008a.ctt/2310–008a.pdf.

[21] See Exhibit 1.

CUSTOMS HAS THE AUTHORITY TO ENLIST INDUSTRY HELP

The most frustrating aspect of the current policy is the fact that CBP has all the legal authority necessary to provide semiconductor manufacturers with the information necessary to stem the tide of counterfeit chips. CBP officials have claimed the 2000 Directive is meant to protect Customs Officers from liability under the Disclosure of Confidential Information (DCI) provision of the Trade Secrets Act.[22] However, such protection is unnecessary, as Customs Officers are only exposed to DCI liability to the extent that CBP decides that information is confidential and may not be disclosed.[23] Therefore, CBP can effectively protect Customs Officers by simply declaring that the information included on the surface of semiconductors is not confidential information, as it had implied prior to its policy shift. Indeed, it is unclear how a code that is readily visible to anyone looking at the product label on a container containing semiconductors or the surface of a semiconductor can be confidential information. Tellingly, when Customs promulgated the rule the 2000 Directive was intended to "fix,"[24] it identified two potential trade secrets that might be divulged when disclosing information: the identity of the manufacturer and the identity of the importer.[25] But sharing the codes on the surface of semiconductors and product labels on the packaging with semiconductor manufacturers would not reveal either, as the manufacturer knows its own identity and the surface codes reveal no information about a chip's importer.

CBP has failed to understand that even if the publicly-viewable codes were confidential, Congress clearly contemplated CBP disclosing such information to rights holders in order to permit CBP to fulfill the many laws and treaties requiring it to stop counterfeits from entering the United States. The DCI simply prohibits government officials from disclosing confidential information that "concerns or relates to ... the identity ... of any person" to "any extent not authorized by law." Accordingly, Congress has authorized CBP to provide unredacted photos to semiconductor manufacturers through the Tariff Act of 1930, the Lanham Act, the North American Free Trade Agreement, and the GATT Agreement on Trade-Related Aspects of Intellectual Property Rights. In addition, CBP's own Disclosure of Information Regulation authorizes such disclosure.[26] It is truly difficult to understand why CBP believes disclosing information to semiconductor manufacturers is unlawful when ICE, DOD, DOJ, NCIS, and even the FBI—the agency tasked with enforcing the Trade Secrets Act—do not, and in fact routinely disclose such information to semiconductor manufacturers.

CONCLUSION

As a trade association that represents one of America's most vital industries, SIA hopes that all executive agencies will support the Obama administration's intellectual property enforcement efforts by working together to reduce counterfeit imports expeditiously. Counterfeit semiconductors are a clear and present national security threat and danger to human health because they are used in many mission-critical applications.

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

---

[22] 18 U.S.C. § 1905.

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

[24] 19 C.F.R. § 133.25 ("Customs may disclose to the owner of the trademark or trade name ... in order to obtain assistance in determining whether an imported article bears an infringing trademark or trade name ... [a] description of the merchandise").

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

[26] See note 24.

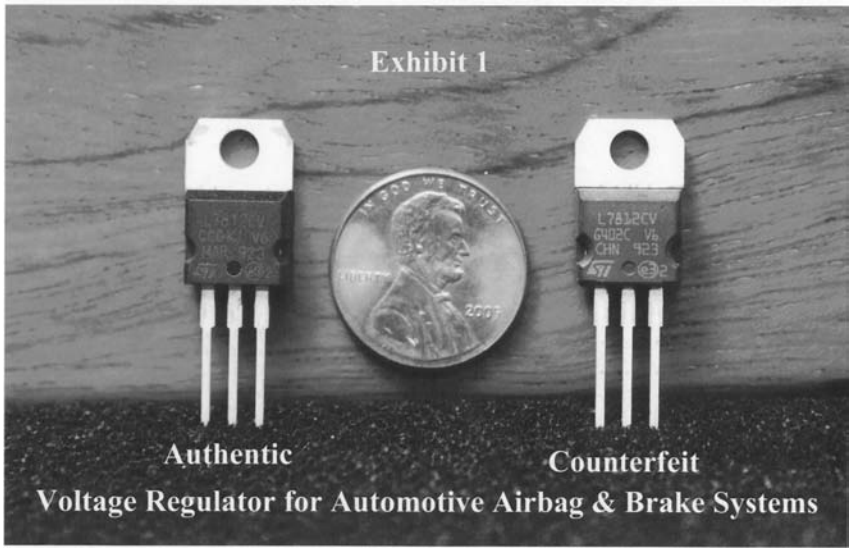
We are pleased with the SIA-DOD Working Group's progress on creating a system for assisting our armed forces in detecting counterfeit chips already in the DOD supply chain. We are optimistic that the Working Group will also craft recommendations to reform government procurement practices to ensure that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

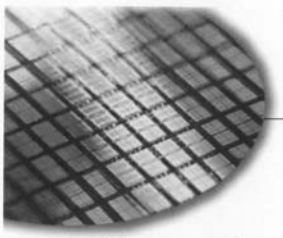
SIA is also pleased with the efforts by the U.S. Attorney for the District of Columbia, ICE, NCIS, FBI, and other Federal law enforcement agencies to bring to justice unscrupulous brokers selling dangerous counterfeits into the military and civilian supply chains. However, the post-2008 CBP policy prevents the U.S. Government from most effectively working with industry to prevent counterfeit chips from being imported into the United States. This is alarming, especially given the danger such chips so obviously present.

We respectfully request this committee and Congress work with DOD to require government contractors and subcontractors to purchase critical components from authorized sources. We also respectfully request this committee and Congress to work with CBP to ensure that the pre-2008 practice of sharing unredacted pictures of suspected counterfeit semiconductors and product labels with manufacturers is reinstated in the interest of safeguarding the health and safety of the American public and our military.

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

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





The World Leader in High-Performance Signal Processing Solutions

Counterfeit Microcircuits: The #1 Threat to Electronics Reliability

Andrew Olney

Director of Reliability, Product Analysis, Calibration & ESD

September 1, 2011

ANALOG DEVICES

© 2011 Analog Devices, Inc. All rights reserved.

Outline

- Categories of Counterfeit ICs
- Increasing Sophistication of Counterfeiters
- Why Counterfeit ICs Have Poor Reliability
- Summary

© 2011 Analog Devices, Inc. All rights reserved.

ANALOG DEVICES

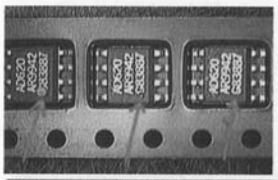
Categories of Counterfeit ICs

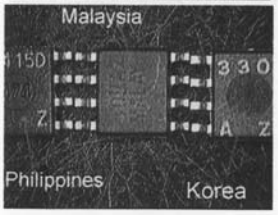
1. Recycled / Used ICs
   - Parts pulled from boards; leads straightened/cleaned; original markings removed or "blacktopped"; new markings added
2. Lower Grade / Inferior "Second-Source" ICs
   - Parts may be new or used; original markings removed or "blacktopped"; new markings added
   - Parts typically are functional but out-of-spec
3. New or Used IC Die Assembled in New Packages
   - Die may be removed from "old" packages and assembled in new packages; extremely difficult to detect these counterfeits!
4. Useless ICs
   - Parts are non-functional: no die, bad die, wrong die, wrong package, etc.

© 2011 Analog Devices, Inc. All rights reserved.

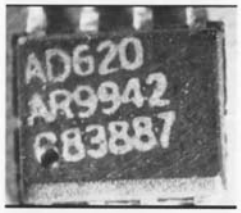
ANALOG DEVICES

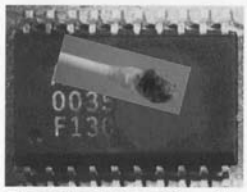
Counterfeits Easy to Detect Years Ago





Counterfeit units with various pin 1 indicators and countries of origin.





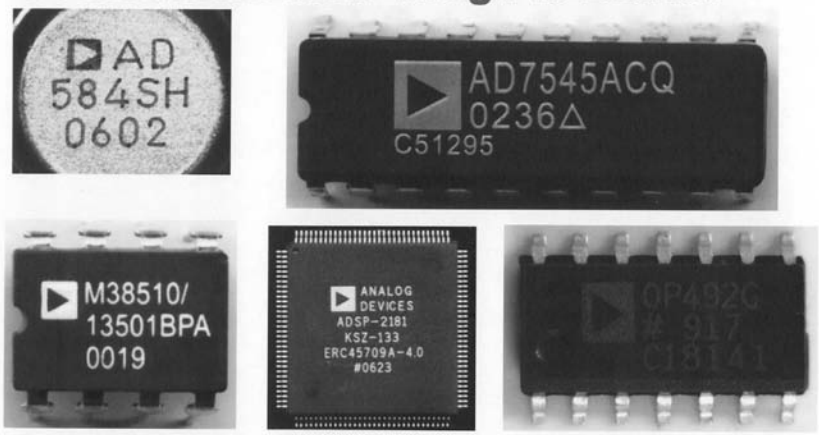
Counterfeit units with poor and/or easily removed markings.

Counterfeit units with obvious sanding marks.

© 2011 Analog Devices, Inc. All rights reserved.

ANALOG DEVICES

Counterfeits Now Tough to Detect



Excellent top marking quality (both ink and laser markings), but these products are all counterfeit.

© 2011 Analog Devices, Inc. All rights reserved.

ANALOG DEVICES

Counterfeit ICs Have Poor Reliability

- Package cracking, package delamination, and/or die cracking induced by IC removal from scrap boards
  - IC "recyclers" rarely take precautions against package damage
  - Package damage is not always detected immediately electrically
- Used ICs zapped by ESD during board removal; stripping markings; adding counterfeit markings; etc.
  - Counterfeiters rarely take precautions against ESD
  - Zapped ICs may fail during field use due to latent ESD damage
  - Especially CMOS gate oxide & Bipolar/BiCMOS capacitors

© 2011 Analog Devices, Inc. All rights reserved.

ANALOG DEVICES

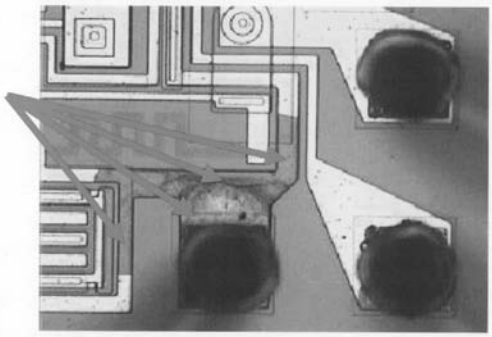
Counterfeit ICs Have Poor Reliability

- Moisture-sensitive parts not handled / stored properly, resulting in "popcorning" during board assembly
  - Counterfeiters are unlikely to dry pack moisture-sensitive parts
  - Brokers may dry pack parts without properly baking them first
- Chemicals used to strip the original markings and/or to clean the package pins result in corrosion
  - Counterfeiters may use harsh chemicals that can damage ICs
  - Such ICs may fail during field use due to the time it takes for chemicals to penetrate the package and corrode the die
  - Especially an issue with plastic-encapsulated microcircuits

© 2011 Analog Devices, Inc. All rights reserved.

ANALOG DEVICES

Counterfeit ICs Have Poor Reliability



Used ICs were removed from PCBs and re-marked by counterfeiters. The pins were cleaned with acid. Over time, the acid migrated into the plastic packages and corroded away the metal on the die (see arrows), resulting in field failures and high OEM warranty costs.

© 2011 Analog Devices, Inc. All rights reserved.

ANALOG DEVICES

Counterfeit ICs Have Poor Reliability

- Counterfeits marked as having Pb-Sn solder may be Pb-free, or vice-versa
  - Parts may be unreliable after board mount at wrong temperature for the true solder composition
  - Parts that should not contain Sn may fail due to Sn whiskers
- Net result of all these potential failure mechanisms
  - Counterfeit ICs can initially work fine and then fail days, months, or years later in the field
  - Classic reliability models (such as MIL-HDBK-217 MTBF calculations) are completely meaningless if even one component in a system is counterfeit!

© 2011 Analog Devices, Inc. All rights reserved.

ANALOG DEVICES

Summary

- Counterfeit ICs far more difficult to detect than in the past
  - Sometimes only OCMs can positively identify good from bad
- Counterfeits are the #1 threat to electronics reliability!
  - Packages or die may delaminate / crack during PCB removal
  - Parts may be ESD zapped & later fail due to latent ESD damage
  - Moisture-sensitive devices may "popcorn" during board assembly
  - Counterfeits marked as Pb-bearing may be Pb-free or vice-versa
  - Chemicals used to clean / re-mark ICs may result in corrosion
  - Net result is large warranty / monetary claims
- All traditional reliability models (MIL-HDBK-217, etc.) are meaningless if any component in a systems is counterfeit
- Best protection is to buy directly from component suppliers or directly from their authorized distributors

© 2011 Analog Devices, Inc. All rights reserved.

ANALOG DEVICES

Chairman LEVIN. Thank you so much, Mr. Toohey. Let us try a 7-minute first round for questioning. If we need a second round, we will have one.

Let me start first with you, Mr. Hillman. This action or activity of the GAO to try to test this market produced some really stunning results. The idea that you can give any part number, make up a part number, and you can find somebody who will act as though they are responding to that order on the Internet is an amazing result. They are all coming from China so far. It fits with what our investigation shows, that China is the source of the counterfeits.

When you set out to buy parts, when the GAO set out to buy parts, you did not specifically aim at any particular country. Right? You went on a global marketplace, the Internet.

Mr. HILLMAN. That is correct. We did not target any specific region such as Asia, Europe, or North America. What we looked at specifically was individual part numbers requested by this committee. We entered those numbers on the Internet trading platforms. Vendors then offered quotations for us and we selected quotations that were amongst the lowest prices that had available information to allow us to make the purchase. It just so happens that the results of our tests show that for the 13 purchases that we have made to date, 12 have come from Shenzhen, China and one from Beijing.

Chairman LEVIN. How much time elapsed between the time that the GAO's fake company, that you created, requested the parts with the bogus part number and the time that you actually received the bogus part? Is that a matter of days, months, weeks?

Mr. HILLMAN. It is a matter of days, Senator. We made purchases and waited for approximately a 24-hour period, sometimes a little longer, to obtain quotations of individuals willing to supply us these part numbers. Upon receiving information from the lowest price bidders on available information with which to make the payment for these purchases, it could have taken from several days to a little over a week for the purchases to actually arrive.

Chairman LEVIN. How did you pay for the parts?

Mr. HILLMAN. We contracted with the vendors through Western Union services to supply the funds for the purchases.

Chairman LEVIN. They were wire transfers?

Mr. HILLMAN. Wire transfers.

Chairman LEVIN. Did you find that there were any operators/counterfeiters that were working more than one company? In other words, did one person, as far as you can say or tell, have more than one company? Was there like a boiler room anywhere?

Mr. HILLMAN. It appeared from the results of our discussions over the Internet that there were individuals with similar names that were supporting multiple vendors that were willing to supply us these parts.

Chairman LEVIN. Mr. Sharpe, you do independent testing—right—at one of your companies that you are affiliated with.

Mr. SHARPE. Yes, sir, we do.

Chairman LEVIN. When you did the testing here on the parts I guess with GAO, did you know who you were testing those parts for?

Mr. SHARPE. We only knew that we were testing them on behalf of GAO.

Chairman LEVIN. You did not know that it was for this committee, though.

Mr. SHARPE. No, sir.

Chairman LEVIN. You sell parts too.

Mr. SHARPE. The biggest part of our business.

Chairman LEVIN. Can you compare the way you saw parts being handled in China with the way you handle parts that you sell?

Mr. SHARPE. There are really no words to describe it. Watching parts literally being washed in rivers, dropped on riverbanks, dumped into cardboard boxes. There was nothing done whatsoever to protect the component at any phase of what we saw going on over there. If anything, the entire process would serve to ruin the component. The processes that are followed by SMT begin with strict ESD controlled rooms and areas, clothing by our employees. The areas are dehumidified, kept between a relative humidity level of between 25 percent and 45 percent not only where we work on them but where we store them. All packaging is ESD compliant and tested. It is a completely different world.

Chairman LEVIN. What impact does the way electronic parts are handled have on performance and reliability?

Mr. SHARPE. Well, in the case of the parts that we saw in Shantou that were either on the sidewalks or in the river, for instance, one of the biggest enemies of an electronic component is moisture. So there is absolutely no safeguards whatsoever to stop moisture ingression into the components. Moisture ingression into the components leads to delamination and die voiding, things that begin to become the beginning of the end. When we look at parts at SMT through an acoustical microscope, we can see the evidence of that moisture ingression, and on parts that are counterfeit, that is a very prevalent thing for us to see.

Chairman LEVIN. In other words, the lifespan of the part is dramatically affected by the way in which they are handled?

Mr. SHARPE. Absolutely.

Chairman LEVIN. When you were there, did there appear to be any steps taken by the Chinese Government to stop the sale and the marketing of these parts? I mean, the Chinese tell us they act against counterfeiters. That is what they tell us. We got a statement today from the Chinese or they issued a statement to the press that they are always taking action against counterfeiters. Did you see any evidence when you were there of any Chinese Government action against what was openly being sold as counterfeits?

Mr. SHARPE. No, I did not. When I was in the Shenzhen marketplace, the parts that were there—the interpreter was reading to me cards that were inside of the showcases where it was describing what level of refurbishment had taken place as they were regarded. This was all right out in the open. When we got into the City of Shantou, the entire business purpose of everything that we saw there was very obviously to harvest components from e-scrap and go through complete refurbishment right there in the open. There was nothing that was hidden.

Chairman LEVIN. Thank you.

Senator McCain.

Senator MCCAIN. Thank you, Mr. Chairman. I thank the witnesses. Mr. Hillman, how serious do you think this problem is?

Mr. HILLMAN. The results of our work to date is based off of a non-generalizable sample of parts that we were requested to purchase. Therefore, we are unable to discuss the prevalence of this activity.

Senator MCCAIN. But it is a serious problem, not so serious, a waste of your time?

Mr. HILLMAN. No, Senator, not at all. We consider the problem itself to be a very serious one, possibly affecting the lives of our military personnel and the capabilities of the systems that they utilize.

Senator MCCAIN. Mr. Toohey, do you agree with that assessment?

Mr. TOOHEY. Yes, absolutely. This is a very, very serious and growing problem, Senator.

Senator MCCAIN. So, Mr. Toohey, what do we need to do about it?

Mr. TOOHEY. Well, Senator, I outlined a number of steps briefly that I think we ought to continue and expand. Certainly working to strengthen the authentication procedures, and we are working in a cooperative way with DOD officials to do this. I think ensuring that that process continues and is strengthened makes sense.

Ensuring that the procurement system is strengthened so that for these mission-critical components, they are only purchased through authorized distributors or DOD-certified resellers. That would be a critical——

Senator MCCAIN. We are doing that now. People are getting certified to be a reseller, but obviously there is very little scrutiny or examination of the people who are getting this certification. Would you agree, Mr. Hillman?

Mr. HILLMAN. There are certainly on the Internet purchasing platforms that we observed a wide variety of attesting or lack thereof associated with the parts that are being made available for sale.

Senator MCCAIN. Mr. Sharpe, we have been told by a number of independent distributors and testing laboratories that more often than not, semiconductor manufacturers refuse to assist them in determining the authenticity of an electronic part. Has that been your experience?

Mr. SHARPE. We have seen it both ways, sir. We generally try to reach out to the component manufacturers to get information on die markings, information on the front markings, things like that on obsolete parts so we do not have data on——

Senator MCCAIN. Sometimes you do not get the cooperation of the manufacturer.

Mr. SHARPE. Sometimes we do not.

Senator MCCAIN. Mr. Toohey, what have you got to say about that?

Mr. TOOHEY. Well, Senator, our companies work very closely with Government officials. As a matter of fact, one of the steps that I——

Senator MCCAIN. So you do not agree with Mr. Sharpe's assessment.

Mr. TOOHEY. Senator, we work very closely with Government officials and cooperatively work——

Senator MCCAIN. Do you agree or disagree with Mr. Sharpe's assessment?

Mr. TOOHEY. Senator, I think our industry has an outstanding record of working cooperatively with both private sector and Government officials to authenticate chips. As a matter of fact, one of the steps that I recommended was changing a customs policy to allow us to cooperate because in many cases at the border, only the manufacturer can authenticate the chip, and right now, given the policy that is in place, we are not allowed to do that. So we do cooperate and we would like to strengthen that cooperation, Senator.

Senator MCCAIN. Well, we would certainly like to help you in that effort.

Mr. Hillman, have you been involved in this issue at all, that some of the laboratories and testing distributors are not—people are not given assistance by the semiconductor manufacturers?

Mr. HILLMAN. Results of our investigation to date have not led us into that area.

Senator MCCAIN. Which means to you in terms of your investigation?

Mr. HILLMAN. In terms of our investigation, we have shown that it is possible to purchase counterfeit parts on Internet purchasing platforms. We have not, as part of this ongoing work, delved into the potential issues that exist currently within those platforms or across the supply chain but hope to be doing additional work as part of the ongoing investigation.

Senator MCCAIN. Mr. Toohey, Mr. Sharpe and others have given us information that the manufacturers many times refuse to assist. I suggest you get on that, and I suggest you get on it quickly. We will be glad to consider legislative changes but if manufacturers are not cooperating, it makes the problem even worse. So I hope you will look at these allegations, find out if they are true or not true, and if they are true, get to work on it.

Mr. TOOHEY. We will absolutely do that.

Senator MCCAIN. Mr. Sharpe, how long has this been going on in your view?

Mr. SHARPE. I have been in the industry for 15 years and I have spoken to folks who have been around the industry since the 1960s and they said they have seen counterfeits going back to the 1960s.

Senator MCCAIN. Is it growing worse, better, or the same?

Mr. SHARPE. It is growing much worse, and the reason why I call it much worse is that the counterfeiters are changing their processes to get in front of the processes that they know that we are currently doing to detect their processes. So the process is evolving and it is getting harder to detect.

Senator MCCAIN. So really it would be extremely difficult to stop this unless we get the active cooperation of the Chinese Government.

Mr. SHARPE. I would agree with that, yes, sir.

Senator MCCAIN. There is very little doubt in your mind that the Chinese Government is aware that this significant industry is taking place.

Mr. SHARPE. Absolutely no doubt.

Senator MCCAIN. Have you ever had a conversation or heard anything from the Chinese Government about this?

Mr. SHARPE. No, sir, I have not.

Senator MCCAIN. Have you, Mr. Hillman?

Mr. HILLMAN. No, sir, I have not.

Senator MCCAIN. Mr. Toohey, I am a great admirer of your association and its members and the enormous contributions that they make to America's economy, but I suggest you give this some priority so that members of this committee and the American people can be assured that there is active cooperation on your part. Okay?

Mr. TOOHEY. Yes, Senator.

Senator MCCAIN. Mr. Hillman, again I have read reports of the desk and the phone, the middle person who basically is just the pass-through, and part of it is because of our encouragement of small business people being able to be involved in DOD procurement. How serious is that part of the problem?

Mr. HILLMAN. Well, we all value the participation by small businesses. In this instance, though, on this investigation, what we have learned in several purchases that we have made is that individuals are posing to be representatives of multiple companies and are willing to supply parts to us that are not authentic where no actual part numbers exist.

Senator MCCAIN. I thank the witnesses. Thank you, Mr. Chairman.

Chairman LEVIN. Thank you very much, Senator McCain.

Senator Udall.

Senator UDALL. Thank you, Mr. Chairman.

Let me first say I think the most important and sobering thing that I have heard is that this is a serious and growing problem. I would like to build on the comments and the questions the chairman and Senator McCain have asked.

I think Senator McCain really put his finger on it here. We need a team effort. The Federal Government and industry have to work together. Mr. Toohey, I look forward to hearing the results of your increased focus in this area as you acknowledged this morning. I am not here to pick on you per se, but I do think this is something that has really gotten the attention of the committee. To my way of thinking, there are roles that the State Department and Customs and Border Patrol (CBP), component manufacturers and suppliers alike can play. It does not seem like there is one solution but it seems like there are a number of relatively simple solutions that we could provide that would, in turn, provide a screen to get at the heart of this.

Let me get into more detail. I think there is something called the Trusted Foundry Program (TFP), and it is a joint DOD–NSA program that ensures that only certified chips and microprocessors are allowed into the supply chain. But as I understand it, we do not require components to be certified through the TFP.

If I could, I would like to ask the industry experts here, would there be any benefit to requiring electronic components to be certified as TFP-compliant before they are allowed into the DOD supply chain. Would a trusted supplier certification requirement not protect manufacturers and the DOD alike? Given that we are spending billions on the fake components, would the investment in

such a certification program not pay for itself in a fairly short period of time? Mr. Sharpe, maybe we could start with you and Mr. Toohey in turn.

Mr. SHARPE. Senator, so I understand the question as it is posed to me, is it that I would send parts to this program to have them certified before I was to send them in to DOD?

Senator UDALL. I think that is in part what I am getting at, but we are basically taking suppliers at their word for the authenticity of the components they provide even though it seems that the suppliers cannot always say for sure where those chips come from. But we do not know how many other systems, whether they are in vehicles or part of the radio and coms efforts we put forth. Aircraft, weapons systems themselves could be at risk of failure. So it seems like we have to go the extra mile here. Again, I am searching, as I think the committee is, for ways to get at this quickly and in a cost-effective manner.

Mr. SHARPE. Well, as far as the TFP goes, as I understand it, this is a group of foundries where material can be built directly for the Government with no brokers in between. So this would be an area where an independent distributor would not have any access to, as far as I know, unless we were to ask them to do work for us. But generally, this is direct from them to you.

As far as product coming from the independent channel, we all know that due to the huge amount of obsolescence that becomes part of weapons systems, that lots and lots of material has to come from our industry, meaning independent sector.

I personally believe that the way into this to mitigate it properly is for heavy requirements on testing being done by the supplier, and I am talking about documented proof of all tests. I will not run through the whole list, but there is an awful lot out there that can be done, including full electrical. This is now being done and required, by the way, by many of the primes that we currently deal with.

Senator UDALL. Mr. Toohey, I would welcome your comments.

Mr. TOOHEY. Senator, as you very well noted, this is a multipronged problem and it will require a multifaceted solution. In that regard, part of the solution is certainly continuing the work that we are doing with DOD for the authentication process and ensuring that that process works and so that manufacturers can very easily authenticate chips that are in the supply chain.

The TFP also plays an important role for a relatively minor part of what the DOD procures, but I understand that process is being reevaluated as well. So I think there are many parts of the solution that we ought to implement in order to ensure we know which chips are going into the DOD supply chains.

Senator UDALL. Could I turn to the Chinese Government? What more can we do? What should we be doing to encourage them, shall I say, to stop the flow of these fake components into the United States? I would welcome any of you on the panel to comment.

Mr. SHARPE. Since the Chinese Government is so well aware of what is going on as far as the counterfeiting in the country, it would seem to me that they could get a handle on this rather quickly if they were to make that effort to do so. Since everything is out in the open, I believe that China can put the right restric-

tions and penalties in place within their own country and stop an awful lot of this right at the bud quickly. So that is the way I would see it.

Senator UDALL. Mr. Toohey, do you have further thoughts?

Mr. TOOHEY. Certainly more can be done in China to stop counterfeiting and enforce intellectual property, although I would note that our association has been working with Chinese Government officials both at the state level and the provincial and local level for quite some time on this problem. For example, part of our work was the establishment of a legitimate market in Shenzhen so that there is a legitimate way in which to procure legitimate chips, and that has been established.

The Chinese Government, certainly during the special campaign implemented earlier this year, has demonstrated that when it focuses, it can have real results. Semiconductors were not part of that special campaign on intellectual property enforcement, but those industries that were involved, pharmaceuticals and others—and officials from the U.S. Embassy also indicated that there was strong progress. So I think having our trade officials and our bilateral relations encouraging stronger enforcement is the right way to go, Senator.

Senator UDALL. Mr. Hillman, do you have any insights into this counterfeit market in China and the Chinese Government's role? Are they simply turning a blind eye or is there evidence of complicity?

Mr. HILLMAN. That is nothing that our investigation has uncovered to date. We will be continuing our investigation and reporting our final results later this year.

Senator UDALL. Did your investigation determine that any of our servicemembers had been injured or that there was loss of life tied to these counterfeit chips?

Mr. HILLMAN. The parts that we have purchased that were authentic fit into a variety of significant military applications. The results of our investigation to date suggests that those parts can be purchased on a counterfeit basis. We have not gone to the extent to determine whether counterfeit parts have actually been placed into those systems, therefore, whether or not lives have been endangered.

Senator UDALL. Let me end with a comment tied to your answer and my question. I think that is why this committee is so concerned. Our servicemembers face enough peril, put themselves on the line day in and day out, and if there is an unseen danger tied to the electronics on which we depend, this is a very, very serious situation.

So, again, we have work to do. We are going to have to do it as a team, DOD, this committee, the private sector. The Chinese Government has an important role to play here.

So thank you again for your appearance. Mr. Chairman, thank you.

Chairman LEVIN. Thank you, Senator Udall.

Senator Brown.

Senator BROWN. Thank you, Mr. Chairman.

Mr. Chairman, I had a question back to you. I want to make sure I understood what you said. You indicated in your initial statement

that we are obviously paying for product, and then we, in turn, have determined that those products are being supplied with defective materials. Then not only are we paying for the product in the first go-round, did you say also we are paying for the replacement and repair of those defective——

Chairman LEVIN. Depending on the contract. There is evidence. We will hear more about that on our second panel. But the example I gave, yes, we paid for the repair because it was a cost-plus contract, and unless you can prove intention, that something is intentionally counterfeit and with knowledge, then we end up paying for it. That is something we can change.

Senator BROWN. Well, count me on the amendment that does that as a cosponsor because it only makes sense here on Capitol Hill that we would do something like that, Mr. Chairman. The fact that we are paying top dollar for a product and then, in fact, we get the product and it is filled with sometimes defective components is mind-boggling.

Chairman LEVIN. We can correct it on Capitol Hill, but the problem is the contracts the Pentagon enters into, if they are cost-plus contracts, do allow and maybe require that the Pentagon pay for replacement unless you can prove that the defective part was put in knowingly by the contractor.

Senator BROWN. We should not have to make that proof. It should be a given that everything that we pay for is of the highest quality.

Chairman LEVIN. That is what our amendment will do.

Senator BROWN. Thank you, Mr. Chairman.

Also, Mr. Hillman, you said the middleman—you described it when you went out and did your research and kind of your sting operation. You provided them with numbers that were not real, and in fact, it came back with some fictitious product. Is that a fair statement?

Mr. HILLMAN. Yes, Senator.

Senator BROWN. What has been done to those people? Have they been let go? Are you not doing business with them anymore? I mean, what does it take to stop doing business with people like this here in Washington?

Mr. HILLMAN. We will be referring the results of our investigation to the Inspector General (IG) of DOD for further review and potential action.

Senator BROWN. With a recommendation, I hope, to terminate any and all contact and recoup any and all payments. Is that a fair statement?

Mr. HILLMAN. Yes, Senator.

Senator BROWN. Thank you.

I mean, this is another reason to not only manufacture in America but buy American so we know what we are getting, we know where the supply chain is going. To rely on entities like you have described, Mr. Sharpe, through your investigation—how did you actually get into the country to do that when we had representatives that were denied? Did you go over like, oh, golly, gee, I want to see what they are doing and maybe have an opportunity to buy some more product? How did that work? I am curious.

Mr. SHARPE. We do not buy product over there, Senator. The trip began as a business trip to visit a U.S.-based customer in Hong Kong that was then to turn into a vacation in Beijing, and it was 2 weeks before the Olympics in 2008. The borders were very porous. When I got into Shenzhen, not knowing that I was going to then be traveling the next day to Shantou, it was nothing more than paying some money to the driver and hiring someone to take me out there. There seemed to be no issues whatsoever. No one really questioned me. There were just areas where I was told that I could not take photographs.

Senator BROWN. I share Chairman Levin and Ranking Member McCain's concerns. From 2005 to 2008, counterfeit incidents have almost tripled possibly as a result of, quite frankly, the manufacturers failing to adhere to the testing requirements. Do you think that is the reason?

Mr. SHARPE. Yes, that is a reason, sir. I agree with that.

Senator BROWN. A lot of the recommendations that you have made and I think, Mr. Toohey, you are making you feel it would change that?

Mr. TOOHEY. Yes, Senator. We believe it would significantly help to strengthen the authentication procedures, to strengthen the procurement policies, to ensure that we are stopping these at our border and ensuring we are using all tools available, and to leverage our law enforcement community as well to continue to aggressively prosecute these——

Senator BROWN. Mr. Toohey, are you giving recommendations to the chairman and ranking member on what you need in terms of legislation to get that done? Are you doing that?

Mr. TOOHEY. Senator, we would be happy to follow up with a more detailed set of proposals.

Senator BROWN. Yes. I would like to be included in that because, quite frankly, I find this—this is unbelievable. So I want to really thank you both for pursuing this. It came out of left field and another thing we have to worry about.

I guess take a shot, any one of you. What is your thought about the likelihood that everything that has been done is malicious in fact, not just out there to make money, but malicious in terms of trying to deliberately breach our DOD equipment and try to gain some type of tactical advantage? Is there anything like that going on, or is it just really, hey, they are just going out to get money just to make money? That is my first question.

My second question is, so why do we not go to the source? Is there a different way we can process a lot of this waste? We can do it internally. Do we not have the ability to do this stuff within our country? Take that supply chain and just cut it off at its head. I mean, it makes no sense to me that we are sending this stuff over there in barges and then they are able to do what they are doing. It is clear from the pictures. I mean, did anyone send over this investigation to the embassy here—the Chinese Ambassador and say, hey, sir, can you explain what is going on here?

So I guess there are a couple of questions in there. Do you think there is any malicious intent to deliberately breach our DOD equipment, number one? Number two, is there a different way we can do it to stop the supply chain from going over in the first place?

I cannot believe America, one of the greatest countries in the world and one of the most innovative countries in the world obviously, cannot do more with this waste.

So anyone can take a shot at that. Dr. Persons, you have been silent. Why not take a shot at one of those?

Dr. PERSONS. Thank you, Senator.

In terms of understanding any malicious intent, sir, that was out of scope of our particular investigation which is still going on. In terms of dealing with those things, GAO has done reports on e-waste and recycling and so on, just that general issue and the legitimacy thereof. I believe the core issue or one of the core issues has to do with just who wants that to happen in their proverbial back yard and who pays for that and that sort of thing.

Senator BROWN. It seems like the American taxpayers are paying indirectly by the fact that we are double paying for equipment that we should be getting that should be top of the line in the first place. Then we are paying by the potential breaches in our security in the way that we are providing equipment to our men and women that are serving. My time is up. I appreciate your holding this, Mr. Chairman.

Chairman LEVIN. Thank you, Senator Brown.

Senator Manchin.

Senator MANCHIN. Thank you, Mr. Chairman.

This will probably be to Mr. Sharpe or Mr. Toohey. Do you know of any Chinese company or government agency that makes any product that they have researched, designed, done the research and brought it to market, that no other country does right now or no other company outside of China does? Do you know of anything unique that they have brought to market in your realm of business?

Mr. SHARPE. I am not aware of any, Senator.

Mr. TOOHEY. Senator, there are a number of domestic Chinese semiconductor manufacturers and design companies. There is a legitimate foundry, a very——

Senator MANCHIN. I am saying do you know of anything they have, let us say, invented?

Mr. TOOHEY. Senator, there are some specific applications, semiconductors, that have been designed in China. There are a couple of good foundries that manufacture quality products, some for American companies even, in China. So while it is very small—the domestic industry is extremely small—in world standards there are examples of research. I should add that the Chinese Government has singled out the semiconductor industry in their 5-year plan as one that they want to build because they know what it means to our country. So they are putting a lot of investment into developing a domestic semiconductor——

Senator MANCHIN. How many of your members have a presence in China?

Mr. TOOHEY. Several of our members, Senator. Several of our large members have a presence in China.

Senator MANCHIN. So it would be right for us to understand that you would be concerned about their protection, also an ability to do business there.

Mr. TOOHEY. Yes.

Senator MANCHIN. Are they there because of price?

Mr. TOOHEY. Senator, it is a global market. China is actually the largest market for semiconductors globally. Not a lot is produced by local companies I mentioned, but they are actually the largest market and that drives many of our international global companies to have presence in China.

Senator MANCHIN. Are we still purchasing these products as a Government? To Mr. Hillman or Dr. Persons, are we still as the U.S. Government for our DOD purchasing, doing business with these people?

Mr. HILLMAN. The parts that we have been purchasing as a part of this ongoing investigation are rare, hard-to-find, and obsolete parts that are still being utilized in major weapons systems. The Internet purchasing platforms demonstrate that contractors or subcontractors that are in need of these hard-to-find, rare, obsolete parts have an outlet through these purchasing platforms to acquire these parts. The concern, though, is that the intent to deceive certainly exists and——

Senator MANCHIN. Are we still purchasing, sir? I just asked a very simple question. Is the U.S. Government still purchasing from these counterfeiters who are putting out inferior products?

Mr. HILLMAN. The Internet trading platforms have 40 million to 60 million line items and parts that are purchased on a regular basis. Yes, sir, Senator.

Senator MANCHIN. So we are still doing business with the people that we know that are making inferior products that could affect our service people.

Mr. HILLMAN. Those businesses certainly continue to be available to——

Senator MANCHIN. Mr. Sharpe, if I may ask you. Your company basically does this after-market. Right?

Mr. SHARPE. Yes, sir, we do.

Senator MANCHIN. Do you know of any companies other than yourself or other companies like yourself that are unable to produce the quality products that are needed for our service people?

Mr. SHARPE. Well, we do not make products over at SMT, but we produce products that have been inspected properly.

Senator MANCHIN. Right.

Mr. SHARPE. Yes. There are other companies in the United States like ours.

Senator MANCHIN. So we would not have to go to China to these counterfeiters if we did not want to because of price.

Mr. SHARPE. We absolutely do not need to go to China.

Senator MANCHIN. Okay.

Who writes the specs? Mr. Hillman, who in the world in our Government writes these specs for these products and does not follow up? The specifications for what we are going to purchase is not written stringent enough that if you basically do not meet those specifics, then you are banned, like in any other purchaser, from State purchasing or Federal purchasing. You should be banned if you are found to be neglective of doing what was supposed to be done. Who would want to answer that?

Dr. PERSONS. I will answer that, sir. In the context of our work, there is a DOD specification. It is called MIL-PRF–38535J in terms

of the context of the tests that we ran on the various parts that we acquired in our undercover operation. There are specs being written——

Senator MANCHIN. Who writes the specs? I mean, does the Government? I am sure we have spec writers. Right?

Dr. PERSONS. Yes, sir.

Senator MANCHIN. From all different agencies, DOD agencies?

Dr. PERSONS. In this case, this was a DOD specification. So I am sure there are others.

Senator MANCHIN. Who follows up on that? We have you all in here to basically check to see if this type of a scam was going on. We found out it was not only going on, it was flourishing. It still is flourishing as we are here at this committee hearing right now. It seems to me you get back to the source. If we are writing the specs, who is following up? Why would you let it get that far? You could shut that down in a heartbeat.

Dr. PERSONS. Sir, I am not aware of who is supposed to follow up, but I do know the specification does exist and is written by, in this case——

Senator MANCHIN. Well, does anybody in DOD—have you brought your report to anybody in DOD?

Dr. PERSONS. Because it was preliminary, no, sir.

Senator MANCHIN. They did not request it all. It was basically this committee that did.

Dr. PERSONS. Yes, sir.

Chairman LEVIN. If I could just interrupt for one second. This was a very specific report that we asked the GAO very recently to try to go on to the Internet and to see what parts would show up when they put in orders, and the cheapest parts that showed up from—they are all from China—turned out to be counterfeit although it had been tested. Some of the numbers that were given to them were totally fake numbers. So they have just been involved working for us very, very recently. We are going to have a third panel here where we are going to have contractors for which those questions would be very——

Senator MANCHIN. Mr. Chairman, the only thing—this is not rocket science. Basically I do not know if they have had an original idea or brought a product to market that would benefit mankind, if you will, from China. Everything from the handbags to watches to mining equipment—everything has been basically stolen by them as far as property rights and those types of things.

I just cannot figure out if we are getting bad product and we know where it is coming from, why do we not shut it down. I think that is the question that you would ask later. Why did DOD not jump in and say, listen, we are paying and getting bad products, inferior, we are buying and paying for it twice to try and get the right product, and we are putting people in harm's way, especially our military people? Why would it take us as a committee? Why would DOD not have an internal audit asking for this?

You were not asked, Mr. Hillman, by DOD at all to check this out? Did they know they were getting inferior products?

Mr. HILLMAN. We are releasing preliminary results of our ongoing investigation this morning and have not had contact with any other outside party associated with these products, other than the

DLA, in order to determine whether or not the parts that we were purchasing were being integrated into major weapons systems and to determine that the bogus part numbers that we were attempting to purchase were not an authentic part.

Senator MANCHIN. Thank you.

Chairman LEVIN. Thank you, Senator Manchin.

Senator Ayotte.

Senator AYOTTE. Thank you, Mr. Chairman. I wanted to follow up with what Senator Manchin said. As I understand it, Mr. Sharpe, you said in your view we do not need to go to China. Can you explain that?

Mr. SHARPE. There is an awful lot of product over in China that is certainly not counterfeit. Going to China to buy from the non-authorized sources is a sure way, as far as we can see right now, to get ourselves into trouble. There are authorized sources in China that get products directly from the authorized component manufacturers. I would not say that dealing with those folks, as long as they are selected and audited, would not be a reason why we could not buy from them. But the open market of China is definitely not a place to go.

Senator AYOTTE. I certainly appreciate that we have a need to trade and to trade with China. However, they seem to be flaunting our intellectual property laws. They, obviously, in this instance, the counterfeit products—let us just be clear. It is a matter of life and death with these products. When I see that some of these counterfeit products—if you are a Navy helicopter pilot or an Air Force C–27J pilot and you cannot trust your flight system or your night vision capability, I mean, this could be a matter of life and death, could it not, for our soldiers?

Mr. SHARPE. Yes, Senator.

Senator AYOTTE. It seems to me that when we know that there is a particular area of China, Shenzhen, that is producing, openly producing, these counterfeit products, why would we even allow those products to come across our borders to get into our supply system.

Mr. SHARPE. It is a very good question. If it is coming from the open market, I agree.

Senator AYOTTE. In my view, I think we need to send a stronger message to China rather than trying to continue to talk when the response we get back is, oh, we are taking care of this and clearly they are openly allowing this to happen. It is a matter of life and death for our soldiers. I hope that we will take stronger actions to cut them off.

As a follow-up, I wanted to ask—one of the concerns that I have had since I have been a member of this committee—Chairman Levin talked about cost-plus contracts and how they could expose U.S. taxpayers to the cost of replacing counterfeit or fraudulent goods. We are basically paying both ways for this. That is one of the reasons why Senator McCain and I—certainly we have introduced legislation to minimize the use of cost-plus contracts. But, Mr. Toohey, can you tell me why should the contractors not bear the risk here within the supply chain for counterfeit products?

Mr. TOOHEY. Well, Senator, from our perspective, everything ought to be done that can be done to ensure that legitimate product

is going into these products. While I am not very familiar with the details of defense contracting, it seems like a reasonable approach to expect companies and contractors to do everything they can to ensure that these products are legitimate.

Senator AYOTTE. So you would agree with me that taxpayers should not have to pay twice for the goods and obviously the important military equipment that we are paying quite a bit of money for.

Mr. TOOHEY. Certainly when measures can be done and policies that can be put in place to better ensure the authentication of these products, I would certainly agree, Senator.

Senator AYOTTE. The other issue I wanted to ask you about—you mentioned the case of VisionTech which was a prosecution in Federal court to address—aggressively prosecute the counterfeiting traffickers. I believe you identified it as a first case of its kind. Why is that? Why are we not prosecuting more of these cases? Because if we prosecute people who are putting these products in the line and obviously know that they are trafficking in counterfeited products, that will also be a great deterrent particularly to contractors within the United States.

Mr. TOOHEY. Senator, I could not agree more. We ought to be aggressively prosecuting these criminal entities, and that is what they are. They are criminal entities that are putting the lives of our soldiers at risk.

I should say my understanding is VisionTech is the first felony conviction for it. There are several other pending cases. But from our perspective, the work of the U.S. Attorney here for the District of Columbia and specifically the assistant U.S. Attorney, Sherri Schornstein, in this regard and really single-handedly sort of forcing these cases and these prosecutions forward has just been extraordinary. It ought to be recognized and we need to do more of it as a country.

Senator AYOTTE. I could not agree with you more. I would like to see more felony prosecutions because we are talking about life or death decisions here. The more we aggressively prosecute these individuals, particularly if we find out that there is a contractor or a company in the United States that knows they are trafficking in counterfeit goods to our military that go into important parts that they have—equipment that they have to rely on, I can tell you that that will also be a way to stop them.

Mr. TOOHEY. Senator, if I could just add, we cooperated closely with the U.S. Attorney on those cases and on a number of other cases, and we stand ready to strengthen that. It needs to be a partnership to authenticate which chips are counterfeit. We have a very strong cooperation with law enforcement officials here, and we would like to strengthen that.

Senator AYOTTE. Mr. Hillman, I believe Senator Brown asked you a question about—one of the issues that leaps to mind for me about this—now it seems to be a profit motive. These cases seem to be the Chinese trying to make money off of us and other countries, but primarily the Chinese are participating in this. But if it is that easy to do this, could this not also easily become a way for sabotage to be conducted on our military espionage? Is this something we should be concerned about not only as something that is

undermining and putting our troops at risk with the equipment they are using, but in the context of our national security?

Mr. HILLMAN. There certainly is the possibility that there could be counter-motives other than financial benefits associated with the counterfeiting and harvesting of old parts put into a fashion that they appear to be new. The vendors that we have purchased these parts from appear to be more of a boiler room operation where they are willing to supply parts of unknown authenticity for the remuneration that is provided from those parts.

Senator AYOTTE. But certainly this represents a vulnerability that goes—could be far-reaching if we do not address it within DOD.

Mr. HILLMAN. I agree.

Senator AYOTTE. Thank you.

Chairman LEVIN. Thank you, Senator Ayotte.

We will have a chance in the next few weeks, when our bill comes to the floor, to take some statutory legislative steps, which I hope we will all be able to support. At any rate, we will have that opportunity that you made reference to. So we thank you for that.

Senator AYOTTE. I appreciate your leadership.

Chairman LEVIN. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman. Mr. Chairman, let me start by thanking you and the ranking member for conducting such an in-depth investigation into such an important problem.

I would point out that this problem is not a new one. I recall back in 2004 looking into this issue of the security of the supply chain. At that time in 2004, DOD initiated the TFP, which Senator Udall referred to. This program was intended to ensure that mission-critical national defense systems have access to trusted parts and assured supplies. Under this program, DOD actually accredits suppliers that provide microelectronic design, manufacturing, and assembly services to meet certain standards to ensure the integrity and the reliability of the product.

I happen to be familiar with this program because one of the trusted foundries is in South Portland, ME. It is now operated by Texas Instruments. It used to be National Semiconductor.

So my question is, what happened to this program? Has it not worked as well as was hoped back in 2004 when it was launched by the Pentagon? Should Government and the owners and operators of critical infrastructure be making better use of these trusted foundries? What is your assessment?

We will start with you, Mr. Toohey, and then go down the panel.

Mr. TOOHEY. Well, Senator, you very well pointed out the TFP is a very important system that allows certain mission-critical items, especially new items to go into the DOD supply chain in a very assured way.

In many ways what we are talking about here are parts that are no longer manufactured and are replacement parts for systems that have been in place for many, many years. That is an area that, at least from my understanding, the TFP does not deal with. I think just given the increasing amount of semiconductor content in so many different products, civilian products and defense products, probably a single solution is not going to do it. There does

need to be a broader solution to authenticate in partnership with the TFP.

Senator COLLINS. Well, I guess my reaction to that is similar to the point that Senator Brown raised which is maybe we should look at where we are buying these parts and reconsider the manufacturing of those parts in the United States. We do have the capability, and if the problem of counterfeiting is that high and if, in fact, it is causing us to pay twice for the same part, then perhaps we should look at not only the integrity of the supply chain but whether we are dealing with reputable countries as sources for vital equipment.

Mr. TOOHEY. Senator, if I could just add. In many cases these counterfeiters are remarking these products. So they may appear as if they were made in the United States. So that is clearly part of the problem. From a third party, these criminal enterprises like VisionTech present these products as certified military spec products, and that is all just fake. That is a big part of the problem.

Senator COLLINS. Actually that leads me very well into my next question. So I still want to hear the rest of the panel's assessment of the TFP, but let me first go to my next question.

Mr. Toohey, in your written testimony, you noted that the CBP agency plays an important role in anti-counterfeiting efforts by notifying trademark owners of suspected shipments that are coming into our ports.

Now, previously this effort by CBP included sending photos of seized chips to the original industry manufacturer, and they could assess whether or not they were legitimate chips or whether they were counterfeit. But I understand that CBP officers have now been given revised guidance to redact the identifying marks on the chips in the photographs except for the trademark. I have to say that makes no sense to me whatsoever because they are redacting information that would allow the manufacturer to assess whether the chip is legitimate or not.

What is your judgment on the change in policy?

Mr. TOOHEY. Well, Senator, you articulated it very well. It was a system that for many years worked very well. Especially now where counterfeiters have very advanced marking techniques, it is almost impossible to tell just by visual inspection whether a chip is counterfeit or not. Really the only way is with the code that is on the chip, and our companies can instantly identify whether that is a counterfeit or an authentic chip—instantly. It is a process that worked very well for many years.

As a result of an interpretation inside CBP, they have changed that practice, and we have been working very hard to encourage them to revert to the practice of sharing those codes. It is virtually the only way that our customs officials can stop a suspect chip and know whether or not it is counterfeit at the border—the only way. We have been really asking anyone who will listen to us about how we can work with CBP to change that policy to allow us to stop these chips at our border. We talked about the industry cooperating. We stand very ready and we have been eagerly asking Government officials to let us help them. It is a policy change that in our view, Senator, needs to happen to protect our borders. We need to close our front door.

Senator COLLINS. Mr. Chairman, I would just note that that is a baffling policy change and one that I hope we can remedy.

I would like to very quickly ask the rest of our panel to comment on those two issues: the TFP and the change by CBP.

Mr. HILLMAN. As part of our ongoing investigation, the parts that we are purchasing are rare, obsolete, hard-to-find parts that would not be included in this trusted accreditation program. Although it is very clear that DOD continues to rely on parts that have old manufacture dates, something similar to what is being done for newer parts would be a possibility that could be considered for these older, obsolete parts as well.

Also, regarding the customs activities, for one of the purchases that we have received there was evidence that CBP did open up our package and reviewed the part that was there. There is no evidence as to what actually occurred as a result of that review, but it was stamped as being opened by our CBP.

Senator COLLINS. Thank you.

Dr. Persons?

Dr. PERSONS. Yes, thank you, Senator. In terms of the TFP, we are aware of that program although again in the scope of this investigation, the analysis of whether TFP would be appropriate and so on is just beyond the scope of our current work. So we do not have any information to share with you at this time.

Senator COLLINS. It seems like it is a good model.

Dr. PERSONS. Sure.

In terms of the CBP, it is the same thing. We did not evaluate CBP's processes and so on. So thank you.

Senator COLLINS. Mr. Sharpe?

Mr. SHARPE. Senator, the TFP, as I had mentioned before, really is not something that is part of what is available to independent distribution. That would be where Government is dealing directly with the trusted foundry. So I really would not have much to say there.

With regards to the redaction, I completely agree with being able to provide the component manufacturer with as much information as possible from what is being seen at the borders right now.

I will say that the most recent counterfeit report that we have released had a part in it that if the date code was correct, instead of being incorrectly stated, it would have most likely passed the scrutiny of a photograph from the component manufacturer as well. So that is the level of difficulty they are currently facing.

As far as the word "trusted" with regards to independent distribution, what we need to do is we need to get a group of trusted distributors whom are required to do over and above a significant amount of testing and have the abilities to do so. That is one of the biggest problems we have out there right now is there are lots of people who are in business and need to be in business, but they do not have the capabilities that are required to mitigate counterfeit parts as we see them today. There are some that do, but we need to identify who they are and use them and let the other ones who do not have that ability know what they need to do to get up to that level as well.

Senator COLLINS. Thank you. Thank you, Mr. Chairman.

Chairman LEVIN. Thank you very much, Senator Collins.

Senator Chambliss.

Senator CHAMBLISS. Thanks, Mr. Chairman.

Mr. Hillman, I will direct this first question to you, but if anyone else has a comment, I would appreciate it. What indication do we have that the Chinese Government is complicit in this counterfeiting operation?

Mr. HILLMAN. As part of our investigation, we have contracted with vendors to supply us part numbers, sometimes legitimate, sometimes totally bogus, and have found that they were willing to supply those parts. The extent to which the Chinese Government itself is complicit in these activities has not been part of our investigation, although it appears clear from the presentation from Mr. Sharpe that those activities are being undertaken in the open.

Senator CHAMBLISS. Mr. Sharpe, I assume, from what you said and what was just stated by Mr. Hillman, that you said about 40 percent, I believe, of the parts that you saw in the marketplace are estimated to be counterfeit. We have notified the Chinese of it. Basically they have done nothing. Is that your indication that the Chinese Government is complicit in this?

Mr. SHARPE. I would have to say that the local businessman who accompanied me—I am working off of what he said as far as the percentages go. I have heard also this information floating around from other folks as well. That is as good as my information gets with regard to that as far as just what the accurate percentage number is.

Regarding the Chinese Government knowing about this, it would be basically impossible for them not to know what is taking place in this marketplace and also in the nearby area of Shantou. It cannot be missed.

Senator CHAMBLISS. Mr. Hillman, your report was focused on the defense industry, and all of you have spoken with reference to that. I assume this is prevalent in every other agency of the Federal Government just as well?

Mr. HILLMAN. Yes. Counterfeit parts and other items that are produced on a counterfeit basis is something that impacts all industries.

Senator CHAMBLISS. Mr. Toohey, that would be the same for individuals going on the Internet and purchasing items such as this. Is that correct? Mr. Toohey?

Mr. TOOHEY. Excuse me. I am sorry, Senator.

Senator CHAMBLISS. I mean, anybody that goes on the Internet and buys these products is going to be subject to the same potential for purchasing counterfeit parts.

Mr. TOOHEY. Absolutely, Senator. This is an enormous problem that affects a broad range of industries and individuals from health care to automotive systems to airplanes mission-critical and non-mission-critical. Unfortunately, though, the biggest incentive is to sell into the most mission-critical systems because that is where the highest markup for these counterfeiters is. But it is a broad problem affecting many industries and it is a growing one, Senator.

Senator CHAMBLISS. In the January 2008 timeframe, a counterfeit chip was found in an F–15 flight control at Robins Air Force Base, and thank goodness it was found by the folks at Robins before it was ever installed. Subsequently, there were another three

or four chips that were found to be counterfeit. Do any of you have any information relative to that particular issue?

Mr. HILLMAN. No.

Senator CHAMBLISS. What other resources are there out there other than the Chinese that we know are counterfeit operators? What other countries are the potential resources?

Mr. SHARPE. Senator, we have seen Department of Commerce report, and it shows that there are many other countries that are involved in counterfeiting. There certainly is. It is just that probably the vast majority is coming out of China. We have counterfeiters right here in the United States, without a doubt, right now who are remarking product, and that is pretty scary to know that.

Mr. HILLMAN. For the purchases that we had made as part of this ongoing investigation, we did an analysis of vendors that were willing to supply the parts that we requested, and 79 percent of the responses came from East Asia. The remaining 21 percent were from Central Asia, Europe, North America, and the Pacific Islands.

Senator CHAMBLISS. Staggering.

Mr. Hillman, I listened to your description of what I basically guess you would call a sting operation that you set up. I also noted in a press report last month about a lady and her mother in Bakersfield, CA, just creating a company—just built it out of nowhere and got on some approved list and started delivering parts to DOD over a period of 3 or 4 years. So according to this report, $2.7 million worth of parts were purchased and sold to DOD, and they just got them off the Internet, just went and got numbers, and it turned out that a number of them were counterfeit. Obviously, action has been taken.

But I am astounded that you could carry out that operation with DOD. I look at it as certainly a problem on the other end, but there is obviously a problem on our end too with respect to how these companies like the company you created are able to get on that list.

What sort of recommendation would you have for us to think in terms of how we address that issue?

Mr. HILLMAN. In our investigation, we attempted to obtain membership on three different Internet trading platforms. Each of the three platforms appeared to have a varying degree of validation in order to determine the authenticity of our company. In one instance through social engineering when we simply talked to the individuals, we were able to pretty much gain access with very little background information.

In another instance when we gain access to a tracking platform, we were asked to provide references, addresses, Web sites, and other information. Based upon the results of our work to date, there was no indication that any of our references were checked or determine whether or not we were an authentic company doing a valuable service.

In the third instance, though, we were denied access to that Web site and they did not really explain their reasons.

Senator CHAMBLISS. Were you asked to give any financial references?

Mr. HILLMAN. Yes, we were asked to provide bank references as well.

Senator CHAMBLISS. How many transactions did you negotiate with DOD in that operation?

Mr. HILLMAN. DOD has not been made aware of our investigation. We are releasing preliminary results this morning.

Senator CHAMBLISS. Thank you, Mr. Chairman.

Chairman LEVIN. Thank you very much, Senator Chambliss.

We will just have a fairly brief second round.

Mr. Hillman, some of the numbers on these parts were real numbers that you were checking out. Some were phony numbers, and you got responses for both. But on the real numbers, those were for real systems. Is that correct?

Mr. HILLMAN. That is correct.

Chairman LEVIN. Those are systems that while they need replacement parts, still need parts.

Mr. HILLMAN. That is correct.

Chairman LEVIN. What systems were they? What weapons systems were those parts for?

Dr. PERSONS. Mr. Chairman, if I may, on the two voltage regulators that we purchased, that is a part that goes into the Air Force's KC–130 Hercules aircraft, also the Navy's F/A–18E Super Hornet fighter plane, the Marine Corps' V–22 Osprey aircraft, and then also the Navy's SSN–688 Los Angeles class nuclear-powered attack submarines.

Chairman LEVIN. Those parts may not be currently manufactured but they still must be currently acquired. Is that correct?

Dr. PERSONS. Yes, sir, that is correct.

Chairman LEVIN. That is the millions figure that our staff looked at millions of parts for the 1,800 cases that they looked at which is just a sliver of the problem. So even though these are, you say, "rare"—Mr. Hillman used the word—these are very important current requirements for these parts. Is that correct?

Mr. HILLMAN. That is correct.

Chairman LEVIN. Now, you said that 21 percent of the parts—or the inquiries or the responses that you got were not from Asia I believe you said, other parts of the world. Most do come from Asia and we all know from other testimony, the vast majority comes from China, and they are openly sold in China. But of the 21 percent not from Asia, many of those could be transshipment points, could they not be, for Chinese counterfeit parts?

Mr. HILLMAN. Yes, that is absolutely correct.

Chairman LEVIN. You do not know the origin of the parts by the fact that you got a response from a particular country.

Mr. HILLMAN. That is correct. Even for the parts that we purchased, oftentimes negotiating with individuals in certain cities within China, at the time that we received payment information, the addresses may have changed considerably, pointing to Shenzhen as the source for the payment as opposed to the manufacturing.

Chairman LEVIN. Mr. Sharpe, you made reference to three new processes that were released by DOD, and I was not sure, but I think they were testing processes. But I am not sure what you were referring to in your original testimony. Do you know what I am referring to?

Mr. SHARPE. Yes.

Chairman LEVIN. Can you explain that a little?

Mr. SHARPE. Yes, Mr. Chairman. I was referring to three test processes that were identified by SMT Corporation that were new counterfeit processes that we had not seen before.

Chairman LEVIN. Processes to try to determine what is counterfeit.

Mr. SHARPE. Processes that we knew the Chinese are now using on the parts themselves.

Chairman LEVIN. Got you.

Mr. SHARPE. So we did extensive reports on these three processes showing what they looked like, what the evidence is of them, and what is being used to create them.

Chairman LEVIN. We are going to act. We cannot rely on the Chinese to act. I think that has been proven for a long period of time. The Chinese say that they have an effort going on to act against counterfeits and it is baloney. They are openly sold. It is a growing problem.

On the other hand, as you pointed out, Mr. Toohey, some of our manufacturers manufacture in China, and so we can put into place a certification system that the supplier of these parts has been certified to be a legitimate supplier, whatever country might have the manufacturer. In China, there is a lot of counterfeiting going on. It is a clear and present danger, as one of you put it. It is a threat to our troops, and we are not going to let it go on.

So here is what at least I am going to be trying to do. We are going to try to put into place a requirement that DOD adopt a certification program for parts suppliers. While they are doing that, we have to defend ourselves. We cannot rely on the Chinese to take action against counterfeits. It has been going on too long. It has been pointed out to them too long. They are not cooperative. They will not even let our staff in, and so forth. We just cannot rely on them. So while we are telling DOD, which I intend to do in an amendment which I will offer, to require a certification for parts suppliers, that these are reliable suppliers, we have to at the border put in an inspection system for parts coming from China.

We do this with agricultural products. If we have a product coming from a particular place which we think will endanger our health, we have a ban on those products or an inspection system on products. We do it with dairy products. We have limits as to what dairy products can come in and so forth.

So what I also would be offering is that while we get a certification program in place, that we require inspection of all electronic parts coming in from China. It is a proven, known source of the problem. It is an epicenter of counterfeits coming into this country.

A third thing which we can do is to put some pressure on our contractors to go back up the chain or down the chain to make sure that the people supplying the supplier and the people supplying the supplier to the supplier, just going all the way down, are legitimate people. The only way I know to do that, other than just requiring contractors to so notify folks, is to make our contractors responsible to replace the parts. We cannot any longer have the Government paying for the replacement of these parts no matter what kind of contract it is. If the contractors are going to be responsible to replace parts which are determined to be counterfeit, we believe—I

believe—that they will take very significant steps to make sure that those folks down the chain are not buying counterfeit parts.

We can try to stop this flood—and it is a growing flood according to testimony—in two ways. One, we can try to get it at the source. I am determined and I think we are determined, and I know Senator McCain has spoken on this and other members have spoken. We are going to try to stop this at the source, but we cannot rely on it. So we have to take all the steps we can to put our fingers in the dyke while we are building the dyke at the same time. We are going to build our wall against counterfeits. We are going to, at the same time, have to put our fingers in the dyke by doing whatever we can that is reasonable, working with our contractors, using the systems which we have to notify the Government and other contractors through the system that we have put in place to make sure that that is used more often.

I guess my last question would be to you, Mr. Toohey, and to you, Mr. Sharpe. While we are asking our DOD to design a system of certification and to help design a requirement for inspection at our border of these parts that are coming in—and we are only talking about the parts that are coming in—we will need the assistance of the industry in trying to figure out how to do that. I want to do it quickly because I would like to offer an amendment, and I know I have a lot of cosponsorship. I would like to do that on this defense bill. So within the next week or so, would you be willing to help us with the actual wording of those provisions? Mr. Toohey, can your organization help in that?

Mr. TOOHEY. Absolutely, Senator. We would enthusiastically be willing to work with you. Let me just say we have been working with DOD to already begin this process of authentication. We want to strengthen that. We would be enthusiastic to work with the committee and ultimately with CBP to ensure that we are catching the parts that are coming in at our border. The industry is critical for that and we have for many years been a partner and we want to strengthen that partnership. So, yes, absolutely, Senator.

Chairman LEVIN. We will be calling on you. Mr. Sharpe, we will be calling on you as well.

Mr. Hillman, I think it is fairly clear now that your mission here was fairly recently given to you, and it is a mission which is a very important one, but it is kind of a limited mission. This is not a broader investigation where you have looked at a whole lot of things which you might have been asked about, but you were asked to see could you buy—what would be the response if you went on the Internet to buy parts. You did it and so far every single one where you have had a response is counterfeit and every single one of the seven that you know the origin of comes from China. That is pretty strong, clear testimony.

I was just wrapping up with this panel.

Senator MCCAIN. I want to thank them.

Chairman LEVIN. As I just mentioned, they are going to be working with us to try to design amendment language which we might be able to offer in the defense authorization bill on two things to try to build some kind of a certification system for parts suppliers so we can have real authenticity assured, and second, while we are doing that, to have an inspection requirement for parts coming in

from China just the way we would with certain vegetables or certain dairy products coming in from certain places where we know there is a problem. We do that with agriculture products. The lives of our troops and the mission of our troops is surely important just the way the good, healthy ag products coming in is important as well.

Senator MCCAIN. Well, I eagerly await the opportunity to put it on the defense authorization bill.

Chairman LEVIN. There is a double meaning in that statement by the way—[Laughter.]

Chairman LEVIN.—which I share, by the way, totally.

We thank this panel. Thank you very much.

We are delighted to have an old friend of ours and a great patriot with us this morning, General Patrick O'Reilly, Director of MDA. We are delighted to have you with us, General, please proceed.

STATEMENT OF LTG PATRICK J. O'REILLY, USA, DIRECTOR, MISSILE DEFENSE AGENCY

General O'REILLY. Thank you, sir.

Good morning, Chairman Levin, Ranking Member McCain, and other distinguished members of the committee. I appreciate the opportunity to testify before you today on the serious problem of counterfeit electronic parts infiltrating our critical defense systems and the steps that MDA is taking to prevent their use in the Ballistic Missile Defense System (BMDS).

The missile defense mission requires that thousands of parts which comprise the BMDS perform flawlessly under stressful conditions over their operational life to confidently protect our homeland, deployed forces, allies, and friends against ballistic missiles. Our confidence in the BMDS is only as good as the least reliable component.

We categorize a part as counterfeit if it is a copy sold without the original manufacturer's permission or a part whose material performance or characteristics are misrepresented by a parts distributor. Whether the part was knowingly misrepresented has little consequence to MDA. We still have to resolve the unanticipated parts replacement challenge regardless of the intent of the supplier. Although a counterfeit part may pass acceptance testing, we do not know its remaining operational life as it may have been damaged when removed from a previous product or handled in a destructive manner. Additionally, there is a risk of counterfeit parts having malicious functions that could be activated to disable a critical component of the BMDS. Thus, we simply cannot tolerate the presence of counterfeit parts in our missile defense system.

There are more than 3,000 suppliers providing parts to the BMDS supply chain.

The genesis of MDA's problem with counterfeit parts is the rapidly changing nature of electronic parts specifications driven by broad market applications which frequently present us with component obsolescence problems. In other words, a manufacturer changes a part specification and we face a decision to either redesign our components at a prohibitive cost or seek other sources for the original parts through independent or unauthorized distributors.

Despite our efforts to eliminate the use of counterfeit parts, we have discovered through acceptance testing, stockroom inspections, and screening for parts bought from independent distributors, seven incidents of counterfeit parts since 2006. One incident resulted in the removal and replacement of almost 800 parts from an assembled missile hardware. In another, 38 assemblies had to be reworked and 250 parts were discarded. A stockroom sweep at another independent distributor found 67 parts that were remarked and falsely sold as new. All those counterfeit parts were identified prior to their installation into our components.

Due to the diligence of the MDA's quality control personnel and our contractors, we have been able to limit the cost and schedule impact of counterfeit parts. To date, MDA and its contractors have suffered $4.5 million in rework costs due to counterfeit parts. Of that $4.5 million, the cost to MDA has been $352,000 and industry has paid $1.35 million, with the remainder of the industry costs to be determined by the MDA. However, if a counterfeit part is discovered years after a missile defense product has been produced, replacing the parts in operationally deployed systems could cost hundreds of millions of dollars.

The best way to eliminate the threat of counterfeit parts in the DOD supply chain is to eliminate their source by restricting the use of independent parts distributors through instituting contract clauses and enforcing their strict compliance. In June 2009, I instituted a policy requiring that only parts acquired from the original manufacturers or authorized distributors will be used in MDA contracts. In cases where a part is no longer manufactured and we must use an independent part distributor, MDA contractors must first verify that they cannot use an authorized distributor. Then our contractors must conduct intensive inspections and testing in order to scrutinize the part's authenticity, including using industry accepted tests like x-rays, die verification, and chemical tests for false coatings.

Additionally, MDA performs site assessments of independent distributors. To date, 51 independent distributors have been inspected and more than 60 percent were assessed as moderate to high risk for providing counterfeit products.

Since 2006, MDA has compiled industry quality assurance best practices called our Parts, Materials, and Process Mission Assurance Plan (PMAP), and incorporated them into all our new contracts. The PMAP provides additional assurances that our parts are not counterfeit. As MDA developed part authentication expertise, we also participate in the Office of the Secretary of Defense (OSD) Anti-Counterfeit Part Working Group. Additionally, we issue mission assurance advisories, GIDEP alerts, and notify the Defense Contract Management Command (DCMC) and the Defense Criminal Investigative Service (DCIS) when counterfeit parts are discovered.

MDA has no indication of a counterfeit part in any of our fielded BMDS hardware, but aside from the financial impacts, our greatest concern from the use of counterfeit parts is the operational cost of a malfunctioning interceptor, a cost measured in lives lost or the negative impacts on our national security strategy.

I am grateful for this committee's attention for the debilitating impact counterfeit parts can have on our missile defense system and the rest of DOD. We do not want a $12 million missile defense interceptor's reliability compromised by a $2 counterfeit part.

Thank you, Mr. Chairman, and I look forward to answering the committee's questions.

[The prepared statement of General O'Reilly follows:]

PREPARED STATEMENT BY LTG PATRICK J. O'REILLY, USA

Good morning, Chairman Levin, Ranking Member McCain, and other distinguished members of the committee. I appreciate the opportunity to testify before you today on the problem of counterfeit electronic parts infiltrating our critical defense systems and the steps the Missile Defense Agency (MDA) is taking to detect and prevent unauthorized or defective parts from being integrated into the Ballistic Missile Defense System (BMDS).

MDA integrates technologically advanced sensor, fire control, battle management, and interceptor systems into a single BMDS to provide a reliable, continuously available, defense of our homeland, deployed forces, allies, and friends against a variety of regional ballistic missiles. The BMDS is one of the most complex systems being developed in the Department of Defense (DOD), and the reliability of the BMDS is only as good as the least reliable component of an interceptor, or any vital subsystem.

There are more than 3,000 suppliers providing parts, materials, subassemblies and assemblies for the BMDS. Each one of our missile defense interceptors comprises hundreds of assemblies containing items such as circuit boards, wire harnesses, connectors, valves, solid rocket motors, and electro-mechanical motors. There are also imagery systems, electro-explosive devices, optical devices and precision inertial components. Each assembly has a specific function to fulfill at specific times and it must perform in harsh environments and stressful conditions. We expect the piece parts of these assemblies to perform flawlessly when needed.

Throughout the development process, we carefully scrutinize the designs to make sure design margins exist. We manage the build process to ensure product manufacturing repeatability. Prior to fielding such systems, we test each assembly under stressful environments, thus assuring ourselves and the American people that the systems we employ will perform as required. A simple change in material, an improper technique in material application, or a lack of cleanliness during manufacturing can result in a loss of quality and, hence, a loss of system reliability.

DOD contractors primarily obtain parts from Original Equipment Manufacturers (OEM) or from distributors the OEMs authorize. An unauthorized distributor is one who is not licensed by the OEM to sell its product. We view a counterfeit part as a part procured from an Unauthorized Distributor that is a copy or substitute assembled or sold without the OEM's permission or authority to do so; or one whose material, performance, or characteristics are misrepresented by a supplier in the supply chain. Whether the part was knowingly misrepresented has little programmatic consequence to the execution of MDA programs, we still have to deal with an unanticipated parts replacement challenge.

One type of counterfeit part is a used part that is remarked, has an unknown pedigree and, when sold as new, has most likely been exposed to extreme environments such as high temperature necessary to remove the part from a printed wiring board. Delamination of the internal die bonding can occur as a result of the thermal shock from the heat source used to remove the part from a used circuit board. These unknown conditions expose the part to potential failure modes that could be manifested after acceptance testing. Additionally, exposure levels to humidity and electro-static discharge are unknown. The mechanical parameters of the part may also be changed. Lead wire integrity may be impacted during the removal and remanufacturing operations. Hermetically sealed military parts may get cracked during removal, exposing them to humidity and corrosion that would not appear during acceptance testing but could appear as a failure in the field.

Parts can be remarked as being a fully military compliant part when in fact the part may only be a commercial version of the part. Later revisions of a part may operate in a slightly different manner than previous versions of the part (one or more performance specs may have been tightened over time). If the circuit application requires a newer part, a previous version remarked as a later version may cause latent failures. Because counterfeiting continually evolves in sophistication, it is possible that electronic parts may have embedded functionality created by an

enemy seeking to disable a system or obtain critical information. Detecting hidden functionality would be a difficult undertaking.

MDA has encountered incidents of counterfeit parts dating back to 2006. We identified seven incidents (six assemblies) of counterfeit parts. Part-level testing, acceptance testing, stockroom sweeps and an identification of parts bought by unauthorized distributors helped surface these instances. In one counterfeit part incident, a single acceptance test failure prompted further investigation into the pedigree of the part that failed. The subsequent investigation found that over 1,700 read-only memory parts were procured from an unauthorized distributor and had questionable attributes, such as multiple lot date codes and indications that the parts were previously used. This case resulted in removal and replacement of almost 800 parts from assembled hardware. In another system, a non-mission critical system, electrical testing during acceptance testing yielded erroneous functionality from a voltage regulator. Further investigations showed that the parts were procured from an Unauthorized Distributor and had external markings that were not in accordance with the part drawing. Further investigations found variations of the internal part die. As a result, 38 assemblies were reworked and 250 parts were discarded. In another mission critical system, two acceptance testing failures prompted failure investigations that resulted in the identification of a counterfeit operational amplifier. In this case, 20 assemblies and 150 parts were impacted. A stockroom sweep found 67 frequency synthesizer parts to be re-marked and falsely sold as new parts. These 67 parts were not installed into an MDA system, but would have been in MDA hardware if they had not been detected as part of the stockroom sweep. Three other MDA counterfeit incidents involved non-mission critical telemetry hardware, resulting in approximately 30 parts being discarded.

Total counterfeit parts found to date number about 1,300. All of them were procured from Unauthorized Distributors. We estimate the total cost to MDA for the seven instances is about $4 million. Our largest case cost the Agency $3 million to remove counterfeit parts discovered in the mission computer of our production Terminal High Altitude Area Defense (THAAD) interceptor.

MDA has taken several steps to identify and remove counterfeit parts from within the BMDS supply chain. The Agency:

- Invokes the Parts, Materials, and Processes Mission Assurance Plan on its contracts;
- Uses an extensive ground-testing program to identify quality and performance concerns prior to flight; and
- Supports interagency and DOD efforts to address this problem—MDA participates in the OSD Anti-Counterfeit Working Group and has shared its internal policies and knowledge base with that group.

Remedial actions are considered in each instance and the actions taken necessarily are dependent upon the facts and the responsiveness of the contractors involved.

Although the source of each MDA counterfeit part occurrence was an unauthorized distributor, there are circumstances, such as parts obsolescence, that require procurement of parts from an unauthorized distributor. Contractors must notify the program office with justification and test data in order to purchase any electronic part from an unauthorized distributor. MDA performs site assessments of unauthorized distributors, pre-flight test reviews and risk assessments of the purchased products from unauthorized distributors, and evaluates contractor and subcontractor counterfeit part detection processes. When MDA evaluates an unauthorized distributor, we first check prior history, such as memberships in reputable unauthorized distributor trade groups. We search for complaints and disputes from other unauthorized distributors during the previous 2 years and review any history we may have with the unauthorized distributor. At the unauthorized distributor's site, we evaluate their part-level handling for electro-static discharge and environmental controls, inspection and testing capabilities, and training records, to verify that they follow proper procedures and perform sufficient testing to detect possible counterfeits. If the unauthorized distributor plans to sell a product to MDA, we evaluate the overall risk based on the criticality of the part.

To date, 51 unauthorized distributors have been visited and assessed. Over 50 percent of the unauthorized distributors assessed were viewed as unacceptable by MDA. MDA also has developed part authentication expertise and issues Mission Assurance Advisories and Government-Industry Data Exchange Program (GIDEP) alerts to provide program offices and contractors information related to the discovery of new counterfeiting techniques and any specific counterfeit part discovery.

The best time to detect a counterfeit part is at receiving inspection before the part enters production inventories. Robust inspection of parts procured from unauthor-

ized distributors is absolutely necessary at receiving inspection. Our experience indicates counterfeit parts are also discovered during end item acceptance testing when electrical stimuli and harsh environments are imposed. However, some counterfeit parts that include the correct die, but are actually used parts, can pass acceptance tests, be fielded and result in a reliability risk.

Due to the early recognition of the counterfeit part problem and the diligence of our contractors, we have been fortunate to identify and limit the cost and schedule impact of counterfeit parts. However, if a counterfeit part is discovered years after it was integrated into the BMDS, recovering the parts through the disassembly of possibly hundreds of operationally deployed systems could be extremely expensive, potentially costing hundreds of millions of dollars. Aside from the financial impacts, the greatest potential impact of counterfeit parts is the operational cost of an interceptor that does not perform as designed when it is needed, a cost that could be measured in lives lost or the negative impacts on foreign policy and national security strategy.

The predominant threat of counterfeit parts in missile defense systems is reduced reliability of a major DOD weapon system. We do not want to be in a position where the reliability of a $12 million THAAD interceptor is destroyed by a $2 part. Among the more significant steps MDA has taken to combat the counterfeit parts risk is establishing requirements in its contracts to provide the pedigree of every single mission critical part used in the BMDS. To date, MDA has had no indication that any mission critical hardware in the fielded BMDS contains counterfeit parts.

Thank you, Mr. Chairman. I look forward to answering the committee's questions.

Chairman LEVIN. Thank you very much, General.

First, let me thank the MDA for providing the committee with assistance in this investigation. It has been very helpful. Our staffs have repeatedly called on Mr. Fred Schipp who is currently supporting MDA from the Naval Surface Warfare Center Crane. He has engineering expertise and other technical advice has come from him, and it has been invaluable. We also would recognize Mr. Isaiah Mullis, I believe his name is, from MDA and also from the Naval Surface Warfare Center who has likewise provided us assistance.

You made reference to your looking into independent distributors to try to certify them. Your preference is to get parts only from the original manufacturers or from authorized distributors, but if there are none available, you say that then independent distributors can be used providing you take a look at them and certify them.

I was trying to find in your testimony—and it probably is in here—your written testimony the number that you used as to how many of them could not be certified with confidence.

General O'REILLY. 61 percent, sir. 61 percent of the ones we have looked at we could not certify. I do not accept a moderate risk. So 61 percent were determined to have either moderate or high risk because of their accounting methods, their stockroom accuracy of how they actually manage their inventories, and their paper trail proving that the components are authentic.

Chairman LEVIN. All right. So part of that process is looking at where do they get the parts that they are distributing.

General O'REILLY. Yes, sir, and how do they account for it.

Chairman LEVIN. How they account for it, as well as the other factors that you mentioned.

The care that you take is care that we need to take in other weapons systems, and I think the model that you have used needs to be shared, if it has not already been shared, with all of our other agencies that are buying components for our weapons systems. I am wondering is your model unique to MDA, or is it something

which is agency-wide through DOD that you have just used and modified? Where did you get that model?

General O'REILLY. Sir, we came up from the—after I took over the agency in 2008, we had had two recent counterfeit parts incidents with telemetry. I know we talk about the operational systems, but when I conduct a flight test, if I lose my telemetry, I lost the complete value of that test and that is quite expensive also.

Looking into that, we determined on ourselves that, in fact, the history and working with our aerospace industry partners, we found that the independent distributors is where we found all of the counterfeit parts were coming from that were affecting the MDA. So at that point we banned—I signed a policy that, in effect, bans the aerospace companies from using independent distributors without first coming to my agency and gaining approval. Then we scrutinize the specific component which they are buying.

I understand some parts of the Navy have a similar program to that, and I am unaware of any other programs.

Chairman LEVIN. Now, when you had the telemetry problems, were they traceable to particular parts?

General O'REILLY. Yes, sir. Before they were used, we found them as failures in acceptance testing actually at a sub-tier level. I have in my supply chain five levels of companies, and at the middle level is where we found the problem with the specific components, which was an operational amplifier and a frequency synthesizer. Those parts that we found were in a particular company, and we went then and traced where did that company get its parts. It was eventually from an independent distributor.

Chairman LEVIN. Do you know where they got their parts from?

General O'REILLY. No. At that point, we handed it over to the DCMC and the DCIS.

Chairman LEVIN. Do you know whether that amplifier and that synthesizer were counterfeits?

General O'REILLY. Yes. Our indications were they were black topped, which is the die is not correct. It does not match what the paperwork said it would be. In the other case, the parts were remarked. There was evidence that the age codes were remarked on those components.

Chairman LEVIN. Again, I am trying to get the chronology here. Did that investigation take place after there was the flight problems or before?

General O'REILLY. It was before. We actually caught all of these before, and so we have not had a failure that we know of related to a counterfeit part. But it was only because our supply chain—at some point someone caught the fact that a part did not look right or it failed an acceptance test.

Chairman LEVIN. There was what? A real possibility of failure if you had not caught it? Is that where you are at?

General O'REILLY. Sir, yes. There is a risk and it is a risk we cannot take. We do not know the history of that component. A lot of times they are damaged when they are removed from their previous product due to heat and then they will be susceptible to stressful conditions in our tests. We are very concerned then about a failure.

Chairman LEVIN. It has been argued that these parts can last some time, and if they fail, that it would be downstream at some point.

General O'REILLY. Yes, sir.

Chairman LEVIN. That is what the argument is of some folks who say that the risks are not real. Your answer to that is, as I understand it, what?

General O'REILLY. Sir, the risks are real. Just because they pass an acceptance test, that only gives you a limited insight to what the remaining life of that component could be, and we cannot take the chance for one of our interceptors to fail.

Chairman LEVIN. So that the life of that part is what is at issue, not whether it can pass an immediate acceptance test, but how long it will last if it is a counterfeit part and how reliable it is.

General O'REILLY. Yes, Senator, or if there is some other damage that occurred that we could not tell because we were not looking for it at the time of the acceptance test.

Chairman LEVIN. Now, in your written testimony, you used a slightly different figure than you did in your oral testimony in terms of the cost to MDA of the seven instances of counterfeit parts, and you used a figure of $4 million. What is the difference between those two numbers?

General O'REILLY. I checked the math of my staff this morning, sir.

Chairman LEVIN. I sometimes do that too, they will tell you. But you are known for that kind of leadership and that is the kind of leadership which we very much welcome. Thank you.

Senator McCain.

Senator MCCAIN. Well, thank you, Mr. Chairman, and thank you, General, for your important testimony. I guess I would like to start out by asking you what I asked the other panel. How serious a problem do you think this is?

General O'REILLY. Extremely serious, sir.

Senator MCCAIN. The largest case, as you have already testified, cost MDA $3 million to remove counterfeit parts discovered in the mission computer of the production THAAD interceptor. Is that correct?

General O'REILLY. Yes, sir. The exact number is $2.74 million, but yes, sir.

Senator MCCAIN. How many counterfeit parts were there in this incident? I believe it was about 800. Is that correct?

General O'REILLY. Yes, sir. It was 800 and there were 49 that were—actually 50 that were used in a mission computer and one mission computer was flown in a flight test. So 49 were actually used in building up computers for the interceptor.

Senator MCCAIN. So I guess my question is—maybe you could briefly trace it for me how the parts could infiltrate so deeply into the supply chain.

General O'REILLY. Sir, it was at one of our subcontractors, Orbital, that builds up the booster system and it was in the control units of that. During their Advanced Testing Procedure (ATP), they then—when they bought the lot of parts, it was a large lot of parts. Therefore, they caught—out of several hundred, one of them found

did not perform right electronically. Then they were able to look into it and discovered that it made the whole lot suspect.

Senator MCCAIN. You made up the cost rather than the contractor for the replacement. Is that correct?

General O'REILLY. Sir, there is an award fee process that is associated with this, and we are going through the evaluation of that award fee period that is to Lockheed Martin and we take this into account. We have not completed that work. It will be due within 60 days, and we have been very strict in the past on ensuring compliance with quality assurance provisions.

Senator MCCAIN. Well, we will try to help you with legislation to make sure that responsibility does not apply to the American taxpayer.

It seems to me that one of the understated or not sufficient emphasis has been placed on these intermediaries. Chairman Levin at the beginning of the hearing, I am sure you noticed that these different entities—they do not go direct from China to THAAD. They go through three or four different iterations. It seems to me that that is a serious problem. Some of these people who are, quote, subcontractors who are intermediaries are simply a phone and a desk and rake off some of the money as it goes through. Is that too stark a generalization?

General O'REILLY. Senator, it is not the subcontractors, but it is the suppliers which they use.

Senator MCCAIN. Intermediaries.

General O'REILLY. But yes, sir, I would say that. That is why we have banned the use of these intermediaries. They must buy directly from an original manufacturer or one of their authorized dealers. If we are in a situation where that source does not exist, my agency has to approve the use of an intermediary or an independent distributor.

Senator MCCAIN. So you are trying to take steps to make sure that never again would you see a graph like Chairman Levin put up on the screen here today, the different layers of intermediaries.

General O'REILLY. Yes, sir. That is exactly what we are trying to do, go directly to the manufacturer or their authorized dealer.

Senator MCCAIN. Are the other Services doing the same thing?

General O'REILLY. Sir, we present our models and our results to the working group that OSD has established. I do not have direct insight into what the other Services are doing.

Senator MCCAIN. Well, Senator Levin and I are committed to trying to put legislation into the defense authorization bill, as he mentioned. Obviously, we do not want to be guilty of overreach. We do not want to be guilty of overreaction. But since you and others have recognized and testified that this is a serious issue, we would appreciate your input in any legislative fixes that need to be made between now and the next week or 2 when, hopefully, we take up the defense authorization bill. Have you got some ideas for us?

General O'REILLY. Sir, one of the implications of the policy which the MDA has established is if—this creates clauses in our contract. Regardless if they are cost-plus or fixed price, if a clause is violated by the contractor and in this case he does not verify authenticity of the parts he is using, then that cost becomes unallowable, and

an unallowable cost, including the rework, then would be borne by industry.

Senator MCCAIN. Well, then why did we end up giving $2.9 million back to Lockheed Martin?

General O'REILLY. Sir, that contract is 10 years old, that particular one, and that was not a clause in the contract. But it still does not exhaust my remedies. I still have award fee and other steps I can take in order to remedy the cost to the Government.

Senator MCCAIN. Well, I guess finally you are in complete agreement with the Chinese foreign minister's spokesman Hung Li who said, quote, the Chinese government has always paid a great deal of attention to and has promoted cooperation with relevant overseas bodies in the fight against counterfeits. This is universally acknowledged. Do you agree with the Chinese foreign ministry spokesman, General?

General O'REILLY. Sir, the data indicates the opposite.

Senator MCCAIN. I am shocked to hear that that is the case. [Laughter.]

I thank you, Mr. Chairman.

Chairman LEVIN. Thank you very much, Senator McCain.

If you would get to us, General, immediately because we are going to be drafting language. The procedures that you use in terms of certification where there is no original manufacturer or supplier available. If you can get us that procedure, I presume it is your own procedure. It is in writing or however it is, or write it up for us.

Also that clause that you just made reference to. Was that a clause which says that you cannot be reimbursed if you have not used a certified—give us that clause again.

General O'REILLY. Our new policy puts into all new contracts a clause that says the contractor has to use—he is responsible for using original manufacturer's parts or their authorized dealer only. If they violate that, the cost that is incurred in the Government, when that is discovered and the remedy is implemented, will then not be an allowable cost to the contract.

Chairman LEVIN. Got it. Does that include if they are not able to get to the original manufacturer, they can get to one of your certified distributors?

General O'REILLY. No, sir. If they come to us and we have done our due diligence and we authorize it and then we find out later that it is still a counterfeit part, which we do our best to ensure that does not happen, but in that case, it would be an allowable cost.

Chairman LEVIN. Okay, and that is also in the language then that would be in the contract?

General O'REILLY. Yes, sir.

Chairman LEVIN. Can you get us that contract language? It would be helpful.

Senator Hagan.

Senator HAGAN. Thank you, Mr. Chairman. General O'Reilly, it is a pleasure to see you again, and thank you for your work as the Director of MDA.

Hearing this testimony and thinking about the telemetry and all of the very fine-tuned calculations that every part has to adhere

to—and I think of probably millions of pieces of parts that we are talking about and dealing with—I guess the question is how comfortable do you feel now with these protocols that you have put in place. I think at one point you said that if they use an independent supplier that is not on this approved, authorized original part, then the companies would have to come to you. I just think if you would have to have a whole other agency just to deal with the sort of contracting issues.

General O'REILLY. Senator, we actually do. We work very closely with the DCMC. They have onsite personnel. I have 50 onsite personnel myself. It is a combined effort. Also, most of these incidents are occurring at lower levels of the supply chain, a third or fourth level, and the prime contractors—obviously, they are motivated not to have this happen too. So we literally form a very large set of scrutinizers that work through the supply chain. But being coordinated and working across industry and with other agencies is the key.

I am not comfortable, even after I have implemented these, because as you sit there in a flight test or in a live fire and you watch the operation of these systems, you know how precisely they must perform, as you have referred to, and we sweat the details. So I really would not be comfortable that would remove the vigilance which we have already put in place. It is necessary.

Senator HAGAN. Certainly.

How comfortable are you that the prime contractors and their subcontractors are also having the due diligence where they are looking out for these same instances that you are?

General O'REILLY. Senator, I believe they are highly motivated to make sure. One is they need to get through the developmental phase to get to production contracts. Then most of our production contracts are fixed price, which means they bear the cost, in fact, if a counterfeit part is discovered.

Senator HAGAN. I know that you do not have this aging equipment as some of the other branches of our military might have. But what if a part is no longer produced by the original either independent supplier or the original authorized dealer and it then has to be remanufactured? Is there a chain of—following that chain, how would you—do you have that as a problem?

General O'REILLY. Yes. There is a series of engineering decisions that have to be made between the prime contractor and the subcontractors affected and MDA. We have to make the decision, is it worth it to go out and produce our own components?

The problem is and the problem referred to before of the trusted foundries is we use very few components, but they are spread out over a large spectrum of part types. So in many cases, we are less than one-tenth of 1 percent of the overall market for our component. So we are confronted with having to decide whether to redesign our circuitry, and that often is the case and we run into obsolescence. Almost every one of my manufacturing contracts has an obsolescence contract line item number part of the contract that has to be redesigned primarily due to electronic parts no longer being manufactured.

Senator HAGAN. So how can you assure that that is in that scenario the original part that you, in fact, are contracting for?

General O'REILLY. We have assessments from industry that project the life of a component, and we select parts that are in the early stages of their life. It is called a sunset clause, and they are not at the end of their operational life and have a tendency to change. Sometimes we are caught off guard, though, on those. It does require a continual amount of engineering work to relook at the designs that have already been proven because of the discontinuity in our supply chain of the electronic parts.

Senator HAGAN. Have you recognized any suppliers lower down the chain of parts that have repeatedly been found to have counterfeit parts being used? If so, are you taking action to be sure we do not contract with those suppliers?

General O'REILLY. We are always scrutinizing our parts usage and our sources because of the nature of our work more than what I have seen in some of my other acquisition jobs in DOD. Because of that, we have not found a case where someone is willfully or repeatedly, but I must say that in the seven cases—in five cases, the supplier actually completed the repair at their own cost and did not charge the Government for it in five of the seven cases. So they recognize. A company such as Honeywell actually went out and did a complete review after one of our cases of their entire stockage and swept through and removed anything that indicated that it was a counterfeit part, and they also instituted new policies.

Senator HAGAN. Thank you, Mr. Chairman.

Chairman LEVIN. Thank you very much, Senator Hagan.

Thank you, General. We really would look forward to your being able to give us that information literally in the next couple days because we are going to try to formulate in amendment form. I think we will have broad support from this committee that has heard this testimony and I think a lot of other Senators who are following it. This is quite an amazing story and it has to change direction quickly.

You have taken action in your agency, which is the right action. It has been strong. It has been direct. It has caught some real problems before they created some real problems, and your testimony has been extremely helpful. We are grateful for it. Thank you.

General O'REILLY. Thank you, Senator.

Chairman LEVIN. You are excused unless you have some other comment you want to make.

General O'REILLY. No, sir. Thank you, sir.

Chairman LEVIN. Okay. Your stomach is not growling there?

General O'REILLY. Not yet. [Laughter.]

Chairman LEVIN. Thank you. We are going to have a vote and break now for just 10 minutes. I am going to go vote. I am going to come back. We are going to get the opening statements before lunch, and then we will break probably for about an hour after the opening statements. But we will be able to get the opening statements in before lunch, and then we will come back after an hour break or so. So we will stand adjourned now for 10 minutes. [Recess.]

The committee will come back to order, and we will move to our third panel. Then we will receive the opening statements, and then as I indicated before, we will break for about an hour for lunch.

Before I call on you, let me thank each of you for being here today and to thank you and your companies for your cooperation. We very much appreciate that cooperation with this committee and we give you credit for doing that because I know that some of these questions may be difficult to answer, but the fact that you are cooperative with us is something that stands in your favor.

Is it Mr. Kamath? Am I pronouncing your name correctly? Kamath?

Mr. KAMATH. Yes, Mr. Chairman. Kamath is fine.

Chairman LEVIN. Okay, and it is Vivek?

Mr. KAMATH. Vivek.

Chairman LEVIN. Vivek Kamath. So you are the Vice President of Supply Chain Operations for Raytheon. So we will start with you.

STATEMENT OF VIVEK KAMATH, VICE PRESIDENT, SUPPLY CHAIN OPERATIONS, RAYTHEON COMPANY

Mr. KAMATH. Thank you, Mr. Chairman. Mr. Chairman, Raytheon appreciates the opportunity to work with you on this important inquiry into counterfeit electronic parts in the DOD supply chain. These parts making their way into military equipment pose a real threat to our national security.

Mitigating the risks posed by suspect and counterfeit electronic parts is an issue that Raytheon takes very seriously. Our business and our reputation demand this approach, which is why Raytheon spends a great deal of time, resources, and effort tackling this problem on a daily basis.

As in any market, counterfeit electronic parts enter the DOD supply chain because of supply and demand. Rapid turnover in high technology items provides a steady source of used materials that can end up as counterfeit parts. In addition, obsolete parts pose a challenge because original equipment manufacturers may have stopped making these parts or left the industry altogether. Despite these challenges, DOD and its suppliers must obtain the authentic electronic parts needed to build, maintain, and refurbish defense systems.

Across Raytheon, our supply chain covers thousands of programs and contracts involving a vast number of suppliers. We issue hundreds of thousands of purchase orders every year. Purchase orders for electronic parts where the risk of counterfeiting is the highest may cover multiple lots comprised of thousands of individual parts.

As a company, Raytheon is committed to providing genuine electronic parts to our customers. Like others in the industry, Raytheon mandates that suppliers certify in writing that the electronic parts they are providing meet the standards in the purchase order, including requirements for authentic parts from authorized sources.

In 2009, Raytheon formed a cross-business team to develop an enterprise-wide counterfeit parts mitigation policy. This policy, which builds on existing business practices, was introduced in July of this year and will be fully implemented by February 2012. Our counterfeit parts mitigation policy assigns specific responsibilities to Raytheon supply chain management, engineering, mission assurance, and other functions. The policy also focuses attention on as-

pects of our supply chain that are most likely to present risks, such as procurement of electronic parts from independent distributors.

To further reduce the possibility that counterfeit parts might find their way into our products, Raytheon is developing a preferred supplier list for distributors and brokers and will mandate its usage across our company. We will also consolidate purchasing through a centralized procurement organization.

In addition, Raytheon is a member of GIDEP. The GIDEP reporting system provides a means for manufacturers and suppliers to alert other GIDEP members when they identify potential counterfeit parts, assemblies, components, and their suppliers. This kind of information sharing can help stop suppliers of counterfeit parts in their tracks. Raytheon treats GIDEP reporting as mandatory. Our new enterprise policy will reinforce this practice.

In conclusion, given the scope and dynamic nature of the threat, counterfeit items will remain a challenge. The policies, practices, and measures that Raytheon has put into place will further protect our supply chain from counterfeit parts and limit exposure and mitigate risks for our customers and our company. Effective policy responses will further refine industry best practices and improve information sharing while avoiding costly or time-consuming solutions that provide little additional protection for the warfighter.

We thank the committee for focusing its attention on this challenging issue. I would be happy to answer questions when we return. I would like to ask that the entire statement be made part of the record. Thank you, Mr. Chairman.

[The prepared statement of Mr. Kamath follows:]

PREPARED STATEMENT BY VIVEK KAMATH

INTRODUCTION

Mr. Chairman, Ranking Member McCain, and members of the committee, Raytheon appreciates the opportunity to work with you on this important inquiry into counterfeit electronic parts in the Department of Defense (DOD) supply chain. These parts making their way into military equipment pose a real threat to our national security.

Mitigating the risks posed by suspect and counterfeit electronic parts is an issue that Raytheon takes very seriously. It is one of our top priorities. Indeed, our business and our reputation demand this approach, which is why Raytheon spends a great deal of time, resources, and effort tackling this problem on a daily basis.

We are hopeful that the detailed information we have provided to you and your staff throughout the investigation has proven beneficial. I look forward to discussing the proactive steps that Raytheon has taken to combat the threat.

THE CHALLENGE OF COUNTERFEIT ELECTRONIC PARTS

According to government and industry data, 7 to 8 percent of world trade every year involves counterfeit products. Each year, due to counterfeiting, hundreds of thousands of American jobs are lost and U.S. companies lose between $200 and $250 billion.

At Raytheon, we consider an item to be "counterfeit" if it is purposely misrepresented to be genuine. Under this definition, counterfeits include unauthorized or illegal copies, items whose appearance is altered or disguised with the intent to mislead, or items that are refurbished or reclaimed, but advertised as new. Unauthorized substitution of materials or components constitutes counterfeiting under our policies. Raytheon also takes the view that counterfeiting includes falsely advertising that the testing, screening, or qualification of an item is complete.

As in any market, counterfeit electronic parts enter the DOD supply chain because of supply and demand. Rapid turnover in high technology items provides a steady source of used materials that can end up as counterfeit parts. Also, obsolete parts pose a challenge because Original Equipment Manufacturers may have

stopped making the parts or left the industry altogether. Despite these challenges, DOD and its suppliers must obtain the authentic electronic parts needed to build, maintain, and refurbish defense systems.

Counterfeiters are innovative, and their efforts pose a dynamic threat to supply chains. The volume of counterfeit items and rapidly improving methods for concealing them require constant vigilance from all participants in the supply chain. Yet, even with a substantial investment of time and resources by the U.S. Government and its suppliers, counterfeit parts will likely continue to find their way into defense and other U.S. Government systems. We are fully committed to making sure they do not.

RAYTHEON SUPPLY CHAIN OPERATIONS

Across Raytheon, our supply chain covers thousands of programs and contracts involving a vast number of suppliers. We issue hundreds of thousands of purchase orders every year. Purchase orders for electronic parts—where the risk of counterfeiting is highest—may cover multiple lots comprised of thousands of individual parts.

As a company, Raytheon is committed to providing genuine electronic parts to our customers. Like others in the industry, Raytheon mandates that suppliers certify, in writing, that the electronic parts they are providing meet the standards in the purchase order—including requirements for authentic parts from authorized sources. In Raytheon's experience, however, the protection afforded by this certification is limited in two principal ways. First, the source information available to suppliers must be reliable. Second, suppliers must be committed to practices designed to mitigate counterfeit electronic parts.

IMPROVING BEST PRACTICES

Raytheon has been addressing the presence of counterfeit parts in the supply chain for years. Raytheon's business units operate under policies for detecting and mitigating the risk of counterfeit parts. These policies have protections that reflect the specific needs of each business.

Building on these experiences, we worked with our partners in the defense industry in 2009 to develop SAE Aerospace Standard (AS) 5553—Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition—an industry guideline to develop consistent policies regarding counterfeit parts.

At the same time, Raytheon formed a cross-business team to develop an enterprise-wide counterfeit parts mitigation policy. This policy, which amplifies and integrates existing business practices, was introduced in July 2011 and will be fully implemented in February 2012. Based on SAE AS5553 and Raytheon's own best practices, our counterfeit parts mitigation policy assigns specific responsibilities to Raytheon's Supply Chain Management; Engineering; Mission Assurance; and other functions. The policy also focuses attention on the aspects of our supply chain that are most likely to present risks, such as the procurement of electronic parts from independent distributors.

To further reduce the possibility that counterfeit parts might find their way into one of our products, Raytheon is developing a Preferred Supplier List for distributors and brokers. This list will allow us to reward suppliers that institute rigorous processes to secure their own supply chains and that have a proven history of supplying us with authentic parts. Limiting our relationships to these responsible suppliers will also allow Raytheon to devote more time to supply chain oversight. In turn, preferred suppliers will have a strong financial incentive to comply with our requirements and standards.

We are also consolidating purchasing across Raytheon through a central procurement organization. All purchases of electronic parts through distributors will be routed through this organization, providing additional governance and oversight of our supply chain.

Like many other organizations in government and industry, Raytheon is a member of the Government-Industry Data Exchange Program (GIDEP). The GIDEP reporting system provides a means for manufacturers and suppliers to alert other GIDEP members when they identify potential counterfeit parts, assemblies, components, and their respective suppliers. This kind of information sharing can help stop suppliers of counterfeit parts in their tracks. Indeed, because of its importance to the security of the entire industry supply chain, Raytheon treats GIDEP reporting as mandatory. Our new enterprise policy will reinforce this practice.

CONCLUSION

Given the scope and dynamic nature of the threat, counterfeit items will remain a challenge. The policies, practices, and measures that Raytheon has put in place will further protect our supply chain from counterfeit parts, while limiting exposure and mitigating risk for our customers and our company. Effective policy responses will further refine industry best practices and improve information sharing, while avoiding costly or time-consuming solutions that provide little additional protection for the warfighter.

We thank the committee for focusing its attention on this challenging issue, and I would be happy to answer any questions you may have.

Chairman LEVIN. Thank you. The entire statement will be made a part of the record and that is true of all statements here today.

Mr. DeNino, you are the Vice President, Corporate Procurement for L–3 Communications. So thank you.

STATEMENT OF RALPH L. DENINO, VICE PRESIDENT, CORPORATE PROCUREMENT, L–3 COMMUNICATIONS CORPORATION

Mr. DENINO. Thank you, Chairman Levin, and good afternoon.

On behalf of L–3 Communications, I appreciate the opportunity to be here today to address the important issue of counterfeit electronic parts in the U.S. military supply chain.

L–3 Communications is a prime contractor in command, control, communications, intelligence, surveillance, and reconnaissance systems, aircraft modernization and maintenance, and Government services. L–3 is also a leading provider of a broad range of electronic systems used on military and commercial platforms. We serve a wide range of customers, most notably DOD and its prime contractors.

The reality that L–3 and the entire aerospace and defense industry faces is that electronic components are increasingly susceptible to two significant risks: obsolescence and counterfeiting. With sophistication levels of counterfeiters escalating, detection and avoidance are becoming increasingly difficult. These issues are exacerbated by the service lives of fielded defense weapons systems being extended well beyond their original planned life cycle, furthering the challenge of the ever-shortening life cycles of electronic components, which is being driven by commercial technology changes.

L–3 has been proactive in both managing obsolescence and counterfeit part risk mitigation. Procedures and processes are in place to manage both of these areas with improvements being driven to stay current with emerging counterfeit threats. Supply chain management techniques have been implemented to limit the number of independent distributors that can sell parts to L–3. Strict and progressive testing methodologies are in place. Reporting of incidents is required and training and education of personnel is ongoing.

L–3 will continue to improve its obsolescence and counterfeit parts mitigation programs through strict adherence to its corporate procedures and policies across the entire enterprise, controlling independent distributor purchases, and by providing training and education to our personnel. Additionally, we will continue to work with our Government and industry partners and professional associations to develop and incorporate best practices throughout the supply chain.

In any case, if any part is identified as suspect counterfeit, L–3 will, as it has in the past, promptly notify all of its affected customers and work with them to remediate the problem in whatever way the customer determines is needed at no cost to the Government.

Finally, while L–3 has made significant efforts over several years to address the counterfeit parts challenge, the Senate Armed Services Committee's examination of the issue has been important in underscoring the seriousness and depth of the problem and the need to rapidly develop an effective solution. L–3 looks forward to working with other companies and the committee in achieving this goal and will be pleased to answer any questions that the committee may have.

[The prepared statement of Mr. DeNino follows:]

PREPARED STATEMENT BY RALPH L. DENINO

INTRODUCTION

My name is Ralph DeNino, and I am L–3 Communications' Vice President, Corporate Procurement. I've been employed at L–3 Communications since December 2000. At L–3, I have corporate-wide responsibility for Supply Chain Management and Quality Management.

ABOUT L–3 COMMUNICATIONS CORPORATION

L–3 is a prime contractor in Command, Control, Communications, Intelligence, Surveillance, and Reconnaissance (C^3ISR) systems, aircraft modernization and maintenance, and government services. L–3 is also a leading provider of a broad range of electronic systems used on military and commercial platforms. Our customers include the U.S. Department of Defense (DOD) and its prime contractors, U.S. Government intelligence agencies, the U.S. Department of Homeland Security, U.S. Department of State, U.S. Department of Justice, allied foreign governments, domestic and foreign commercial customers and select other U.S. Federal, State, and local government agencies.

L–3 is composed of four business segments:

1. Command, Control, Communications, Intelligence, Surveillance, and Reconnaissance (C^3ISR)

L–3 provides airborne and ground-based products and services for the global ISR market, networked communications systems and secure communications products for real-time situational awareness and response.

2. Government Services

L–3 provides a full range of engineering, technical, enterprise information technology (IT) and cybersecurity, advisory, training, and support services to the U.S. military, government agencies, and allied foreign governments.

3. Aircraft Modernization and Maintenance

L–3 provides modernization, upgrades and sustainment, maintenance, and logistics support services for military and government aircraft and other platforms.

4. Electronic Systems

L–3 provides a broad range of products across several business areas that include marine and power systems, microwave and satellite communications products, displays, aviation products, training and simulation, electro-optical/infrared products and systems, warrior systems, precision engagement, security and detection systems, applied technology, telemetry and RF products, power and propulsion systems, and undersea warfare and ocean sciences products.

OBSOLESCENCE AND THE RISK OF COUNTERFEIT PARTS

As a major aerospace and defense contractor, L–3 Communications provides our worldwide customers with a sophisticated array of high tech products. In the world of high tech products there is a common element: the need for and availability of quality, high reliability electronic components. The reality that L–3 and other aerospace/defense contractors face is that electronic components are increasingly suscep-

tible to two significant risks: obsolescence and counterfeiting. Component obsolescence is a constant issue that must be considered early in the design and product development phases to mitigate risks to schedule and multi-year maintenance needs. Counterfeiting, primarily originating in Asia, is now a sophisticated multi-billion dollar industry. With sophistication levels of counterfeiters escalating, detection and avoidance are becoming increasingly difficult. These issues are exacerbated by the service lives of fielded defense weapon systems, which are now being extended beyond their original planned life cycle. It is not unusual for a fielded system to be operational for anywhere from 25–40 years. These problems are further complicated by a reduction in the industrial base dedicated to production of electronic components that support military products. Defense and civil aerospace related acquisitions now account for less than 1½ percent of total microelectronic semiconductor sales.

Compounding the problem in the Aerospace and Defense industry are the long product design cycle inherent in military systems and the ever shortening life cycle of available components. Obsolescence challenges are especially apparent for electrical, electronic, and electromechanical commodities. Obsolescence in the last few years has been driven not only by the increasing speed of technological change and market consolidation, but also by new environmental regulation, such as restriction of hazardous substances, which affected the market by driving change to a "lead free" environment. The obsolescence and counterfeit parts challenge was astutely summarized by Ted J. Glum, director of the DOD's Defense Microelectronics Activity Unit when he stated, "The defense community is critically reliant on a technology that obsoletes itself every 18 months, is made in unsecure locations and over which we have absolutely no market share influence." ("Pentagon Worries About Chinese Chips" A.T. Gillies, 9/4/08).

Having to find sources for obsolete electronic parts also increases the need to buy from nontraditional sources, because by definition the Original Component Manufacturer (OCM) or its authorized, franchised distributor no longer stocks the original part that is now obsolete. In turn, having to rely on non-traditional sources of supply, typically referred to as Independent Distributors (ID), results in increased risks of encountering counterfeit parts. Independent Distributors operate under far less regulation and control than OCMs, and are not as accountable as OCMs are to long-term customers. While obsolescence can be dealt with in other ways, such as redesign to utilize currently available electronic components or reproducing the original part, these options are normally not available due to a lack of government funding, a problem that would appear likely to increase in the current budget environment.

L–3 recognizes the need to address these risks and obstacles to ensure both supply chain availability of electronic components and customers' confidence in our products. The creation at the corporate level of L–3's Diminishing Manufacturing Sources and Material Shortages (DMSMS) program was the first step taken to proactively work obsolescence issues. The DMSMS program features a system that provides divisions a tool for uploading their Bills of Material (BOM) to receive life cycle analysis and up to date obsolescence information on Military Standard and commercial electronic components.

Similarly, understanding that obsolescence challenges increase the serious risk of exposure to counterfeit parts in the supply chain, a corporate level Counterfeit Parts (CP) program was established to focus on addressing the emerging risk and to implement a strategy that could be deployed by all divisions of the corporation.

L–3 COUNTERFEIT PARTS RISK MITIGATION PROGRAM

More specifically, L–3 formed a corporate-wide Counterfeit Parts Team (CPT) in December 2007 to share information and experiences across all L–3 divisions, to increase awareness of the challenges and to provide education and training. The CPT developed a database of information and lessons learned about counterfeiting techniques, which is shared with all divisions of the corporation. The team also set out to develop procedures and to define testing requirements to detect counterfeit parts and mitigate risks.

This resulted, in December 2008, in L–3 implementing Material Quality Operating Procedure (MQOP–001): Counterfeit Parts Risk Mitigation Program to address the counterfeit parts issue. As Counterfeiting techniques evolved, the Procedure was updated in March 2011. To further improve our process, to impose more stringent testing requirements and to increase the focus on avoiding the use of obsolete parts, we updated our Procedure again in early November 2011.

Our CPT's efforts are closely tied with our DMSMS Team because, as noted above, obsolescence increases exposure to the counterfeit market place. In that regard, to address the risks posed by Independent Distributors, we began our efforts

to narrow the listing of Independent Distributors used for sourcing obsolete devices. An assessment of our approved independent suppliers resulted in the corporate approved listing of IDs being reduced from 16 suppliers to 6 in March 2011, with a stated goal of further reducing the listing to 4. In May 2011, this goal was achieved. Correspondingly, and earlier, in March 2008, L–3 became a member of the Electronic Retailers Association International, the global resource for companies involved in purchasing and selling of manufacturing electronic components.

Our teams also recognized that improvements were required in education, training, and data sharing on counterfeit parts techniques and counterfeit parts occurrences taking place across the entire aerospace and defense industry. Accordingly, the corporation sponsored two series of Counterfeit Part Risk Mitigation and Component Obsolescence Management events. This included three regional symposia held in fall of 2008. More recently, five regional symposia were conducted in the fall of 2010, attended by over 250 professionals in the disciplines of Supply Chain Management, Quality Management, Program Management, and Engineering. These symposia were also open to and supported by L–3 subcontractors. In addition to presentations by L–3 personnel at these training and education sessions, the event was supported with presentations by industry experts and a representative from the Government Industry Data Exchange Program.

To supplement training, articles on the CPT's activities and industry trends in counterfeiting techniques, as well as our DMSMS/obsolescence management program are regularly featured in our corporate-wide Supply Chain and Quality Management Newsletter. In addition to regularly scheduled teleconferences, the CPT maintains a robust intranet site that provides valuable information accessible to L–3 employees. Suspect and counterfeit part experiences at L–3, training materials for use with our subcontractors, industry guidance and other important resources are housed at this site.

SPECIFIC INCIDENTS OF COUNTERFEIT PARTS THAT L–3 HAS EXPERIENCED

L–3 Communications Integrated Systems L.P. (L–3 IS) is the prime contractor for the United States Air Force Joint Cargo Aircraft C–27J program. This program began as a U.S. Army-led program in 2007 and transitioned in 2010 to the Air Force under the current C–27J System Program Office (SPO) within the Mobility Directorate at the Aeronautical Systems Center (ASC) of the Air Force Material Command (AFMC) at Wright-Patterson Air Force Base, Ohio. It is a program of record and classified as an Acquisition Category (ACAT) ID. Although the aircraft is based upon the C–27J transport produced by Alenia Aeronautica, S.p.A., its avionics elements derive heavily from the Lockheed Martin C–130J aircraft.

The C–27J program experienced four instances of suspect counterfeit electronic components since the program started. These have involved the avionics systems for the Mission Computer provided by BAE Systems of Austin, Texas; the Color Multipurpose Display Units (CMDU) provided by L–3 Communications Display Systems of Alpharetta, Georgia (which has been affected on two separate occasions); and the Type I Bus Adapter Unit (BAU) provided by Goodrich of Vergennes, Vermont. One additional instance of suspect counterfeit electronic components involved Ground Support Equipment (GSE) for the ALE–47 Countermeasures Dispensing System (CMDS) provided by BAE Systems of Austin, TX.

In the case of the C–27J, L–3 IS, as the prime contractor, promptly notified its Government customer on each occasion as soon as it became aware of suspect counterfeit components. L–3 Display Systems, which manufactures the CMDUs, also notified all of its customers in both cases of the suspect counterfeit part.

In the case of the counterfeit Lattice chip used in the CDMU, L–3 Display Systems received it from its approved (at the time) Independent Distributor along with a test report showing that the part was authentic. When parts were sent out for retinning (a normal process even for authentic parts), the retinning facility encountered difficulty and proposed an alternative method. When L–3 Display Systems queried the OCM about the part, the OCM informed L–3 Displays that the part was counterfeit. L–3 Displays notified its customer, Alenia Aeronautica, on February 2, 2010. By May 2010, the Lattice counterfeit parts had been removed from U.S. Air Force aircraft and replaced.

In November 2010, a Samsung VRAM chip that had been previously tested and represented as authentic by a third party lab was identified as suspect counterfeit as the result of a supplemental third party independent test. This additional testing was performed after anomalies were noted during L–3 Display Systems' standard testing methodology. L–3 Display Systems notified its customer, Alenia, of the counterfeit part but that notification was not passed on to the prime contractor, L–3 Integrated Systems, until September, 2011. When L–3 IS was notified, it in turn noti-

fied its customer, the Air Force C–27J Systems Program Office. L–3 IS will take whatever corrective action its customer requests, and the current remedy is to replace the VRAM chips during normal scheduled depot maintenance unless a failure occurs for any reason that would necessitate immediate repairs.

It should be noted that there has been no discernable effect on the C–27J. The C–27J program tracks avionics performance and failures by means of a Failure Reporting And Corrective Action System (FRACAS). After analyzing the FRACAS history through this past summer, there have been no abnormal failures attributed or noticed for the affected Mission Computers, CMDUs, BAUs, or CMDS Test Sets. No degradation to performance has been observed due to these parts.

This can be partially attributed to the mechanisms put in place for the assembly, test and delivery of avionics systems in nearly all DOD procurement programs. The process of procuring piece parts and their progressive assembly from wafer to integrated circuit to circuit board to final avionics Line Replaceable Units (LRUs) or Weapons Replaceable Assemblies (WRAs) is always founded on progressive verification and testing of the item through each stage of assembly. Even at the circuit board or LRU/WRA box level, the use of complex acceptance test processes and "burn-in" (or Environmental Stress Screening) at the manufacturing plant before delivery into the DOD supply system, adds confidence that the items will perform in service and that defective parts will be identified and removed from the delivered inventory.

In the case of the C–27J JCA, there is also the benefit of contractor logistics support (CLS) for the entire maintenance of the aircraft fleet, whether in the continental United States or deployed. Whether by term of the contractual warranty provisions or by means of the CLS maintenance in the contract, the U.S. Government does not bear any cost for labor or material if the avionics systems should be affected by defective material. All costs would be borne entirely by the contractor and its suppliers.

CONCLUSION

The rise in instances of suspect and counterfeit electronic components results from a rapid turnover of technologies in the commercial and military markets, which drives critical obsolescence issues daily across all areas of the electronics supply base. This is particularly troublesome for the DOD and its need to continue to support deployed systems—a need further complicated by the extended life of these systems. These issues are constant, daily challenges not only for the industry that contracts with the DOD, but also for all of the Government service agencies throughout their various support systems.

L–3 will continue to improve its obsolescence and counterfeit parts mitigation programs by reiterating strict adherence to its corporate procedures and policies across the entire enterprise, controlling Independent Distributor purchases, and by providing training and education to our personnel. Additionally, we will continue to work with our Government and industry partners and professional associations to develop and incorporate best practices throughout the supply chain. In any case, if any part is identified as suspect, L–3 will, as it has in the past, promptly notify all of its affected customers and work with them to remediate the problem in whatever way the customer determines is needed.

Finally, while L–3 has made significant efforts over several years to address the counterfeit parts challenge, the Senate Armed Services Committee's examination of the issue has been important in underscoring the seriousness and depth of the problem and the need to rapidly develop an effective solution. L–3 looks forward to working with other companies and the committee in achieving this goal.

Chairman LEVIN. Thank you very much, Mr. DeNino. Is it Mr. Dabundo or Dabundo?

Mr. DABUNDO. Dabundo.

Chairman LEVIN. Dabundo. Mr. Dabundo, turn your mike on there, if you would. You are the Vice President and the P–8 Poseidon Program Manager at Boeing. Please proceed.

STATEMENT OF CHARLES DABUNDO, VICE PRESIDENT AND P–8 POSEIDON PROGRAM MANAGER, BOEING DEFENSE, SPACE AND SECURITY

Mr. DABUNDO. Mr. Chairman, thank you for the opportunity to appear before this committee regarding counterfeit electronic parts

in defense systems. This is a serious issue that has commanded the attention of Boeing, the defense industry, and the U.S. Government for some time. Unlike my counterparts on this panel, I do not have overall supply chain responsibilities for my company, and accordingly, Boeing requests permission to submit a separate letter that addresses in detail Boeing's policies and initiatives on counterfeit parts.

Chairman LEVIN. That will be made part of the record.

[The information referred to follows:]

Tim Keating
Senior Vice President
Government Operations

The Boeing Company
1200 Wilson Blvd. MC PS-00
Arlington, VA 22209

November 8, 2011

The Honorable Carl Levin
Chairman, U.S. Senate Armed Services Committee
United States Senate
228 Senate Russell Office Building
Washington, D.C. 20510

The Honorable John McCain
Ranking Member, U.S. Senate Armed Services Committee
United States Senate
228 Senate Russell Office Building
Washington, D.C. 20510

Dear Chairman Levin and Ranking Member McCain,

The Boeing Company commends your decision to hold a hearing to address ways to combat counterfeit parts in the U.S. military supply chain. As a recognized leader in the aerospace industry, Boeing welcomes the opportunity to participate in shaping public, industry, and military policy regarding the detection and prevention of counterfeit parts.

We begin below by summarizing Boeing's extensive efforts to address counterfeit parts—with industry to develop effective standards and specifications, with suppliers to impose stringent requirements for procurement and risk mitigation practices, particularly with respect to electronics distributors, and with employees, in the form of internal processes and training. We next briefly describe Boeing's FAA-approved quality system which efficiently produces safe, high quality commercial aircraft that serve as the platform for some government programs, such as the P-8A Poseidon.

Boeing sets the industry standard for safety, quality, and reliability of aerospace products. Our company has developed effective measures to minimize the risk posed by counterfeit parts. But we are always striving to further reduce that risk. Boeing looks forward to continuing our collaboration with industry, our government customers, and Congress to detect counterfeit parts and prevent them from compromising the vital products we make for our armed forces.

BOEING

Boeing's Efforts to Mitigate Risk Posed by Counterfeit Parts

1. Initial Industry Efforts

Boeing, along with other aerospace and defense industry members, began tackling the issue of electronic counterfeit parts in the aerospace supply chain through several concurrent efforts. First, Boeing representatives participated as members of the SAE G-19 Committee, which was initiated in November 2007 and helped develop a Counterfeit Electronic Part Control Specification. Second, Boeing representatives participated in the Aerospace Industries Association (AIA) Counterfeit Parts Integrated Product Team, which was initiated in March 2008, and with the TechAmerica Supply Chain Assurance Committee, assembled in December 2008 to respond to the government's request in November 2008 to define an acquisition framework for regulating inauthentic IT and microelectronic products.

Each of these industry groups was chartered to identify shared industry problems with globally sourced counterfeit parts and propose institutional and policy solutions to mitigate the risk of counterfeits entering the domestic supply chain. At the same time, Boeing began working on developing its own set of strategies to prevent, detect, and counteract the threat of counterfeit parts. Boeing previously had implemented traditional industry quality assurance and enforcement mechanisms, both as a quality and contracting matter, and participated in broad scale industry initiatives to ensure supply chain quality (such as the Government Industry Data Exchange Program or GIDEP), and, as a result, had infrequent encounters with counterfeit parts. In late 2009, Boeing was impacted by a counterfeit part incident that cut across several programs. That event heightened the existing sensitivity to counterfeit parts within Boeing, and the company responded by developing additional internal compliance requirements and processes to help combat counterfeit parts.

2. Combating Counterfeit Parts at their Source

Because a majority of the electronics Boeing purchases are embedded in Line Replaceable Units (LRU) and are not individually-procured electronic component piece parts, Boeing's risk is more often associated with lower tiers of the supply chain. Consequently, Boeing's strategy to address the problem of counterfeits initially focused on improving the

counterfeit risk mitigation of Boeing's first tier suppliers. In 2009, the industry standard for Counterfeit Electronic Parts, Aerospace Standard (AS) 5553, was published. AS5553 provided guidance for procurement and contract requirements, and facilitated Boeing's development of purchase contract requirements specific to counterfeit avoidance. New supplier requirements specific to counterfeit goods were released in 2010, and are being implemented on purchase contracts. The new requirements include definitions, procurement preferences and risk mitigation practices, enhanced warranties, and notification and supplier flow-through requirements. New supplier surveillance tools were also developed to verify compliance with these new requirements.

Boeing's strategy also addresses electronic distributor requirements. When electronic components are purchased, Boeing recognizes that buying from OEM or OEM-authorized distributors, while preferred, may not always be feasible (e.g., due to parts obsolescence). In February 2011, Boeing published new requirements for unauthorized distributors and parts brokers. The new requirements include specific provisions for procurement, seller flow-down, verification of purchased product, reporting, and material control and disposition. Boeing's suppliers must prove adherence to these requirements before procurement occurs. Boeing is currently working with production procurement distributors who will be transitioning to the new requirements, with approval required beginning in October 2012. Boeing's internal processes also require program-specific risk assessment and risk mitigation in the limited cases when parts must be procured from an unapproved or unauthorized distributor. Boeing's purchase contract requirements for suppliers (H900) prioritizes procurement from OEMs and OEM-authorized distributors. However, in the case that an unauthorized distributor must be used, additional documentation, inspection and testing are required to ensure part authenticity.

3. Internal Processes and Training

Boeing has also revised internal processes to mitigate counterfeit risk. A cross-functional team consisting of engineering, supplier quality, supplier management, and program representatives has been assembled to address ways to reduce counterfeit risk through an integrated process that permeates the program and product lifecycle. This network of cross-functional personnel includes many subject matter experts within the company dedicated to

collaboration across the Boeing enterprise who act as resources and share information to support anti-counterfeiting efforts. A new cross-functional process document for Boeing procurement of electronic parts from distributors was released in April 2011. Additional documents are being prepared to provide specific source selection guidance that will help minimize counterfeit risk. An electronic component part management plan is being revised to address counterfeit risk, lead-free solder, obsolescence management, and parts management for the entire enterprise. Communication bulletins and newsletters within supplier management, supplier quality and engineering have frequently highlighted counterfeit parts and associated risks.

To facilitate awareness of counterfeit risk and ensure access to the latest counterfeit awareness activities within Boeing, the industry, and the government, an internal Counterfeit Parts Team website has been developed and is constantly updated with new information. The site is available to all Boeing employees. Topics covered include internal and external communications (letters and bulletins), checklists, command media, presentations, contact lists, requirements documents, government and industry reports, industry weblinks, inspection checklists, purchase contract requirements, reporting agencies and resources, sharepoints, training, and related links.[1] Boeing representatives have also attended and participated in conferences on Suspect Unapproved Parts and Diminishing Manufacturing Sources and Material Supply that have focused on counterfeit parts and included presentations by subject matter experts on counterfeit analysis and detection, reporting, and risk reduction. These conferences help increase awareness of the need for early counterfeit avoidance practices. In addition, counterfeit subject matter experts have briefed Boeing supplier management on counterfeit risks and have been involved during supplier contract negotiations to facilitate understanding of anti-counterfeit requirements.[2]

---

[1] For suppliers, a Counterfeit Electronic Parts Avoidance web portlet has been added to the Boeing supplier portal. Communications, requirements, and training will continue to be added as needed to keep our suppliers informed of the risks associated with counterfeit parts. Boeing also participated in an industry effort with the International Aerospace Quality Group to develop a Supply Chain Management Handbook with a chapter specifically focused on counterfeit risk. An integrated supplier information system will be implemented in 2012 and will allow all Boeing functions to access and verify approved suppliers, including approved electronics distributors.

[2] Boeing follows internal and external reporting processes for sharing counterfeit part incidents across programs and with the industry. Reporting requirements also flow down to suppliers (H900). Internally, detailed processes document requirements for processing a supplier notification of escape and reporting the issue internally to ensure other programs are not at risk (BDS: PRO 6916, BPI 5575 , BPI 4564; BCA: PRO 3907, BPI 1179). For external

4. Boeing's Commitment to Combating Counterfeit Parts

Boeing recognizes that combating the problem of counterfeit electronic parts requires stakeholders from industry and government to work together. Boeing's strategy includes continuing to work closely with industry associations, regulators, and government in helping to shape aerospace standards and practices. Boeing continues to be actively involved with its industry partners in developing new aerospace industry counterfeit parts standards including:

- AS5553, "Counterfeit Electronic Parts; Avoidance, Detection, Mitigation and Disposition";
- AS6081, "Counterfeit Electronic Parts; Avoidance Protocol, Distributors" (not yet published); and
- AS6171, "Test Methods Standard; Counterfeit Electronic Parts" (not yet published).

Additionally, Boeing was involved in developing the Aerospace Recommended Practice (ARP) 6178, "Distributor Risk Assessment," and participated with the Missile Defense Agency and NASA in conducting assessments at distribution facilities. Boeing has leveraged ARP6178 in developing Boeing verification processes for distributors. Boeing is also working with industry to define new third-party AS5553 certification processes. Finally, Boeing supports policy analyses, such as the AIA white paper entitled "Counterfeit Parts: Increasing Awareness and Developing Countermeasures," published in March 2011, and a response to an Office of Management and Budget request for public comments regarding U.S. government anti-counterfeiting strategy in September 2011.

5. Policy Efforts

As stated above, Boeing has long been engaged with industry and government to identify appropriate quality assurance and acquisition policy solutions to counterfeits in the supply chain, including offering risk management solutions and thought leadership through AIA,

---

reporting of issues, Boeing uses GIDEP to exchange safety and failure data among government and industry participants, and follows process BPI 5525.

TechAmerica, and within the parameters of the GIDEP and other similar programs. Boeing has also supported, since early 2010, the ongoing efforts by DOD (Acquisition, Technology & Logistics – Material Readiness), the Intellectual Property Enforcement Coordinator's Interagency Anti-Counterfeiting Working Group, and the National Intellectual Property Rights Coordination Center to gather actionable data and provide feedback to regulators and law enforcement groups tasked with policing counterfeit goods. We hope these and other participatory efforts lead to a common set of industry tools and an effective and appropriate regulatory framework to combat counterfeit parts.

On the legislative front, Boeing supported a variety of provisions that addressed supply chain risk management in bills developed over the past three years, including Section 253, Supply Chain Strategy for Federal Cybersecurity Management included in Senate Bill S. 3480 (Collins-Lieberman, not enacted, but on the legislative calendar again for the 112th Congress), Section 806 of the Fiscal Year 2011 National Defense Authorization Act, Supply Chain Risk Management (signed into law January 2011 and authorizes DOD to exclude sources that present known counterfeit risks), and other legislative attempts to secure the supply chain from counterfeits.

Recently, a bill to prevent trafficking in counterfeit military goods, S.1228, Combating Military Counterfeits Act of 2011, was introduced in the Senate. It provides for enhanced criminal and civil penalties for knowingly introducing counterfeit parts into the military supply chain that could be expected to cause harm to national security and/or personnel. Boeing prides itself on the quality and capabilities of the products delivered to support our military customers and would support without qualification any policy that punishes those who deliberately put the nation and its service personnel at risk by introducing counterfeit parts into the supply chain. With minor alterations, Boeing believes S.1228 may provide the impetus needed to drive supply chain protection forward as a national and global priority. Iterations of similar legislative language to combat counterfeits through various enforcement mechanisms have also appeared in the PRO IP Act (S. 968) introduced in late May 2011 and the draft Stop On-line Piracy Act introduced in late October 2011. While we have not had the opportunity to fully analyze those individual pieces of legislation, Boeing has consistently supported legislative and regulatory

efforts to define a risk management policy framework to combat counterfeits and will continue to support all efforts to stem their flow.

Boeing's FAA-Approved Production Quality System

As discussed by P-8A Program Manager Charles Dabundo in his prepared statement, the P-8A leverages the commercial 737NG production system to efficiently provide high quality and proven aircraft platforms. By many measures, the Boeing 737 is the most successful large commercial jet airplane in history. Aircraft in the 737 family have accumulated more than 230 million flight hours—or more than 26,000 years in the air. No other commercial airplane family matches this record of quality and endurance. More than 5,500 Boeing 737 airplanes are in service worldwide—more than any other commercial airplane. The 737 accounts for more than one-third of Boeing's delivered in-service airplanes and 25 percent of the world's commercial airline fleet. The 737's robust safety and reliability record is among the primary reasons the U.S. Navy elected to derive the P-8A aircraft from the 737NG.

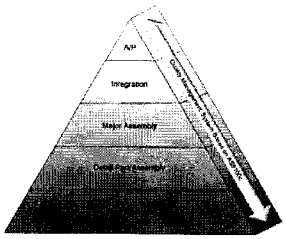
The Boeing Company has separate divisions, Boeing Defense, Space and Security (BDS) and Boeing Commercial Airplanes (BCA). The Federal Acquisition Regulations (FAR) require that a contract be in place governing the transfer of the commercial item from BCA to BDS.[3] BCA produces the 737 under its FAA-approved quality management system, and pursuant to an FAA Production Certificate. In general terms, the Production Certificate signifies that BCA has demonstrated to the FAA that it complies with Part 21 of the Federal Aviation Regulations, including that the company has and can maintain a quality control system for products to be manufactured under the Production Certificate. That system adheres to an International Quality Management System standard, AS9100 "Quality Management Systems – Requirements for Aviation, Space and Defense Organizations". BCA's multi-tiered quality control process, summarized in the following graphic, has been demonstrated through decades of use to be an effective method to maintain quality and safety.

[3] Federal Acquisition Regulations 12.001 – Definition.

BOEING

Boeing Quality Management System

- Based on the AS 9100C – Aerospace Standard
- Requirement of CFR Title 14, Part 21
- Processes and procedures approved by the FAA as a part of production certificate oversight
- Inspection and test procedures are established to validate the product conforms to type design
- Audited both internally and externally
- Encompasses the entire supply chain



One element of BCA's FAA-approved quality system addresses material nonconformities. This includes methods and requirements for nonconforming material disposition through a Nonconformance Management system, processing of notifications of escapement received from commercial suppliers, and processes for notification to the fleet when action is recommended to address the presence of nonconforming commercial parts on aircraft. In addressing nonconformities identified in the production process, BCA uses a Material Review Board that includes both quality and engineering personnel. The nonconforming product can be dispositioned by the Material Review Board in several ways, including:

- Rework: A disposition action for the reprocessing of nonconforming product to make it conform completely to requirements;
- Repair: A disposition action taken on nonconforming product so that it will fulfill the intended usage requirements, although it does not conform to the originally specified requirements;
- Standard Repair: A disposition action applied to nonconforming product using an approved Standard Repair Procedure that has been demonstrated as a cost-

BOEING

effective method to reduce, but not completely eliminate, the nonconformance and returning the hardware to serviceable condition;

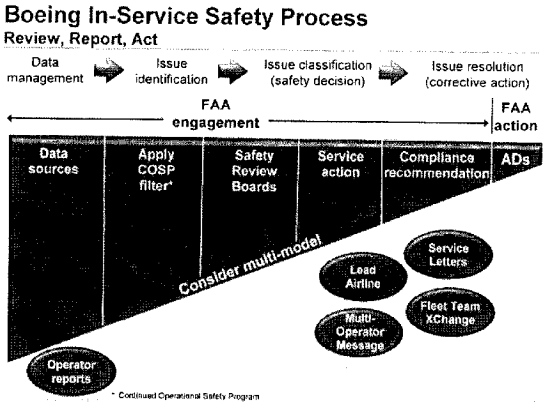
- Use-As-Is: A disposition that is used when the nonconforming item has been determined to be useable in its present state;
- Return to Supplier: A disposition that the nonconforming item shall be returned to the supplier for rework or replacement; and
- Scrap: A disposition for nonconforming product that is not suitable for its intended purpose and cannot be economically reworked or repaired.

For nonconformities discovered outside of the production process, BCA uses a Service Engineering process to determine if fleet action (for instance, via a Service Bulletin) is required or whether the nonconformity is structurally and functionally acceptable.

Boeing has supplied the committee with information about several incidents of suspect counterfeit parts that have impacted Boeing programs. The handling of those incidents demonstrates the effectiveness of the Boeing quality system. In most cases, the affected parts were caught and never installed on any U.S. military aircraft. In others, the affected parts were removed from military aircraft prior to delivery to the government. In all instances, the nonconformity was evaluated by Boeing subject matter experts and, on the few occasions in which suspect parts were found to have been delivered on aircraft to the government, a technical determination was made about whether and how long the suspect part could safely remain on the aircraft.

None of the incidents have resulted in a concern about the safety of any Boeing aircraft. However, any time there is a safety issue in the fleet, whether due to a nonconforming part or for any other reason, BCA's in-service safety process, in coordination with the FAA, provides a proven and effective method for resolving the issue. The following graphic provides an outline of the process:

BOEING



In sum, BCA operates a comprehensive, FAA-approved quality system, from supplier management through fleet action, that has proven over decades of experience to produce safe, reliable and high quality commercial aircraft, including the industry workhorse 737 which serves as the platform for the P-8A Poseidon.

On behalf of the 165,000 men and women of Boeing, thank you again for your leadership in convening a hearing to address counterfeit parts in the U.S. military supply chain. We look forward to continue our work with industry, with government, and within Boeing to address the issue.

Sincerely,

Tim Keating

Tim Keating

Senior Vice President

Government Operations

Mr. DABUNDO. Thank you, sir.

Based on my experience working at Boeing for nearly 30 years, I can say Boeing is fully committed to the safety, quality, and integrity of our products, and ensuring that those products are able to accomplish the missions required by our military and civilian customers. As an aircraft manufacturer, Boeing purchases and installs thousands of parts from suppliers. We require our suppliers to deliver a conforming product that meets our spec requirements. Addressing nonconforming products is essential, and Boeing and our suppliers have rigorous quality processes to address such parts.

The P–8 program was awarded to Boeing in 2004 and has had a longstanding track record of successful execution. The program is based on an in-line production process that leverages the commercial 737 production system and utilizes robust Government-approved military and commercial processes in accordance with the Federal Acquisition Regulations (FAR) and the contract between the U.S. Navy and Boeing Defense, Space, and Security (BDS). These processes have been a key to enabling the program to meet its program or record milestones with a safe, quality product at a cost that has been consistently below cost projections at program inception.

Boeing and our P–8 teammates have built six flight test aircraft and two ground test aircraft to date. Four of those aircraft are at the Naval Air Station in Patuxent River and have flown in excess of 1,200 flight hours, and 2 additional aircraft will be delivered to the Navy by February 2012.

The first low-rate initial production aircraft has completed its maiden flight, and it is in the final stages of installation and checkout at the BDS facility prior to delivery to the U.S. Navy in February 2012.

The program remains on track to meet IOC in 2013.

As mentioned above, leveraging the commercial production system has been a key to the success demonstrated by the program, and separate divisions of Boeing Company, BDS, and Boeing Commercial Airplanes (BCA) are required by the FAR to have a contract in place governing the transition of the commercial item from BCA to BDS. The aircraft that BDS purchases from BCA is manufactured in accordance with BCA's existing Federal Aviation Administration (FAA)-approved quality system, and once delivered to BDS, the work is completed in accordance with applicable Government quality assurance requirements. Both sets of processes are based on many years of experience with a wide range of customers and a strict focus on safety, quality, and product integrity.

Addressing nonconforming products is essential and we rely on our quality processes to identify and disposition parts that have been identified as such. Boeing treats all nonconformances with a significant level of concern to ensure that safety and integrity of the product is maintained, and this is accomplished by qualified subject-matter experts who utilize a comprehensive set of processes and procedures for addressing nonconformances encountered during the build of the aircraft. Suspect counterfeit parts represent a subset of the potential types of nonconformances and, as such, are covered within these processes.

If nonconformances are encountered during the build of the BCA commercial deliverable, the processes utilized on the P–8 are governed by BCA's quality and material review processes which are AS9100 compliant and part of an FAA-approved quality system under production certificate 700. PC 700 was issued to Boeing in 1997 for the 737NG production by the FAA after demonstration that Boeing has adequate facilities and quality control systems to ensure it meets the stringent safety and reliability requirements.

If nonconformances are encountered during the installation and checkout portion of the build that is executed by BDS, the processes utilized on P–8 are governed by BDS's quality and material review processes which are also AS9100 compliant, overseen by the Defense Contract Management Agency, and part of our Navy Air Systems Command-approved P–8 quality system plan in accordance with our contract with the Navy.

To my knowledge there have been three instances of suspect counterfeit parts that have been installed on P–8 aircraft. Two of those were assessed and dispositioned using the BCA commercial quality and engineering processes and the third using BDS quality and engineering processes. In all three cases, the safety of the P–8 and the people who operate it were not at risk and the appropriate processes were utilized by people qualified to assess and disposition these nonconformances.

So in summary, sir, suspect counterfeit parts are a serious and industry-wide issue that has affected the P–8 program. Boeing has utilized our Government-approved quality and material disposition processes to address these suspect counterfeit parts, and while BDS and BCA have slightly different quality and material disposition systems, they are both under Government regulatory control and oversight and have a pedigree that ensures the safety and integrity of the P–8 and the people who operate it are maintained at all times. That pedigree is based on many years of application on Boeing military and commercial products which have and continue to set the industry standard for safety, quality, and reliability.

That concludes my oral statement to the committee.

[The prepared statement of Mr. Dabundo follows:]

PREPARED STATEMENT BY CHARLES DABUNDO

Mr. Chairman, Senator McCain, members of the committee: Thank you for the opportunity to appear before this committee regarding counterfeit electronic parts in defense systems. This is a serious issue that has commanded the attention of Boeing, the defense industry, and the U.S. Government for some time. Unlike my counterparts on this panel, I do not have overall supply chain responsibilities for my company, and accordingly, Boeing will be submitting a separate letter that addresses in detail Boeing's policies and initiatives on suspect counterfeit parts.

Based on my experience working at Boeing for nearly 30 years, I can say that Boeing is fully committed to the safety, quality, and integrity of our products, and ensuring that they are able to accomplish the missions required by our military and civilian customers. As an aircraft manufacturer, Boeing purchases and installs thousands of parts from suppliers. We require our suppliers to deliver a conforming product that meets our specification requirements. Addressing nonconforming products is essential, and Boeing and our suppliers have rigorous quality processes to address such parts.

In this statement I will provide an explanation of how this approach was used in the three known instances of such parts being installed on P–8A aircraft. But first I'd like to set a foundation by giving a brief overview of the P–8A and our approach to execution of the program.

P–8A POSEIDON PROGRAM OVERVIEW

Boeing was selected by the U.S. Navy in 2004 to develop the P–8A, a long-range anti-submarine warfare, anti-surface warfare, intelligence, surveillance and reconnaissance aircraft. The P–8A possesses an advanced mission system that enables interoperability in the future battle space. Capable of broad-area maritime and littoral operations, the P–8A will influence how the U.S. Navy's maritime patrol and reconnaissance forces train, operate and deploy. The P–8A is being developed for the Navy by a Boeing-led industry team that consists of CFM International, Northrop Grumman, Raytheon, GE Aviation, BAE Systems and Spirit AeroSystems.

Boeing and its P–8A teammates have built six flight-test and two ground-test aircraft. Four P–8As are currently in flight test at NAS Patuxent River where they have flown in excess of 1,200 flight hours. Two additional aircraft will be delivered to the U.S. Navy for operational evaluation by February 2012. The first Low Rate Initial Production aircraft has completed its maiden flight, and is in the final stages of installation and checkout prior to delivery to the U.S. Navy fleet in February 2012. The program remains on track to meet initial operational capability in 2013.

The P–8A program is being executed by Boeing using a first-in-industry in-line production process that leverages the commercial 737NG production system. The maturity, robustness, and pedigree of this system has been a key enabler to production of a quality product that has met all program-of-record milestones, allowed the U.S. Navy to save in excess of $1 billion, and achieve a recurring cost reduction of 10 percent in Initial Production aircraft. The benefits of leveraging a mature commercial aircraft will carry forward as the P–8A is delivered to the fleet and is able to leverage the 737NG support systems.

As a testimony to the successes that the Navy-Boeing team has achieved, the P–8A program recently won Aviation Week's Program Excellence Award for System-Level Research and Development/System Design and Development based on a rigorous assessment of program practices and performance relative to peer programs. Furthermore, positive customer comments about the P–8A program's track record and successes have been numerous. At the ribbon cutting ceremony for Boeing's P–8A Installation and Checkout Facility, Rear Admiral Steve Eastburg, then Program Executive Officer for Air ASW, Assault and Special Missions Programs, and now Vice Commander for Naval Air Systems Command (NAVAIR), stated:

> "The P–8A program is quickly becoming the DOD and industry standard for how to do acquisition right. At our recent defense acquisition board, at the end of the meeting, the team was asked to come back with a composite set of lessons learned and best practices from this program that we can feed into all the other programs across the Department of Defense. That's how much confidence and such a high esteem that not only Dr. Carter but many others have in the program at the most senior levels of the DOD."

BOEING PRODUCTION SYSTEM

As mentioned above, leveraging of the commercial production system has been a key to the successes demonstrated by the P–8A program. As separate divisions of a single company (The Boeing Company), Boeing Defense, Space and Security (BDS) and Boeing Commercial Airplanes (BCA) are required by the Federal Acquisition Regulations (FAR) to have a contract in place governing the transfer of the commercial item from BCA to BDS.[1] The aircraft that BDS purchases from BCA is manufactured in accordance with BCA's existing, The Federal Aviation Administration (FAA)-approved quality system. Once delivered to BDS, BDS completes its work in accordance with the applicable government quality assurance requirements. Both sets of processes are based on many years of experience with a wide range of customers, and with a strict focus on safety, quality, and product integrity.

Addressing nonconforming products (any product that does not meet its specification requirement) is essential, and Boeing and our suppliers have rigorous quality processes to identify and review parts that we or our suppliers identify as nonconforming. Boeing treats all nonconformances with a significant level of concern to ensure the safety and integrity of the product is maintained. This is accomplished by qualified subject matter experts who utilize a comprehensive set of processes and procedures for addressing nonconformances encountered during the build of the aircraft. Suspect counterfeit parts represent a subset of the potential types of nonconformances, and as such, are covered within these processes.

If nonconformances are encountered during the build of the BCA commercial deliverable, the processes utilized on P–8A are governed by BCA's quality and mate-

[1] FAR 12.001-Definition.

rial review processes, which are AS9100 compliant and part of an FAA-approved quality system under Production Certificate 700. PC 700 was issued to Boeing in 1997 for 737NG production by the FAA after demonstration that Boeing has adequate facilities and quality-control systems to ensure it meets stringent safety and reliability requirements. AS9100 is a widely adopted and standardized quality management system for the aerospace industry.

If nonconformances are encountered during the installation and checkout portion of the build that is executed by BDS, the processes utilized on P–8 are governed by BDS's quality and material review processes which are also AS9100 compliant, overseen by the Defense Control Management Agency, and part of our NAVAIR approved P–8 Quality System Plan in accordance with our contract with the U.S. Navy.

P–8A Suspect Counterfeit Parts

I was recently interviewed by the Senate Armed Services Committee staff regarding the P–8A program's processes for handling nonconforming parts, including those that are suspect counterfeit. Parts that are suspect counterfeit that could potentially present a risk of harm to military personnel or members of the flying public are of critical concern to Boeing, and to me personally.

To my knowledge, there have been three instances of suspect counterfeit parts that have been installed on P–8A aircraft. Each of these instances was addressed in a manner that complies with Boeing's government approved processes and procedures, and our contract with the U.S. Navy. A brief summary of each is included below.

1. Ice Detection Module—Notice Of Escape January 2010

The first incident occurred in January 2010, when BAE Systems notified BCA of a nonconformance associated with the BAE Ice Detection Module (IDM) Assembly. The IDM is optional equipment used to detect ice on the exterior of the aircraft.

In accordance with Boeing's approved processes and procedures, BCA Engineering evaluated the nonconformance, dispositioned it as "No Action Required," and called for repair "on attrition," meaning that the IDM could be replaced if it needed repair for any reason. Per standard BCA approved processes, this disposition does not require action by, nor result in a notification to its contractual customer, in this case BDS. Had there been a nonconformance which created a safety concern or a required maintenance action, BDS would have been notified by BCA, and appropriate action would have been taken to comply with the associated service bulletin instruction.

I became aware of the IDM nonconformance and associated disposition in September 2011. An affected IDM was on one of the P–8A airplanes located at Patuxent River, MD (T–3). Although there were no inherent or residual safety concerns or maintenance actions associated with the IDM, BDS decided to remove and replace the IDM on T–3 at a convenient point in time that would not disrupt test activities. T–3's IDM was removed and replaced on 21 October 2011.

2. Distance Measuring Equipment—Notice Of Escape November 2010

The second incident occurred in November 2010, when Honeywell notified BCA of a potentially unapproved component contained in Honeywell's Distance Measuring Equipment (DME). The DME measures the distance between an aircraft and a ground station.

In accordance with Boeing's approved processes and procedures, BCA Engineering evaluated the nonconformance, and dispositioned it as "No Action Required," "use as is." Per standard BCA approved processes, this disposition does not require action by, nor result in a notification to its contractual customer, in this case BDS. Had there been a nonconformance which created a safety concern or a required maintenance action, BDS would have been notified by BCA, and appropriate action would have been taken to comply with the associated service bulletin instruction.

I became aware of the DME nonconformance and associated disposition in October 2011. Affected DMEs were on P–8A airplanes T–1, T–2, T–3, T–4, and T–5. Although there are no inherent or residual safety concerns or maintenance actions associated with the DME, BDS decided to remove and replace the DME on T–5 prior to delivery to the U.S. Navy. T–5's DME was removed and replaced on 3 November 2011.

3. Receiver-Exciter and HF Power Amplifier—Notice Of Escape July 2010

The third incident occurred in July 2010, when Rockwell Collins notified BDS of a potentially unapproved component contained in Rockwell Collins Receiver-Exciter and HF Power Amplifier. These parts were installed on two P–8As—T–2 and T–3.

In accordance with Boeing's processes and procedures, BDS Engineering evaluated the nonconformance, and dispositioned it as "Remove and Replace at earliest

convenience." Per standard BDS approved processes, the government was notified on 27 July 2010, and a Service Letter was issued on 11 November 2010. In accordance with the Service Letter, the nonconforming parts were removed from T–2 on 13 November 2010 and T–3 on 27 February 2011.

SUMMARY

The P–8A program, awarded to Boeing in 2004, has had a long-standing track record of successful execution. The program is executed using a first-in-industry in-line production process that leverages the commercial 737NG production system, and is based on robust, government-approved, military and commercial processes in accordance with BDS's contract with the U.S. Navy. These processes have been key to enabling the program to meet all program-of-record milestones, at a cost that has been consistently below cost projections at program inception.

Suspect counterfeit parts are a serious, industry-wide issue that has affected the P–8A program. Boeing has utilized its government approved quality and material disposition processes to address suspect counterfeit parts in an appropriate manner. While BDS and BCA each have slightly different quality and material disposition systems, they are both under regulatory control (Defense Contract Management Agency and FAA, respectively) and ensure that the safety and integrity of the P–8A and the people who operate it are maintained at all times. They also represent a pedigree based on many years of application on Boeing Military and Commercial products which have, and continue to, set the industry standard for safety, quality, and reliability.

This concludes my submitted statement to the committee. Thank you again for the opportunity to appear before you.

Chairman LEVIN. Thank you, Mr. Dabundo.

We will now recess until 2 o'clock, and for the convenience of those of you who want to take advantage of it, there is a cafeteria here, a public cafeteria, in the basement of this building that you are free to use if you so desire. So we will stand in recess until 2 o'clock.

[Whereupon, at 12:57 p.m., the committee recessed, to reconvene at 2:00 p.m.]

Afternoon Session - 2:00 p.m.

Chairman LEVIN. Good afternoon, everybody; we will come back to order.

Mr. DeNino, let me start with you. Between October 2009 and November 2010, L–3 identified two counterfeit parts in display units that it had sold to the military. When the second counterfeit was discovered in November 2010, L–3 learned from its supplier, which was Global IC in California, that both counterfeits, both the October 2009 one and the 2010 November one, had been supplied to Global IC by the same company in China called Hong Dark Electronic Trade. Global IC was the supplier to L–3.

Global IC then identified a third part which had been sold to L–3 from Hong Dark, but L–3 did not test that third part until October 2011, which is nearly a year later after you were notified. You did not test that part until after our investigation began, and you were notified of it. Now, that testing identified the third Hong Dark-supplied part as suspect counterfeit.

L–3 had already installed that third part on display units for another military aircraft.

The question is why did it take L–3 so long to test that third part?

Mr. DENINO. The third part was initially quarantined when L–3 found out back in November 2010. We had purchased 89 parts. Only three had been used. The other 86 were quarantined. The parts were to be tested, and they did not get tested until as you

indicated, until recently, and we did confirm that those parts were suspect counterfeit.

The parts—there is no real good answer on that other than the parts should have been tested and we did not. But we are taking the corrective action now. We have notified the customer, as we have with the other two incidents, and we will take whatever action is necessary to repair and replace those parts.

We have also developed a system to avoid instances like that in the future.

Chairman LEVIN. Now, what we learned is that Hong Dark had supplied parts to L–3 via Global IC on approximately 30 occasions. There was a total of 28,000 parts that had been supplied to L–3 via Global IC which had originally come from Hong Dark. You learned about that, I think, recently from staff. Is that correct?

Mr. DENINO. That is correct, Senator. We learned, with the help of the committee, that there were additional parts that Hong Dark had provided to L–3. We took action, issued a demand letter to Global IC Trading, received the information. We requested the data on October the 20th, received it on October 21. Upon receipt of that letter, we notified the affected companies of L–3 the same day, October 21, that they had parts that were suspect just by the nature of them coming from a supplier that had already provided three counterfeit devices to L–3.

The divisions took the action to go off and test parts. Many of those devices are in testing right now. We do not have any of the test results back yet. Where we do not have stock on those parts, we are looking at other data and analysis, and we will notify all customers upon completion of that.

We also took a couple other actions just to be very conservative. We checked with the suppliers that we currently have today. We only have four independent distributors that divisions can use. We went to all four to validate that. Not only did they never sell anything to us from Hong Dark, but they never purchased parts from Global IC Trading that were provided to L–3. All four confirmed that.

We then went one step deeper with another 11 suppliers that were formerly on our list of approved suppliers, and we found the exact same information.

Chairman LEVIN. Why did it take so long for you guys to ask Global IC for the information? Why did it take a committee investigation before you would ask your supplier, hey, how many times has Hong Dark been the supplier to you, Global IC? I mean, this is 30 occasions, 28,000 parts and now you are scrambling to find out where those parts are?

Mr. DENINO. We would much prefer not to be scrambling to make that determination.

Chairman LEVIN. Why did it take a committee investigation before you would ask your supplier, hey, we have three occasions now where the company that supplied you parts, this Chinese company, Hong Dark. How many other occasions have you given us parts, sold us parts that originally came from Hong Dark? Why did that take so long?

Mr. DENINO. Well, it happened when we found out about the third part, and in retrospect, it would have been better if we had

checked earlier. It was not something that was picked up. We had——

Chairman LEVIN. No, it did not happen, as I understand it, when you found out about the third part. You found out about the third part in November 2010, but until we told you during our investigation that we thought there were 30 occasions, when we learned that via Global IC, then you found that out. My question is why did you not ask Global IC how many times they had supplied you with Hong Dark parts?

Mr. DENINO. We should have done that checking on our own.

Chairman LEVIN. Now you are saying you have taken steps so that that is not going to happen again.

Mr. DENINO. Yes, we have.

Chairman LEVIN. Has L–3 determined what military systems those—I want to get the right number here—28,000 parts are on? Have you determined that yet?

Mr. DENINO. Yes, we have. The balance of the parts, roughly 6,500, are not on DOD systems. We have the information on the balance.

Chairman LEVIN. How many different systems are the balance on?

Mr. DENINO. Probably 12 to 15.

Chairman LEVIN. Have you notified the Services which 12 to 15 they are on?

Mr. DENINO. We are in the process. As I stated, we are doing the testing and we want to provide a complete package.

Chairman LEVIN. When you do that, when you provide that information to the Services, will you let this committee know.

Mr. DENINO. We would be pleased to.

Excuse me, Senator. I would just like to add one other comment.

Chairman LEVIN. Sure.

Mr. DENINO. Of those 28,000, roughly 14,000 have already been identified, and that information has been provided to the committee.

Chairman LEVIN. Of which systems?

Mr. DENINO. This is on the VRAM and Lattice chips on the C–27J and the C–130J.

Chairman LEVIN. Let me get to that in a minute.

But you have identified, you believe, 12 to 15 systems that those parts are on?

Mr. DENINO. As a max. We will provide detailed information.

Chairman LEVIN. Can you tell us some of those systems now?

Mr. DENINO. General Dynamics, L–3050V. There is a thermal imager, MK–46, sold to Kollmorgen.

Chairman LEVIN. Do you know what that goes on, what weapons system that is a part of?

Mr. DENINO. I do not——

Chairman LEVIN. That is okay. Keep going then. We will figure it out.

Mr. DENINO. There are some spares for Northrop Grumman.

Chairman LEVIN. For what? What system, do you know?

Mr. DENINO. Global Hawk Maritime Demonstration, and there is also Global Hawk, and Raytheon Excalibur, and Raytheon Missile Systems, and United Launch.

Chairman LEVIN. Do you know what system for United Launch?

Mr. DENINO. I do not, sir.

Chairman LEVIN. How about the Raytheon Missile Systems? Do you know——

Mr. DENINO. I do not.

Chairman LEVIN. The Global Hawk has some suspect parts on it?

Mr. DENINO. There is one part that was provided that is being tested. It is suspect only in that it came from Hong Dark.

Chairman LEVIN. Which is a pretty good reason to be suspicious, would you agree, given their history?

Mr. DENINO. That is why we are having it tested. Yes.

Chairman LEVIN. Do you know if Raytheon was notified of that suspect part that you just told us about before today?

Mr. DENINO. Not yet at this point. The parts are being tested. We have quarantined whatever stock on any of these parts exist in our facility.

Chairman LEVIN. How long is it going to take to be tested?

Mr. DENINO. I suspect everything will be complete within 2 weeks.

Chairman LEVIN. On September 19, just about 2 months ago, a month and a half ago, L–3 Integrated Systems, the prime contractor for the C–27J, notified that Air Force of a suspect part on eight 27Js, including two that are in Afghanistan. Is it true that you did not notify the Air Force of that because you were not aware of it until the committee's investigation?

Mr. DENINO. That is correct. We had properly notified our customer—our Displays Division had.

Chairman LEVIN. But did the Displays Division notify the Air Force?

Mr. DENINO. No, they did not.

Chairman LEVIN. Do you know why?

Mr. DENINO. They did not notify the Air Force because Displays' customer was not the Air Force. It was Alenia, and Displays, upon finding out the problem, which they found out on their own, quarantined the parts, had them tested, confirmed that there was a suspect, wrote the GIDEP, provided notification.

Chairman LEVIN. When did they find that out?

Mr. DENINO. Can you just confirm the date of the part, please?

Chairman LEVIN. Okay.

Mr. DENINO. The date that you stated. Was it September?

Chairman LEVIN. No. The date of the notice to Alenia.

Mr. DENINO. Oh, I am sorry. It was December 16, 2010.

Chairman LEVIN. Now, Alenia was supplying that component, were they not, to L–3 Integrated Systems?

Mr. DENINO. That is correct.

Chairman LEVIN. So L–3 is the prime on that. Did L–3 Display, which found the problem, notify its sister corporation or sister——

Mr. DENINO. They did not.

Chairman LEVIN. Why would they not do that?

Mr. DENINO. The responsibility was to notify the customer. We recognized, through the efforts of the committee, that there could be improvement in our own system, and this probably applies across the board in our industry. So we are implementing a revised system so that when we have a failure or a suspect counterfeit de-

vice, I personally will be notified through the system. We will know from that system—we are modifying an existing process that we have to add data so that we can make the determination on where those parts are used upstream and we can put in place a closed loop system.

Chairman LEVIN. So everybody in your own company and its components will know when there is a suspect counterfeit part.

Mr. DENINO. That is correct.

Chairman LEVIN. That was not the case at that time.

Mr. DENINO. No. We knew that there was a suspect counterfeit part, and notification had been issued.

Chairman LEVIN. But not to your own——

Mr. DENINO. Not to our own company. To our customer.

Chairman LEVIN. I understand, but inside of your company, you did not notify the prime which was also a subsidiary of L–3.

Mr. DENINO. That is correct. There was no process in place to do that.

Chairman LEVIN. That is another process that you put in place now.

Mr. DENINO. Yes, sir.

Chairman LEVIN. Now, do you know whether or not the reporting system, GIDEP, was notified of the counterfeit by L–3 Displays?

Mr. DENINO. Yes, they were. A GIDEP report was issued on December 20, 2010.

Chairman LEVIN. So that was put into the GIDEP system.

Mr. DENINO. Yes, it was.

Chairman LEVIN. Do you use GIDEP for every counterfeit you find or just some of the time?

Mr. DENINO. No. It is not used on every device.

Chairman LEVIN. Why is that?

Mr. DENINO. We will be using GIDEP going forward. As you have probably seen from the GAO report, there are challenges with the GIDEP system primarily. GIDEP is not designed for counterfeit parts. GIDEP handles all sorts of issues and nonconformances on everything across the spectrum. It is not specific to electronic components.

Chairman LEVIN. But it includes——

Mr. DENINO. Yes. It includes.

Chairman LEVIN. Is it now your plan to utilize that system for every suspect counterfeit part you discover?

Mr. DENINO. We will be using both GIDEP and ERAI.

Chairman LEVIN. But GIDEP you are going to use for every counterfeit now?

Mr. DENINO. Yes, we will.

Chairman LEVIN. Mr. Dabundo, let me ask you a couple questions now about Boeing.

Boeing found out about the suspect counterfeit part in the ice detection module on the P–8 in January 2010. On August 17, 2011—that is more than a year and a half later—Boeing finally notified the Navy. That in that book of yours, if you need to look at it, is tab 28. The notification says, "priority critical," and quote, "it is suspected that the module may be a re-worked part that should not have been put on the airplane originally and should be replaced

immediately." So Boeing had known for more than a year and a half that the "critical," in its words, problem existed.

Why did it take a year and a half to recommend the removal of that part?

Mr. DABUNDO. Sir, if I may walk you through a little bit of the chronology of that part. As you noted, BAE notified Boeing via a notice of escape in January 2010. That notice of escape initiates the engineering investigation between Boeing and BAE, in particular, the BCA engineering group. BCA in February initiated a suspect discrepancy report that indicated that there were no safety concerns identified with that part and may require correction during the service life. So at that point in time, that was the overall assessment of the part.

Chairman LEVIN. So you knew it was a suspect counterfeit part, but you did not think there was a concern about that at that time.

Mr. DABUNDO. I am not aware if at that time it was a suspect counterfeit part or a nonconforming discrepant part.

Chairman LEVIN. Why would it have been a nonconforming part? Was it not tested?

Mr. DABUNDO. I do not know the details. I am sure there was an ATP, a test that is done prior to delivery of the part to Boeing, but at the time they were doing the engineering investigation as to the cause of the failure that occurred initially in the BCA factory in December 2009.

Chairman LEVIN. Before you go on, the notice that I think you referred to in January 2010 from BAE said that the parts show, "signs of resurfacing." This is in tab 26, by the way—signs of resurfacing, repainted metal tabs, bent leads, peeling coating. They said that the chips were, "unacceptable for use" and that "BAE Systems recommends replacement of the suspect components." That is what Boeing was told by BAE. Is that not enough to test it to see if it is a counterfeit?

Mr. DABUNDO. Well, that was enough to initiate the engineering investigation that ensued by both the BCA and the BAE engineers.

Chairman LEVIN. Boeing is BCA. Right? It is part of Boeing.

Mr. DABUNDO. Boeing Commercial.

Chairman LEVIN. I would just as soon use the term "Boeing."

So Boeing then said that what? According to tab 27, it may have a somewhat lower reliability. Right? So you got your sub saying it is unacceptable for use. You have your own engineers believing it may be less reliable. That is tab 27. Then, nonetheless, you do not do anything.

Mr. DABUNDO. I think, sir, the pertinent information that goes with that is in June 2010 when BAE did issue the final service bulletin that came out of the investigation, it indicated that there could be a long-term reliability concern, that it was not a safety issue, and said to do the rework that was provided in that service bulletin at customer convenience and customer option. In coordination with BAE, the BCA final suspect discrepancy report, which came out in July 2010, indicated that there was no action required and that the part could be repaired on an attrition basis.

Chairman LEVIN. So you are saying that in June 2010 that BAE said that there was no need to replace the part? They changed

their mind from January 2010 when the notice to Boeing said that BAE Systems recommends replacement?

Mr. DABUNDO. Their verbiage in the draft service bulletin that was—or I am sorry—the final service bulletin that came out in June 2010 indicated it was a long-term reliability concern and do at customer convenience/customer option.

Chairman LEVIN. "Do" Is that the word?

Mr. DABUNDO. Do the rework that was defined in that service bulletin at customer convenience/customer option.

Chairman LEVIN. The customer's option was not to replace it.

Mr. DABUNDO. Correct.

Chairman LEVIN. Then you decided apparently—in tab 28, Boeing decided priority critical. So you changed your mind. Is that correct? Take a look at tab 28.

Mr. DABUNDO. I am familiar with——

Chairman LEVIN. It is suspected that the module may be a reworked part that should not have been put on the airplane originally and should be replaced immediately.

Mr. DABUNDO. Right. So that message——

Chairman LEVIN. What changed between July 2011 when you decided that you would just go with it I guess? You were supposed to give the customer the option, but who is the customer here?

Mr. DABUNDO. In that particular case, the customer was Boeing Commercial Airplanes (BCA).

Chairman LEVIN. Did they give their customer—did the Government ever have the option of replacing this part? Was the U.S. Government, which was also a customer—was it given the option of replacing this part? Were they notified of the part?

Mr. DABUNDO. They were notified in August 2011.

Chairman LEVIN. The Government was notified.

Mr. DABUNDO. The Government was notified.

Chairman LEVIN. By?

Mr. DABUNDO. By Boeing via the message that you were quoting.

Chairman LEVIN. Until then—so it was a year and a half later now—was the Navy notified for that year and a half?

Mr. DABUNDO. Not to my knowledge, and the rationale for that was the final disposition that came out of BCA Engineering who were the qualified folks to make the disposition on that type of nonconformance was that there was no action required and the part could be repaired on an attrition basis.

Chairman LEVIN. But the customer was supposed to be notified and they were not for a year. Right? Is that correct?

Mr. DABUNDO. No, sir. The way that the——

Chairman LEVIN. Let me go through the chronology. The Navy was notified on August 17, 2011. Right?

Mr. DABUNDO. Correct.

Chairman LEVIN. This part was discovered by Boeing in January 2010. Right?

Mr. DABUNDO. Yes. That is when Boeing was——

Chairman LEVIN. The customer was not notified until August 2011, and that is the Navy. Those are the facts. Right?

Mr. DABUNDO. Correct.

Chairman LEVIN. How do you justify that? You got a critical part here which by your own notice is critical, but they were not notified

for a year and a half after it was suspected there would be deficient defective, and as it turns out, a phony part. How do you justify the year and a half?

Mr. DABUNDO. So again, the way that our commercial processes work, there is notification made to the end customer, which in this case would be BDS and the Navy, if there is a safety concern or a functionality impact. In this case with the IDM, there was not a safety concern or a functionality impact associated with the nonconformance, and so the philosophy that they use in the commercial industry is that the notification occurs when there is an actionable piece of action that goes to the maintenance departments.

Chairman LEVIN. When there was a notification in August 2011——

Mr. DABUNDO. Right. So that notification came, I believe, via awareness to this that came through the Navy talking to the committee and then the committee talking to BDS. So that——

Chairman LEVIN. However it came, your notice says that the part may be a reworked part that should not have been put on the plane originally. Is that true?

Mr. DABUNDO. That is what that document says.

Chairman LEVIN. Is that a Boeing document?

Mr. DABUNDO. That is a Boeing document, and if you go through the details of that document, there is conflicting wording in the message that you are quoting. In the first sentence, it says replace at next available opportunity, and then in the second sentence, it says replace immediately. With that confusing language, we did go back and verify with the cognizant engineering group, the experts, BCA in this particular instance, that there were no safety concerns. It was a long-term reliability issue. Their recommendation was to repair on attrition, but because of the concerns raised by the customer, we decided to issue that message to drive a maintenance action to move forward and remove and replace that part.

Chairman LEVIN. So you do not agree that a problem which has not yet appeared and may be a long-term problem represents a safety concern.

Did you hear the general today tell you that just because there is a long-term problem, you just do not know when that term is going to occur? You do not know when the axe is going to fall. You know that it can meet a current test, but you do not know for how long. If it is counterfeit, it could fail at any time. So the fact that it meets a current test, if it is known to be counterfeit, which you guys knew, is not a reason to allow a part to stay in a plane because it may not fail. It may fail but it may not fail. You are kind of shooting the dice with the mission and the lives of our people here. So did you hear what the general said about your approach that long-term means you can do this even though it is a counterfeit with all the problems of counterfeit parts and the likelihood of failure sooner?

Is it Boeing's position that you are just going to continue the way you have been going and you are not going to replace counterfeit parts?

Mr. DABUNDO. We evaluate every nonconformance on a case-by-case——

Chairman LEVIN. Including counterfeits.

Mr. DABUNDO. It is a subset of nonconformance. Suspect counterfeit parts is a subset of nonconformance.

Chairman LEVIN. Right.

Mr. DABUNDO. We have processes that have been used on our products. We have experts who execute those processes. We rely on those folks to make the judgment calls with respect to these situations.

Chairman LEVIN. The Navy told Boeing on October 31, 2011 that, "any counterfeit material received is nonconforming material and shall be immediately reported to the Government". Do you believe you have a contractual obligation to report counterfeits to the Government immediately?

Mr. DABUNDO. If there is a safety or a functionality concern, we would report that to the Navy.

Chairman LEVIN. Only if in your judgment there is a safety concern, which you do not think there is if it is long-term and you do not know when the axe is going to fall. So if you make a judgment it is not immediate, it could happen next month, it could happen the month after, we do not know when it is going to happen, but you know it is counterfeit. You do not feel you have an obligation to immediately report that to the Government.

Mr. DABUNDO. I will just again reiterate the processes that we use.

Chairman LEVIN. No. I want you to just tell me whether Boeing believes that you have an obligation, as the Navy says in their letter to you of October 31, to immediately report to the Government any nonconforming material. Period. They do not say whether in your judgment it is a safety concern. They say any counterfeit material received is nonconforming and shall be immediately reported to the Government. You are saying, well, we are not going to follow that requirement if we in your judgment believe it is not an immediate safety concern. So that is my question.

Mr. DABUNDO. That statement does not flow from our contractual documentation.

Chairman LEVIN. Until it does, you are not going to abide by it.

Mr. DABUNDO. No, sir.

Chairman LEVIN. Pardon?

Mr. DABUNDO. We abide by that for safety-related issues.

Chairman LEVIN. Only if in your judgment it is safety-related, and if it is a future safety problem and not a current one, in your judgment, you are not going to do what the Navy says that you must do which is to report any counterfeit material immediately to the Government. You just disagree with the Navy.

Mr. DABUNDO. Sir, we received this letter a week ago, and we are actively looking at the statements that they have made. Our plan is to engage in discussions on this letter with them to really make sure we fully understand where they are coming from. Our track record on the program has been to work with the customer through these types of things, and I believe that we will do that in this particular instance.

Chairman LEVIN. Well, let me tell you where we are coming from. There is no justification—no justification—for not notifying the Government when you know there is a counterfeit. In fact, I think by law you are required to do that, by the way. I think we

have a system for it. In any event, you got a customer here, a pretty good customer. It is the Navy. The Navy has told you that they interpret your obligation contractually to notify the Government when you have reason to believe that material is counterfeit, and you got to report it to the Government. I would think just in terms of good business practice that you would say, okay, we are going to report that to the Government.

Now, we are going to try to change the law so that it is not going to be up to you as to whether or not something represents a safety concern or not. That has to be up to the customer, in this case the Navy, because it cannot be your unilateral decision that, well, this is not necessarily an immediate safety problem in our judgment. The axe can fall months from now. We do not know, and we will replace it during our usual service process. It is not good enough. You have customers here, and the customers ultimately are the men and women in uniform. But the Navy and the other Services represent those folks, and if they say that you have an obligation to let them know immediately of counterfeit parts, from a pure business practice I would think you should do that.

Now, the contract with the Navy includes a requirement, section 52.211–5, that "used, reconditioned, or remanufactured supplies may be used in contract performance if the contractor has proposed the use of such supplies and the contracting officer has authorized their use". Did you ask the contracting officer here to authorize the use of counterfeit or used parts?

Mr. DABUNDO. No, sir. That particular clause is something that is explicitly required of us as to not be flowed to commercial end items, and we did not.

Chairman LEVIN. It does not apply you are saying? That did not apply?

Mr. DABUNDO. For the commercial end item, it did not apply.

Chairman LEVIN. For commercial. This is military.

Mr. DABUNDO. I am sorry. What is the question?

Chairman LEVIN. This is commercial? You are saying it does not apply in your commercial contracts?

Mr. DABUNDO. Yes, sir. As I stated in——

Chairman LEVIN. But this is a military contract.

Mr. DABUNDO. The contract between BDS and the U.S. Navy is a military contract. We obtain the P–8 airframe from Boeing Commercial as a commercial end item.

Chairman LEVIN. What does that have to do with what you supply the Navy? It says here the Navy contract with Boeing has a requirement that you must propose the use of used or reconditioned or remanufactured supplies and you must be authorized to do that. You were not given authority here.

Mr. DABUNDO. Yes. The way that the FARs direct us to implement that commercial contract, they state that we shall rely on the existing quality system as a substitute for compliance with the Government inspection requirements and the clause that you are referring to. So——

Chairman LEVIN. You shall comply with the current contract—with the current what system? Read that again. You shall comply with the current.

Mr. DABUNDO. We shall rely on the contractor's existing quality system, in this case our commercial quality system, as a substitute for compliance with Government inspection requirements.

Chairman LEVIN. That is unconditional. So in your contract, it said they are going to rely on your own quality system.

Mr. DABUNDO. The existing commercial quality system. The difference in the commercial quality system is they do not notify customers of nonconformance unless there is an explicit maintenance action to be taken or there is a safety concern. They do that. They intentionally filter out nonactionable messages so that it is clear when there is an action to be taken by the maintenance department.

Chairman LEVIN. The P–8 is built in a facility of Boeing which is apparently been certified to aerospace standards, the number being 9100B, which is a widely adopted quality management system for the aerospace industry. I think that is the one you are referring to.

The standard states that nonconforming material—that is surely the counterfeit parts in the P–8—shall not be used, "unless specifically authorized by the customer if the nonconformity results in a departure from the contract requirements." The contract requirements here require new material.

Mr. DABUNDO. In this instance——

Chairman LEVIN. Therefore, you cannot rely on your aerospace standard 9100B.

Mr. DABUNDO. I think the PC700 is really the FAA approval that enables us to use the quality system.

Chairman LEVIN. That quality system allows you to use used parts—is that what you are saying—without authority from the customer?

Mr. DABUNDO. It allows us to disposition all nonconformances, and as I mentioned, the process basically provides information to the end user when there is an action to be taken.

Chairman LEVIN. You are saying that the existing commercial rules allow you to use used material without notice to the customer.

Mr. DABUNDO. They allow us to use our existing quality system which does not require notification.

Chairman LEVIN. If that is the situation, number one, I think the Navy is going to be pretty shocked to hear that you are not going to let them know about counterfeits.

Second, we are going to change it. I mean, if that is currently—despite what the Navy says, you are obligated to notify them of nonconformities, including counterfeits, the Navy is wrong in their letter to you, and if you want to ignore a customer like the Navy, go your own way, and argue that, we are going to change it by law. We have to do it.

Now, do you know whether we paid full price for these used parts?

Mr. DABUNDO. BAE is covering the cost of replacing those parts.

Chairman LEVIN. All right. But did we pay full price originally for these parts?

Mr. DABUNDO. I do not know.

Chairman LEVIN. Let me read something that Xilinx, which is the part maker has to say about the part here. I think this is the best answer to your comment that if you decide unilaterally that you are going to replace the parts through attrition, that that is a safe way to proceed. Here is what Xilinx, who is the manufacturer of the real parts, has to say about these anomalies and about the risks of using them.

Number one, that "the devices are of dubious origin. These cases pose a significant reliability risk. There are many potential damage mechanisms that could have affected the devices. Some of these could be catastrophic. Others may create a damaged mechanism that is latent for an undetermined amount of time. The combination of these events calls into question the integrity of the devices. Though the devices may initially function, it would be next to impossible to predict what amount of life is remaining." That is the company that made the original parts. It is impossible to predict what amount of life is remaining—and then they finished—or what damage may have been caused to the circuitry.

Does that trouble you to hear that?

Mr. DABUNDO. Sir, I am not a reliability expert.

Chairman LEVIN. Well, just as a citizen who cares about men and women in uniform, does it trouble you that the original parts maker here says they do not know how long this part is going to last if it is a counterfeit part? It is impossible to predict what amount of life is remaining. Some of the risks could be catastrophic and so forth. Does that not just trouble you kind of as a citizen?

Mr. DABUNDO. I am a concerned citizen and I am very concerned about the counterfeit parts problem. In the case of the Ice Detection Module, there were people with expertise both at BAE and Boeing who evaluated that part. Also, in consideration, that part is not a safety-critical item on the P–8 or on the commercial 737.

Chairman LEVIN. The Xilinx part? They are wrong about——

Mr. DABUNDO. The ice detector module.

Chairman LEVIN. They are wrong about their own part?

Mr. DABUNDO. I am talking about the ice detector module as a unit on the P–8.

Chairman LEVIN. Are you talking about what Xilinx is referring to, or do you not know?

Mr. DABUNDO. I am not familiar with the Xilinx——

Chairman LEVIN. With that particular part that they supply on the P–8. You are not familiar with the Xilinx part on the P–8.

Mr. DABUNDO. No. I believe that is provided to BAE or one of their sub-tiers.

Chairman LEVIN. You do not think that that part got into the ice detection module?

Mr. DABUNDO. I do not know.

Chairman LEVIN. If it did, would that trouble you what I just read?

Mr. DABUNDO. If it did, it would trouble me and we would want our engineering experts to assess that part and the associated module and make a disposition on it to ensure the safety of the aircraft was maintained.

Chairman LEVIN. Double check with your engineers and get back to us, will you, as to whether the ice detection module is a safety issue or not?

Mr. DABUNDO. I have, sir.

Chairman LEVIN. They do not think it is a safety issue?

Mr. DABUNDO. That is correct.

Chairman LEVIN. Why do you think the Navy puts these modules there if it is not a safety issue? Why are we paying money for an ice detection module if it does not relate to the safety of the plane?

Mr. DABUNDO. It has a functionality that is not a direct safety impact. Sir, they did evaluate the reliability aspects of the module and its failure mode and effects and determined that there was not a residual safety concern and recommended replace on an attrition basis.

Chairman LEVIN. No, I understand all that. You repeated that a few times. I am just asking you why are we buying the ice detection module if it is not a safety issue, if it is not for the safety of the plane and the pilot and the crew? Why are we laying out all this——

Mr. DABUNDO. It has a function——

Chairman LEVIN.—to Boeing. Why are you taking our money?

Mr. DABUNDO. The ice detection module does have a function that is not safety-related.

Chairman LEVIN. What is it? What is it for? Just to help steer the plane? I mean, what is it for?

Mr. DABUNDO. It gives the pilot an indication if there is ice building up on the exterior of the airplane.

Chairman LEVIN. Does an ice buildup create a safety issue? Or do your engineers ice buildup does not create a safety issue?

Mr. DABUNDO. I am not an expert in that system, sir.

Chairman LEVIN. You say your engineers have said that ice buildup is not a safety issue.

Mr. DABUNDO. They have stated that the ice detector module nonconformance did not create a safety issue.

Chairman LEVIN. Which means in your understanding that ice buildup is not a safety issue.

Mr. DABUNDO. I cannot make that claim. I am not a qualified icing engineer.

Chairman LEVIN. Are they making that claim?

Mr. DABUNDO. I do not know. I did not ask that explicit question.

Chairman LEVIN. I would suggest you not make these decisions, and you are not allowed to make these decisions unilaterally. You have to notify the Government when you have counterfeit parts, and if you think you do not under existing contracts or under existing laws, then you are either wrong, or I think it is bad business to make the argument, or we are going to change it, because one of those three things, it seems to me, has to be the case.

Mr. DABUNDO. Sir, we are looking at the counterfeit parts issue across all the divisions of the company and implementing policies that will help detect and control those parts.

I will say we read the Navy's letter to us loud and clear and we will engage with them, as we have done in the past, to have discussions and really understand where they are coming from and what we collectively need to do to address those concerns.

Chairman LEVIN. It does not sound here like you got a loud and clear message at all, to me. I mean, you say that it is a loud and clear message. I thought it is a loud and clear message too, but I do not think it has been received, other than you are now saying it is received, from anything you have testified to earlier. It just seems to me that you are trying to defend something which is indefensible.

Mr. DeNino, let me get back to you, if you would. When you interviewed with the committee staff, staff asked why it is important for L–3 to prohibit the purchase of refurbished parts for use in defense systems. Your answer was, "because of the risk, the associated risk. Plain and simple, the risk if that part isn't going to function the way it is supposed to."

Now, then we asked L–3's chief engineer for the C–27J program why they had not committed immediately to removing and replacing the counterfeit parts on the C–27J, and he said L–3's acceptance testing process would show whether a part was functional or not.

Now, given the risk that you cited, should L–3 not offer to immediately replace suspect counterfeit parts in the display systems that it sold to the military?

Mr. DENINO. L–3 did offer to replace the parts. We have provided notification to the customer, and we are working with the customer to replace the parts. It is not a question of will we. It is a matter of when and how.

Chairman LEVIN. When did you tell the military again?

Mr. DENINO. I want to clarify that you are talking about the device on the C–27J.

Chairman LEVIN. Right.

Mr. DENINO. This was the notification to the customer that took place on or around September 19.

Chairman LEVIN. You are waiting to hear back from them?

Mr. DENINO. I just want to clarify that is the question, that is the device you are speaking about.

Chairman LEVIN. Yes.

Mr. DENINO. Okay. Yes. I know that our L–3 Integrated Systems Division is working closely with their customer to work those issues and to take the corrective action. But L–3 has been clear with the multiple people that have been interviewed that we will replace those parts at no cost to the Government, to the customer, and it is just a matter of working through those issues with the customer.

Chairman LEVIN. Okay, thank you.

Mr. Kamath, just a few questions for you. I mentioned in my opening statement that Raytheon manufactures a FLIR, an infrared system that is used on the Navy's SH–60B helicopter for missile targeting and night vision. The committee's investigation uncovered, as I mentioned, a suspect counterfeit electronic part in three FLIR's provided to the Navy. We tracked the counterfeit through this maze of subcontractors and parts suppliers all the way back to a company called Huajie Electronic Limited in Shenzhen, and this supply chain is in tab 1 of the binder in front of you.

Before this investigation, had you ever heard of Huajie Electronic Limited?

Mr. KAMATH. Mr. Chairman, no, I had not.

Chairman LEVIN. Are you surprised that Raytheon's supply chain is as convoluted as this, considering that the parts are destined for a critical system?

Mr. KAMATH. Mr. Chairman, I think I would characterize, given all the testimony we have heard today, it would not surprise me that there was a supply chain that is convoluted, using your words.

Chairman LEVIN. Is that something that we ought to worry about?

Mr. KAMATH. Absolutely, yes, sir.

Chairman LEVIN. I think you testified that Raytheon requires all of its suppliers and subcontractors to purchase parts from the original equipment or component manufacturer or an authorized dealer or to obtain advance permission from Raytheon to purchase from an independent distributor. Is that correct? I think you testified to that.

Mr. KAMATH. That is correct, Mr. Chairman.

Chairman LEVIN. So you are able then to take risk mitigation measures, additional testing when it knows parts have been purchased from a source that is not the component manufacturer or their authorized distributor. The subcontractor who sold Raytheon the subsystem containing the suspect part failed to seek permission from Raytheon to buy the part outside of authorized channels.

I believe that you talked about your experience prior to being employed by Raytheon, I may say, and seeing factories, huge factories with 10,000 employees that were set up to manufacture counterfeit parts. Is that correct?

Mr. KAMATH. Mr. Chairman, as you have heard with other testimony today, it is my observation. It is what I recall from the time that I visited China, yes.

Chairman LEVIN. That was before you worked for Raytheon.

Mr. KAMATH. Several years ago and before I worked for Raytheon, yes.

Chairman LEVIN. Now, well, just tell us in your own words. Is it a concern to you and should it be a concern to all of us that counterfeit parts are used in defense systems and that they are coming from China?

Mr. KAMATH. Mr. Chairman, I think our larger concern is that we have counterfeit parts, period, in the——

Chairman LEVIN. Regardless of where they come from.

Mr. KAMATH. Regardless of where it is coming from. I think that was made clear by all the panelists today.

Chairman LEVIN. I think we would all agree with you. Most of it comes from China, so that is obviously our primary concern.

But when you were there, did it appear to you that there was any concern about the counterfeiters being shut down by the Chinese Government, or was it open?

Mr. KAMATH. Mr. Chairman, I mean, it is the same recollection I think Tom Sharpe had. It appeared to be the same.

Chairman LEVIN. Open.

Mr. KAMATH. Open.

Chairman LEVIN. Raytheon identified to the committee a counterfeit part that was installed on a system that was sold by Raytheon to General Dynamics. It was intended for the Stryker mobile gun system vehicle. It costs Raytheon $750,000 to remediate that counterfeit part. Raytheon has identified a total of 32 counterfeit parts in its supply chain since 2009. Is that correct?

Mr. KAMATH. 32 instances.

Chairman LEVIN. 32 instances. More than 32 counterfeit parts. 32 instances?

Mr. KAMATH. That is correct, Mr. Chairman.

Chairman LEVIN. Do you know how much money this counterfeiting has cost Raytheon?

Mr. KAMATH. Mr. Chairman, we have not calculated the number.

Chairman LEVIN. It is a significant amount?

Mr. KAMATH. I have no way to know, sir.

Chairman LEVIN. Now, does Raytheon report counterfeit parts to GIDEP?

Mr. KAMATH. It is our practice to either issue a GIDEP or to ensure that a supplier issues a GIDEP every time we know that there is a confirmed counterfeit part.

Chairman LEVIN. Does the failure by other companies to report counterfeits into the GIDEP system increase the risk that Raytheon will inadvertently buy counterfeit parts?

Mr. KAMATH. Mr. Chairman, I think this is a larger issue. I think we talked about it today. I think the GIDEP is only as good as its usage by everybody that is a member. I think the consistent usage of GIDEP certainly makes it a better tool.

Chairman LEVIN. If it is not used by some people and used by others, it is less valuable.

Mr. KAMATH. We do not have the value of getting more information through the system.

Chairman LEVIN. I talked to you, Mr. DeNino, before about whether L–3 reports counterfeit parts that they find to GIDEP. I think your answer was that you do but not 100 percent of the time. Is that fair?

Mr. DENINO. In the past, that is correct.

Chairman LEVIN. But now you are going to do it 100 percent of the time?

Mr. DENINO. We are going to use GIDEP.

Chairman LEVIN. 100 percent of the time?

Mr. DENINO. 100 percent of the time.

Chairman LEVIN. What about Boeing?

Mr. DABUNDO. Sir, I am familiar with the GIDEP process very top level, but I do not have insight into the detailed workings of that process.

Chairman LEVIN. Do you know whether that suspect counterfeit part in the detection system was put into the GIDEP system? Do you know?

Mr. DABUNDO. I do not.

Chairman LEVIN. It did not, by the way. I mean, we have checked it out. Boeing did not file a GIDEP report, and I think the testimony of our witnesses here is that the failure to file a GIDEP increased the risk that another defense contractor or DOD may inadvertently purchase a counterfeit part. I think that is just a fact

of life. I mean, would you agree, to the extent people do not use that system, it is less valuable?

Mr. DABUNDO. Yes.

Chairman LEVIN. Mr. DeNino, let me ask you about something in your written testimony. I am not sure it was in your oral testimony. I think it was relative to the C–27J. You appear to explain the continued use of counterfeit parts by pointing to the screening of L–3's display units through acceptance testing or burn-in. I am wondering—and I asked this already of Mr. Dabundo—about General O'Reilly's testimony this morning. He told us it is just not enough to hope the parts will be screened out through acceptance testing. Were you here for that?

Mr. DENINO. Yes, I was, sir.

Chairman LEVIN. He said that some counterfeit parts that include the correct die but are actually used parts can pass acceptance tests, be fielded, and result in a reliability risk. Do you disagree with him?

Mr. DENINO. I do not disagree with that statement.

Chairman LEVIN. Thank you all. You have heard a discussion today about the problem which I think everybody recognizes as a major problem that jeopardizes the well-being and safety of our troops and the success of their mission. We are going to act, I hope, in the next couple weeks on the defense authorization bill.

I have outlined today what my ideas are and I think there is a lot of support for those ideas in terms of we have to have a certification system in place for parts that do not come from the original manufacturer or their authorized dealer.

We have to do something to inspect parts from China at the border because they are the predominant source of the counterfeiting and they are obviously not doing anything about it. I do not want to rely on them to do something about it.

We also have to make it clear that where the counterfeit parts end up in a system, that it has to be the contractor and the contractor's suppliers that have to be responsible for making the corrections. It cannot be the taxpayers of the United States.

We would welcome any comment that you have either now or, if you wish, you can provide to the committee later about these suggestions. Feel free to do so.

I think this investigation and the great work of our staffs has shown that we have a problem. It is a serious problem. We have an obligation to act, to do something about it. We know that DOD has been working doing something in the counterfeiting area for a long time, but we are not willing to wait any longer. So we will be asking them to help us to put into amendment form and legislative form the kind of ideas which have been discussed here this morning.

Again, we would welcome any comment that you might have either now or that you might want to submit to the committee in the next couple days.

Let me close by asking any of you if you would like to comment on any of those suggestions at this time.

Mr. DENINO. We will be providing a comment, and I would just like to thank the entire committee for their efforts. This is a critical

issue for us, and we look forward to working with the committee going forward. Thank you.

Mr. KAMATH. Mr. Chairman, the same thing here. I think we would like to provide comments as quickly as you would like.

Chairman LEVIN. Well, make it within the next week because this bill could come to the floor within another week.

Mr. KAMATH. That works for us. We will work with your committee staff on this.

Chairman LEVIN. Feel free to do so.

Mr. Dabundo?

Mr. DABUNDO. Sir, Boeing did provide some input beyond the statement that I made, and we do welcome participating with the committee to help find good solutions.

Chairman LEVIN. Any comments that you might want to make on the legislative ways to change the status quo here we would be happy to look at. I think you heard a lot of determination on the part of this committee today that—a lot of shock, frankly. Some of this is stunning. It is the only word I could use. Some of the GAO testimony is just absolutely stunning what is available there on the Internet. Phony numbers will be filled. I mean, these counterfeiters will do anything, obviously. They will stoop to anything. They will do anything.

I know you all have your hands full in trying, even if you put forth an adequate effort, which I do not think has been the case, but nonetheless, even if you do put forth an adequate effort to screen out the counterfeits from this flood of counterfeits, it is still going to be a challenge.

So we are going to do everything we can to stymie and stop this at the source. It is going to be a two-track effort on our part, and we will welcome your cooperation with both tracks. We will stand adjourned with our thanks.

[Questions for the record with answers supplied follow:]

QUESTION SUBMITTED BY SENATOR CARL LEVIN

1. Senator LEVIN. Mr. DeNino, please provide a list of all military systems (including the quantity of each type of system) for which electronic parts that L–3 received either directly from Hong Dark Electronic Trade or through an intermediary supplier were intended. If known, identify the military systems (including the quantity of each type of system) into which the parts were integrated.

Mr. DENINO.

3/4/2012

Global IC Trading Group Parts Supplied to L-3 Sourced from Hong Dark Electronic Trade

L-3 Division	Manufacturer Part # (and date code) of the Suspect Counterfeit Part at Issue	Name of L-3 System Containing the Part at Issue	Quantity of L-3 Systems Shipped Containing the Part	Name of the DoD Program that the L-3 System is Incorporated into	Quantity Shipped to DOD Incorporating the Part in Question
ACSS	[redacted]	TCAS 2000	2	USAF C-5AMP	Unknown
		TCAS 2000	1	RQ-4B Global Hawk	Unknown
	[redacted]	ATDL/IFF Transponder	1	USAF C-12 (shipped to L3 Vertex)	1
		ATDL/IFF Transponder	1	U.S. NAVY Inventory Control Point - NAVY ICP	Unknown
	[redacted]	TCAS 2000SP	3	General Atomics Predator Demonstrator	Unknown
		T2CAS	1	USAF C-12 (shipped to L3 Vertex)	1
		TCAS 2000	1	USAF C-5AMP	Unknown
		T2CAS	12	Taiwain P-3C, FMS Program	Unknown
		TCAS 2000	5	Global Hawk	Unknown
	[redacted]	None	Parts not used.	None	0
	[redacted]	None	Parts not used.	None	0
	[redacted]	Non-DOD	Not used in DOD programs	None	0
	[redacted]	None	Parts not used	None	0
Cincinnati Electronics	[redacted]	KOLLMORGEN MK-46 THERMAL IMAGER	3	US NavyMK-46 Optical Site System	Unknown
		KOLLMORGEN PMP THERMAL IMAGER	37	US Navy Photonics Mast System	Unknown
		KOLLMORGEN CG-47 THERMAL IMAGER	18	US Navy MK-20 Electro Optical System	Unknown
		KOLLMORGEN NIGHTCONQUEROR 640	17	US Navy Integrated Submarine Imaging System (ISIS)	
		GDLS MOBILE GUNSIGHT	130	US Army Stryker Mobile Gun	Unknown
		BAE NIGHTCONQUEROR IR CAMERA	1	US Army Unknown Program	Unknown
		BOOZ ALLEN HAMILTON NIGHTCONQUEROR 256	3	US Army Unknown Program	Unknown
		TEXTRON NIGHTCONQUEROR	3	US Air ForceCobra Ball	Unknown
		BOEING AVENGER THERMAL IMAGER	4	AVENGER	Unknown
	[redacted]	KOLLMORGEN MK-46 THERMAL IMAGER	3	US Navy MK-46 Optical Site System	Unknown
		KOLLMORGEN PMP THERMAL IMAGER	37	US Navy Photonics Mast System	Unknown
		KOLLMORGEN CG-47 THERMAL IMAGER	18	US Navy MK-20 Electro Optical System	Unknown
		KOLLMORGEN NIGHTCONQUEROR 640	17	US Navy Integrated Submarine Imaging System (ISIS)	
		GDLS MOBILE GUNSIGHT	130	US Army Stryker Mobile Gun	Unknown
		BAE NIGHTCONQUEROR IR CAMERA	1	US Army Unknown Program	Unknown
		BOOZ ALLEN HAMILTON NIGHTCONQUEROR 256	3	US ArmyUnknown Program	Unknown
		TEXTRON NIGHTCONQUEROR	3	US Air force Cobra Ball	Unknown
		BOEING AVENGER THERMAL IMAGER	4	AVENGER	Unknown
	[redacted]	KOLLMORGEN MK-46 THERMAL IMAGER	3	US Navy MK-46 Optical Site System	Unknown
		KOLLMORGEN PMP THERMAL IMAGER	37	US Navy Photonics Mast System	Unknown
		KOLLMORGEN CG-47 THERMAL IMAGER	18	US NavyMK-20 Electro Optical System	Unknown
		KOLLMORGEN NIGHTCONQUEROR 640	17	US Navy Integrated Submarine Imaging System (ISIS)	
		GDLS MOBILE GUNSIGHT	130	US Army Stryker Mobile Gun	Unknown
		BAE NIGHTCONQUEROR IR CAMERA	1	US Army Unknown Program	Unknown
		BOOZ ALLEN HAMILTON NIGHTCONQUEROR	3	US ArmyUnknown Program	Unknown
		TEXTRON NIGHTCONQUEROR	3	US Air Force Cobra Ball	Unknown
		BOEING AVENGER THERMAL IMAGER	4	AVENGER	Unknown
	[redacted]	THERMAL IMAGING SENSOR ASSY (TISA)	107	US Army Lightweight Laser Designator Rangefinder	Unknown
	[redacted]	KOLLMORGEN MK-46 THERMAL IMAGER	3	US Navy MK-46 Optical Site System	Unknown
		KOLLMORGEN PMP THERMAL IMAGER	37	US Navy Photonics Mast System	Unknown
		KOLLMORGEN CG-47 THERMAL IMAGER	18	US Navy MK-20 Electro Optical System	Unknown
		KOLLMORGEN NIGHTCONQUEROR 640	17	US Navy Integrated Submarine Imaging System (ISIS)	
		GDLS MOBILE GUNSIGHT	130	US Army Stryker Mobile Gun	Unknown
		BAE NIGHTCONQUEROR IR CAMERA	1	US Army Unknown Program	Unknown
		BOOZ ALLEN HAMILTON NIGHTCONQUEROR 256	3	US Army Unknown Program	Unknown
		TEXTRON NIGHTCONQUEROR	3	US Air ForceCobra Ball	Unknown
		NGLS THERMAL IMAGING SENSOR ASSY (TISA)	155	US Army Lightweight Laser Designator Rangefinder	Unknown
		BOEING AVENGER THERMAL IMAGER	4	AVENGER	Unknown

123

[redacted]/2012

Global IC Trading Group Parts Supplied to L-3 Sourced from Hong Dark Electronic Trade

L3 Division	Manufacturer Part Number Supplied to L-3 Sourced Component Part Number	Sourced L-3 System Component Part Number	Quantity of L-3 Sourced Delivered Containing the Parts	Name of the DoD Program that the L-3 System is Incorporated into	Quantity Required to DoD Incorporation Per Each Question
Communication Systems - West	[redacted]	CATE CART	1	US Air Force Global Hawk	Unknown
		MODEM TAGE ASSY	2	US Navy Global Hawk	Unknown
	[redacted]	AIRBORNE MODEM ASSY - DUAL BAND	1	US Navy P-3 FMS	1
		AIRBORNE MODEM ASSY DUAL BAND	4	US Navy P-3	4
		CIRCUIT CARD ASSY - NETWORK INTERFACE CONTROLLER	1	US Navy P-3 FMS	2
		CIRCUIT CARD ASSY - GIFP NETWORK INTERFACE CONTROLLER	2	US Navy P-3 AUSTRALIAN RETROFITS	2
		CIRCUIT CARD ASSY - VIDEO	3	US Air Force Gorgon Stare	Unknown
		CIRCUIT CARD ASSY - MPEG-2 ENCODER-DECODER	2	US Army Warrior	Unknown
		MODEM ASSY - DUAL-LINK AIRBORNE	1	US Navy P-8A	Unknown
		MODEM ASSY - DUAL-LINK AIRBORNE	4	US Navy P-8A	Unknown
		GROUND SECURE TERMINAL EQUIPMENT	1	US Army Bell 407 Datalink	Unknown
		LINK INTERFACE ASSEMBLY	5	US Air Force FFT Iraqi AF	Unknown
		MICROWAVE MODEM ASSY	7	US Army Warrior	Unknown
		MICROWAVE MODEM ASSY	12	US Army Warrior	Unknown
		AIRBORNE MODEM ASSY - DUAL BAND	1	US Navy SPAWAR FMS P-3 TCDIN	1
		LINK INTERFACE ASSEMBLY	1	US Navy SAIL IDIQ	1
		CIRCUIT CARD ASSY SPARES MODEM	8	US Navy Tactical/Mobile	8
		SECURE TERMINAL EQUIPMENT	8	US Navy Tactical/Mobile	8
Display Systems	[redacted]	Color Multipurpose Display Unit	40	US Air Force C-27J	Unknown
		Color Multipurpose Display Unit	29	US AF C-130J	Unknown
	[redacted]	Single Avionics Management Unit	59	US Air Force C-27J	Unknown
		Communication Navigational Radio Panel	25	US Air Force C-27J	Unknown
		Multifunction Display	9	US Air Force T-38 COMBS	Unknown
		Electronic Engines Display	5	US Air Force T-38 COMBS	Unknown
		Vertical Instrument Display	2	Boeing Demo AH-6J	Unknown
		Vertical Instrument Display	3	Special Operations Force A/MH-6M	3
	[redacted]	Color Multipurpose Display Unit	98	US Air Force C-27J	Unknown
		Color Multipurpose Display Unit	376	US Air Force C-130J	Unknown
		Multifunction Color Display	62	US Air Force C-130J	Unknown
		Display Unit	1	US Air Force C-17	Unknown
		Horizontal Mover Situational Indicator	1	US Marine Corps CH-46	1
		Electronic Flight Instrument	2	US Air Force C-130H	Unknown
		Electronic Flight Instrument	11	US Air Force C-130H	Unknown
		Electronic Flight Instrument/Radar Display Unit	6	RAAF C-130H	Unknown
		Multifunction Display	21	US Air Force U2	Unknown
	[redacted]	Electronic Countermeasures Officer	2	US Air Force EA6B	Unknown
		Pilot Display	1	US Air Force EA6B	Unknown
Interstate Electronics	[redacted]	GPS Receiver	660	Excalibur	Unknown
Ruggedized Command & Control	[redacted]	CCA - CPU Board	49	General Dynamics Inventory	Unknown
Telemetry West	[redacted]	PMC Bit Sync Modules - Test Equipment	1	L-3 TE Test Equipment	Unknown
		PMC Bit Sync Modules - Test Equipment	1	Rolling Airframe Missile (RAM) (NATO-Germany)	Unknown
		PMC Bit Sync Modules - Test Equipment	2	US Air Force - United Launch EELV Program	Unknown
		PMC Bit Sync Modules - Test Equipment	1	International Commercial Sales - Japan	Unknown
		PMC Bit Sync Modulies - Test Equipment	4	DOE - Sandia Laboratories	Unknown
Communication Systems - East	[redacted]	Audio amplifier for speakerphone	12,499	STE phone	12,499 speakerphone amplifiers

PATTON BOGGS LLP

2550 M Street, NW
Washington, DC 20037-1350
[redacted]
Facsimile [redacted]
www.pattonboggs.com

March 2, 2012

John J. Deschauer, Jr.
[redacted]

Senator Carl Levin, Chairman
Senator John McCain, Ranking Member
United States Senate Committee on Armed Services
Washington, D.C. 20510-6050

Dear Chairman Levin and Senator McCain:

Re: Global IC Trading Group Parts Supplied to L-3 Sourced from Hong Dark Electronics Trade

This is in response to your email dated February 25, 2012. All but one of the parts identified on the chart were sent to SMT Corporation for testing. The other part, Xilinx XCR3128XL-7CS144I, Date Code 0509, was tested at 4Star Electronics, Inc. Testing was performed on all the parts from November 2011 through early 2012.

The testing houses identified all but two of the parts as suspect counterfeit. The two parts that were not deemed suspect counterfeit are the ST Micro SD8257-01, Date Code 0105 and the Freescale MC34119EFR2, Date Code 0812.

L-3 has notified the affected customers and is working with them on the appropriate resolution.

Please contact me at [redacted] or my partner, Mike Nardotti at [redacted] if you have any questions.

Sincerely,

John J. Deschauer, Jr.

Encls.

cc: Michael J. Nardotti

5223629

ANNEX

[The documents for the November 8, 2011, hearing on Counterfeit Electronic Parts in the Department of Defense Supply Chain follow:]

Index of Documents for November 8, 2011 Hearing on Counterfeit Electronic Parts in the Department of Defense Supply Chain

1. Flow chart for Raytheon Company FLIR supply chain.

2. Image of FLIR on SH-60B Helicopter.

3. August 1, 2011 letter from Technology Conservation Group to Senate Armed Services Committee informing the Committee that suspect counterfeit parts were sold to Texas Spectrum Electronics.

4. August 23, 2011 letter from Raytheon Company to Senate Armed Services Committee informing the Committee that suspect counterfeit parts were integrated in Forward Looking InfraRed (FLIR) systems sold to the U.S. Navy.

5. September 8, 2011 letter from Raytheon Company to the U.S. Navy informing the U.S. Navy that suspect counterfeit parts were integrated in FLIRs sold to the U.S. Navy.

6. September 27, 2011 letter from the U.S. Navy to Raytheon Company requesting removal of the affected sub-systems.

7. September 30, 2011 letter from Raytheon Company to the U.S. Navy confirming the affected sub-system.

8. August 22, 2011 email from Fairchild Semiconductor to Raytheon Company concluding that the origin of the parts are questionable.

9. October 20, 2011 Senate Armed Service Committee Letter to Fairchild Semiconductor and October 25, 2011 Response Letter from Fairchild Semiconductor to Senate Armed Services Committee regarding the authenticity and reliability of the suspect counterfeit parts.

10. Flow chart for L-3 Communications display unit supply chain.

11. Image of Color Multipurpose Display Units (CMDU) in C-27Js and C-130Js.

12. October 31, 2011 letter from the Senate Armed Services Committee to the Secretary of the U.S. Air Force regarding counterfeit parts sold to the U.S. Air Force for the C-27J and C-130J.

13. February 2, 2010 letter from L-3 Display Systems informing Alenia Aeronautica of the first counterfeit part (Lattice components) supplied by Hong Dark.

14. L-3 Display Systems Counterfeit Parts History Card on the Lattice part (posted on the L-3 Intranet).

15. December 16, 2010 letter from L-3 Display Systems informing Alenia North America of the second counterfeit part (Samsung memory chip) supplied by Hong Dark.

16. November 9, 2010 testing report of the Samsung memory chip that failed on a fielded aircraft.

17. December 20, 2010 report on the Samsung memory chip, filed by L-3 Displays in the industry-accessible Government Industry Data Exchange Program (GIDEP) database.

18. L-3 Display Systems Counterfeit Parts History Card on the Samsung memory chip (posted on the L-3 intranet).

19. September 16, 2011 document detailing Internal Corrective Actions taken by L-3 Displays in response to the counterfeit Samsung memory chip.

20. September 19, 2011 letter form L-3 Integrated Systems to the U.S. Air Force providing notice of suspect parts on the C-27J aircraft.

21. November 10, 2010 email from Paul Meyers of Global IC Trading Group to L-3 Communications disclosing that Hong Dark Electronic Trading of China was the supplier of both the Lattice and Samsung counterfeit parts.

22. June 24, 2011 letter from Global IC Trading Group to Senate Armed Services Committee listing electronic parts that Global IC sold to customers from suppliers who had previously provided them with suspect counterfeit parts.

23. October 20, 2011 letter from Senate Armed Services Committee to Samsung Semiconductor Inc. and November 7, 2011 response Letter from Samsung Semiconductor to Senate Armed Services Committee regarding the authenticity and reliability of the suspect counterfeit parts.

24. Flow chart for The Boeing Company ice detection module supply chain.

25. January 12, 2010 BAE Systems Supplier Corrective Action Request issued to Tandex Test Labs relating to counterfeit chips purchased from Tandex.

26. January 7, 2010 BAE Systems Notification of Escape issued to The Boeing Company relating to the suspect counterfeit chips on ice detection module.

27. Undated Boeing SDR Closure Template relating to Boeing assessment that suspect counterfeit chips on ice detection module may have lower reliability.

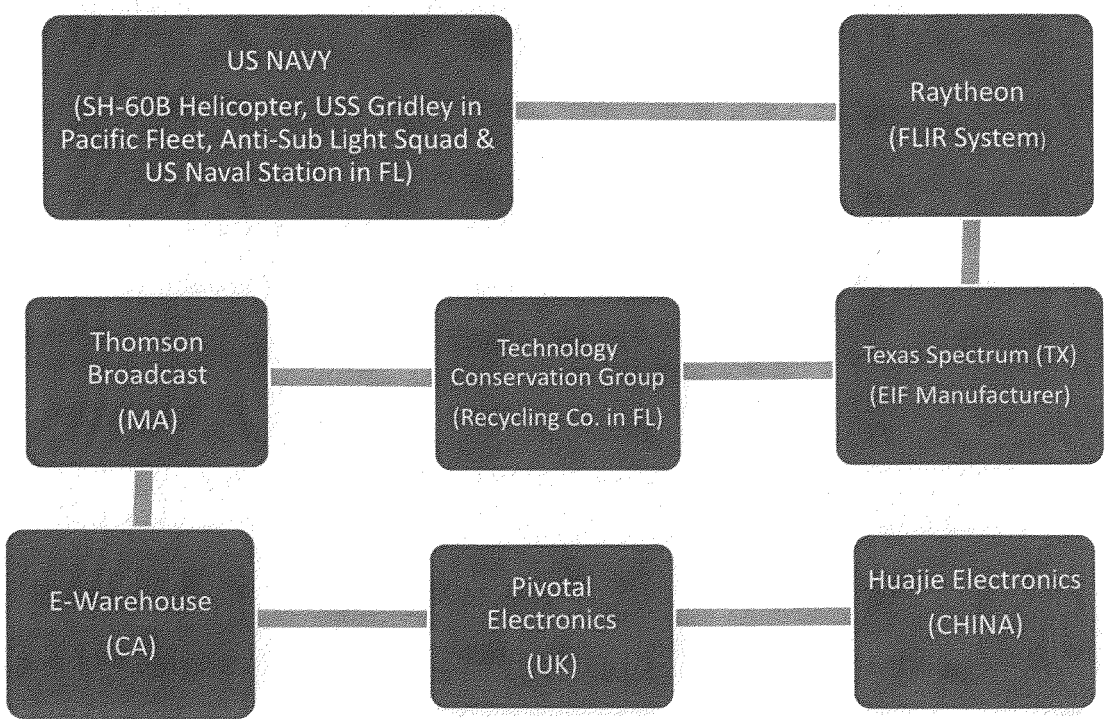
28. August 17, 2011 The Boeing Company message alerting the Navy to the presence of suspect counterfeit part on P-8 aircraft.

29. October 31, 2011 letter from Department of the U.S. Navy to The Boeing Company regarding Boeing's obligation to report counterfeit parts.

30. October 20, 2011 letter from Senate Armed Services Committee to Xilinx, Inc. and October 26, 2011 response letter from Xilinx, Inc. to Senate Armed Services Committee regarding the authenticity and reliability of the suspect counterfeit parts.

31. December 23, 2010 Boeing document describing suspect counterfeit chips in Distance Measuring Equipment (DME).

Supply Chain for Suspect Counterfeit Parts in FLIR for U.S. Navy SH-60B Helicopter



Raytheon

Photo of FLIR on SH-60B Helicopter

TURRET UNIT(WRA-1)

HAND CONTROLLER (WRA-3/4)

ELECTRONICS UNIT (WRA-2)

RAYTHEON PROPRIETARY
FOIA CONFIDENTIAL TREATMENT REQUESTED

TAB 3

TECHNOLOGY CONSERVATION GROUP
Office of the General Counsel
715 S. Easy Street
Lecanto, FL 34461
Office: [redacted]
Fax:
Toll Free: 877-926-8824
www.tcgrecycling.com

August 1, 2011

VIA EMAIL

United States Senate
Committee on Armed Services
Washington, DC 20510-6050

Re: Investigation into counterfeit electronic parts;
Fairchild [redacted]

Dear Chairman Levin and Committee Members:

We are in receipt of your request for information regarding the aforementioned part sold to Global IC Trading Group on or about July 27, 2010. In particular, you have asked specific questions with regard to this transaction that are addressed below.

Our records indicate that the parts were received as part of a shipment from Thomson, Inc. ("Thomson"), 104 Feeding Hills Road, Southwick, Massachusetts. The shipment was booked for pickup on or about February 25, 2010 under PO26813-2, and was received at our Louisville, Kentucky facility on March 3, 2010. The material received was pulled, sorted and weighed. Seventy-two pounds of miscellaneous inventory was recorded, among which were 342 pieces of Fairchild [redacted] semiconductors. On June 3, 2010, Purchase Invoice PI-23612 was issued to Thomson for the shipment in its entirety. After calculating the value and costs, a total sum of $134.08 was remitted to Thomson. This sum does not appear to have included any value paid for the miscellaneous inventory.

Before a part is listed, several processes are conducted as required by our procedures. I have included our confidential and proprietary work instructions for New Inventory; Sort, Package and Label New Inventory, and; Research eWorksheet. These work instructions indicate the processes that would have been followed up to the point of listing with regard to the 342 pieces in question. Once sold, the parts would have gone through an additional quality control visual and scope inspection to review for the quality measures indicated in the Sort, Package, and Label New Inventory instruction. If a part is suspected to be counterfeit, that part is isolated in a

TECHNOLOGY CONSERVATION GROUP
Office of the General Counse
715 S. Easy Street
Lecanto, FL 34461
Office: [redacted]
Fax:
Toll Free: 877-926-8824
www.tcgrecycling.com

separate locked holding area, is sent for testing by a third party, and if confirmed counterfeit all like pieces scrapped. If informed by a customer of a suspected counterfeit part, we follow the same process upon return of the product by the customer. In this case, there was no indication that the part in question was counterfeit.

On May 27, 2010, following all required research and inquiry, the 342 pieces of Fairchild [redacted] semiconductors were entered into our inventory system as available for purchase. On July 19, 2010, Texas Spectrum Electronics, Inc. ("Spectrum") purchased 60 pieces at $1.00 each and was issued Sales Invoice #SI-44444. On July 27, 2010, Global IC Trading Group ("Global IC") issued Purchase Order #14791 for 60 pieces at $0.84 each. On July 28, 2010, TCG issued Sales Invoice #SI-44688 for those pieces and shipped via 2nd day air. On August 20, 2010, Purchase Order # PO-102158 was received from Sigma Technology Inc., Ltd. ("Sigma") for the remaining 222 pieces in inventory.

On August 23, 2010, an issue was raised by Global IC regarding the quality of the pieces received. On August 24, 2010, Sigma cancelled its purchase after reviewing photographs of the pieces. Based upon the subsequent quality concerns noted by Global IC and Sigma, the pieces were determined to have higher scrap value then resale value and on August 24, 2010, TCG scrapped the remaining 222 pieces in its inventory. On September 2, 2010, a credit memorandum was issued to Global IC for the 60 pieces, and on September 27, 2010, the 60 returned pieces were also scrapped. To scrap, the items were placed into a 55 gallon drum of like parts and sent directly to Xstrata Recycling, Inc. for smelting. No return was requested or received from Spectrum.

Should you have further questions, please contact me.

Sincerely,

Michele L. Lieberman
General Counsel

TAB 4

Confidential Treatment Requested by Raytheon Company
Consistent with FOIA and Senate Rules [1]

Raytheon

Mark T. Esper, PhD
Vice President,
Government Relations

Raytheon Company
1100 Wilson Blvd.
Suite 1500
Arlington, VA 22209

August 23, 2011

Via Hand Delivery

The Honorable Carl Levin, Chairman
The Honorable John McCain, Ranking Member
United States Senate
Committee on Armed Services
Washington, DC 20510-6050

Dear Chairman Levin and Ranking Member McCain:

Raytheon Company ("Raytheon") recognizes the critical importance of ensuring that the electronic parts contained in the products and systems used by the United States Armed Forces are safe, reliable, and effective. As such, we fully support the Committee's efforts to look into the issue of counterfeit parts in the Defense Department supply chain. As the Senate Armed Services Committee's (the "Committee's") inquiry proceeds, we look forward to continuing to work with you to mitigate the risk that counterfeit electronic parts pose to the Nation's security.

On August 16, 2011, Raytheon received a request for information from Ozge Guzelsu, of the Committee's staff, regarding Electromagnetic Interference Filters (EIFs) delivered to Raytheon from Texas Spectrum Electronics (TSE). The following sets forth Raytheon's responses to the questions received:

Concerning Raytheon part number 3169762-0001 REV R, as referenced in Raytheon purchase orders dated June 8, 2010 and June 21, 2010:

1. For what purpose did Raytheon use the EIFs that were purchased from TSE?

Raytheon purchased the EIFs from TSE to fulfill open orders on the Light Airborne Multipurpose System (LAMPS) program, which provides a control unit that supports a Forward Looking InfraRed (FLIR) System for domestic and international customers.

---

[1] Raytheon Company ("Raytheon") requests that this letter and accompanying documents be retained and protected as if submitted in a closed hearing consistent with Senate Rule XXVI(5)(b)(5) and (6) and Rules 4(e) and (f) and 10(f) of the Rules of Procedure of the Committee on Armed Services, as disclosure of this commercial or financial information would cause undue injury to the competitive position of Raytheon. Some of the documents included in this production are subject to export controls under applicable International Traffic in Arms Regulations ("ITAR") and therefore cannot be provided or disclosed outside of the United States or to a foreign person without proper U.S. Government approvals. This production also contains documents that may be subject to Export Administration Regulations ("EAR"). Raytheon also asks that the letter and accompanying documents be protected from disclosure consistent with 5 U.S.C. § 552(b)(4) on the grounds that they contain confidential commercial and financial information. Raytheon further requests that in the event the Committee seeks to disclose part or all of (1) this letter or (2) the accompanying documents bearing Bates numbers RTN_CPR003042-003054, that Raytheon be notified in advance of such potential disclosure so that Raytheon may have the opportunity to object to such disclosure and work with the Committee to protect any trade secrets or confidential commercial and financial information from public disclosure.

2. Were the EIFs integrated into systems sold by Raytheon?

TSE shipped eight EIFs to Raytheon in December 2010. Six of the eight EIFs have been integrated into systems which have been sold by Raytheon. Of the remaining two EIFs, one has been integrated into a system, but has not yet been delivered. The other EIF is in Raytheon's inventory. Both of the remaining EIFs have been quarantined.

2A) If yes, were the EIFs integrated into systems that were sold to the Department of Defense or other U.S. government agencies?

The following is an account of the six EIFs that were integrated into systems and sold by Raytheon:

- *Three EIFs were sold to Fujitsu of Japan in support of the Japanese Ministry of Defense.*
- *The other three EIFs were sold to the US Navy.*

2B) If yes to 2A above, were any safety, performance, or reliability issues identified for these systems due to the EIFs? Please provide documents that discuss or note any safety, performance, or reliability issues for these systems due to the EIFs.

Raytheon is not aware of any safety, performance, or reliability issues identified for these EIFs. It is Raytheon's understanding that all eight EIFs passed acceptance testing at TSE, including vibration, burn-in, electrical testing, and inspection prior to shipment to Raytheon. In addition, prior to shipment from Raytheon, all eight EIFs passed additional electrical testing and inspection.

3. Where are the EIFs currently? Please provide documents that reflect where the EIFs are currently.

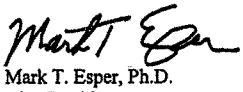
- *Three of the eight EFIs have been delivered to Fujitsu in Japan.*
- *Another three of the eight EFIs have been delivered to US Navy locations in Mayport, Florida (2) and Sasebo, Japan.*
- *Two of the eight EFIs remain at Raytheon in Jacksonville, Florida*

In support of its responses set forth above, Raytheon submits herewith documents bearing Bates numbers RTN_CPR003042-003054.

Raytheon also includes within this paragraph additional background information that might be useful to the Committee. Raytheon first learned of a potential counterfeit product issue related to these EIFs on August 12, 2011 from TSE. At this time, Raytheon is not aware of any evidence indicating that these eight EIFs are counterfeit. However, Raytheon will continue to work with TSE to investigate this issue and, if requested, will provide any additional information to the Committee.

If Raytheon can be of further assistance as your inquiry continues, feel free to contact me.

Sincerely,



Mark T. Esper, Ph.D.
Vice President
Government Relations

TAB 5

Raytheon

Raytheon Company
2501 W. University
M/S 8024
McKinney, TX 75070
USA

8 September 2011

In Reply Refer to:
11-40022-463-1310

Department of the Navy
NAVSUP Weapon Systems Support
700 Robbins Ave.
Philadelphia, PA 19111-5098

ATTENTION: Ms. Kathy Andrews
Contracting Officer

SUBJECT: Suspect Counterfeit Parts Notice

REFERENCE: (a) Contract N00383-03-D-006A-0008; AN/AAS-44 Performance Based Logistics (PBL)

Dear Ms. Andrews,

SUMMARY

Raytheon Company has become aware of suspect counterfeit components used in five (5) Electro-Magnetic Interference (EMI) Filters (P/N 3169762-0001) having been sold to the US Navy as part of the AN/AAS-44(V) PBL program. These EMI Filters are used on the AN/AAS-44(V) FLIR Converter Control WRA2 (P/N 3154212-1). Of the five EMI Filters, three (3) have entered the AN/AAS-44(V) FLIR PBL supply chain, via recently repaired units out of FRCSE Jacksonville facility. The remaining two (2) EMI Filters have been quarantined, one at the Raytheon-McKinney facility and the other at the FRCSE-Jacksonville facility. Both EMI Filters are undergoing testing. This notice is being provided to the US Navy for information only. Raytheon does not recommend replacing these suspect counterfeit EMI Filters at this time.

BACKGROUND

The EMI Filters, used on the AN/AAS-44(V) PBL program, are from Texas Spectrum Electronics (TSE). The suspect counterfeit component at issue, inside the EMI Filter, is a Fairchild MOSFET, part number [redacted], date code 0548. The five (5) EMI filters were supplied to Raytheon by TSE, under PO 4200275227 dated 09 June 2010. Around 24 January 2011, Raytheon received the five (5) EMI Filters ordered and subsequently shipped them to our third party logistics provider (AAR Defense Systems & Logistics) to support AN/AAS-44(V) PBL repairs at FRCSE – Jacksonville. Unbeknownst to Raytheon, around 19 JULY 2011, the Senate Armed Service Committee (SASC) identified TSE's component supplier, Technology Conservation Group Incorporated (TCGI), a parts broker, as having provided TSE with the suspect counterfeit Fairchild MOSFETs. On 15 August 2011, Raytheon was notified by TSE of the suspect counterfeit MOSFETs used in the EMI filters. Raytheon did a subsequent analysis of the status of the EMI Filters purchased and discovered that three (3) of them were incorporated into the AN/AAS-44(V) FLIR fleet via prior repairs out of FRCSE Jacksonville. It is our understanding, from TSE, that all suspect counterfeit EMI Filters passed acceptance testing at TSE, including vibration, burn-in, electrical testing, and inspection prior to shipment to Raytheon. Further, The WRA2's that shipped from FRCSE passed all Acceptance Testing prior to shipment after repairs were completed. Raytheon Quality Assurance is in the process of issuing a GIDEP alert regarding this incident. The two (2) remaining EMI Filters are now under Raytheon control and are quarantined. They will not enter the AN/AAS-44(V) repair supply chain. Their current status is as follows:

- EMI Filter S/N 0488 was shipped to Raytheon-McKinney on 31 August 2011 for further testing, and
- EMI Filter S/N 0489 was shipped to FRCSE-Jacksonville and is installed in a test asset to confirm laboratory testing of the suspect counterfeit part. The installation of the EMI filter in the test asset is to simulate the filter's performance and reliability at full system operation and to have the EMI filter undergo typical electrical loads and accrue operational hours to assess reliability performance.

The most current status of the suspect counterfeit EMI Filters is provided under **TABLE I**, below:

TABLE I. SUSPECT COUNTERFEIT PARTS SHIPMENTS

EMI SERIAL NO.	CURRENT STATUS	SHIP DATE	SHIP TO (DoDAAC)
0487	Shipped in WRA2 TKW00066	16 June 2011	U.S. Naval Station Mayport, FL (N60201)
0488	Pulled from inventory and quarantined	N/A	Resident at Raytheon-McKinney
0489	Removed and installed in lab asset for testing	N/A	Resident at FRCSE – Jacksonville under Raytheon control
0490	Shipped in WRA2 TKW00036	09 March 2011	Sasebo DET (SW3143)
0491	Shipped in WRA2 TKW00079	01 June 2011	HSL 60 Mayport (N60201)

At this time, Raytheon continues to assess the impact of the incorporation of these suspect counterfeit EMI Filters in the fielded systems. Should they fail, the Converter Control WRA may or may not fail. However, a failure of the Converter Control WRA will result in the Turret Unit (TU) to cease operation. There is no danger to crew or a safety of flight issues as a result of this issue.

RECOMMENDATION

This notice is being provided for information only. Until this issue is resolved, or test data indicate otherwise, Raytheon is not recommending a forced replacement of these suspect counterfeit EMI Filters at this time. As additional information is forthcoming, or should additional testing indicated a change in course, Raytheon will immediate so notify the US Navy.

If you have any additional questions, please do not hesitate to call [redacted] [w], [redacted] [c], or email at [redacted]@raytheon.com.

Regards,

RAYTHEON COMPANY
Space and Airborne Systems

Daniel B. Forbes
Manager, Contracts
Intelligence, Surveillance, and Reconnaissance Systems (ISRS)

TAB 6

DEPARTMENT OF THE NAVY
NAVSUP WEAPON SYSTEMS SUPPORT
700 ROBBINS AVENUE
PHILADELPHIA PA 19111-5098
5450 CARLISLE PIKE - PO BOX 2020
MECHANICSBURG PA 17055-0788

4200
27 SEPT 2011
KMA

Daniel Forbes
Raytheon Company 2501 W. University
M/S 8024
McKinney, TX 75070

Mr. Forbes:

In response to your letter (11-40022-463-1310) dated 8 September 2011 and telecon of 21 September 2011, NAVSUP WSS would like to provide you with our clear assessment and decision on the issue of suspect counterfeit parts provided by you under NAVSUP WSS contract N00383-03-D-006A. The Navy considers the five (5) Electro-Magnetic Interference (EMI) Filters, serial numbers: 0487, 0488, 0489, 0490 and 0491, which are a subcomponent of the Electronic Unit (EU), one of the three (3) Weapons Replaceable Assemblies (WRAs) covered the Navy's AN/AAS-44(V) Performance Based Logistics (PBL) contract, as non-conforming material under the contract. As such, three (3) EUs will be returned to you under Product Quality Deficiency Records (PQDRs) for replacement. Because the EMI Filters are considered non-conforming material in accordance with section C2 - 10.11, Configuration Management and Obsolescence Management of the contract, you are asked to replace with new material and return a total of five (5) new EMI Filters at no additional cost to the Government.

Please advise your forecasted shipment date for the replacement material after receipt of the PQDRs as well as the actual date of shipment to the attention of the undersigned. The PQDRs are in process and you are requested to make every effort to ship EUs with new EMI Filters back to the fleet as soon as possible.

In addition, you were asked during the 21 September 2011 telecon, if Texas Spectrum Electronics (TSE) had procured any other parts from Technology Conservation Group Incorporated (TCGI). Please respond to this request with a list of parts and identify those supplied parts used in support of the AN/AAS-44(V) PBL contract. Your response is requested by 30 September 2011.

It is my understanding that you have a Raytheon Command/Corporate Counterfeit Parts Plan and Engineering Instructions on "Non Franchised Distributor Procurement" and "Process for Executing Counterfeit (CFP) Detection Analysis". Please provide these plans to me at your earliest convenience.

If you have any questions, please contact the undersigned at [redacted] or email to: [redacted]

Sincerely,

Kathryn M. Andrews
Contracting Officer

TAB 7

Raytheon

Raytheon Company
2501 W. University
M/S 8024
McKinney, TX 75070
USA

30 September 2011

In Reply Refer to:
11-40022-463-1310_C_

Department of the Navy
NAVSUP Weapon Systems Support
700 Robbins Ave.
Philadelphia, PA 19111-5098

ATTENTION: Ms. Kathy Andrews
Contracting Officer

SUBJECT: Suspect Counterfeit Parts Notice; Response to NAVSUP Questions on Suspect Counterfeit Parts

REFERENCE: (a) NAVSUP Letter dated 27 SEPT 2011

Dear Ms. Andrews,

Per the Reference (a) letter, Raytheon Company is pleased to provide the following responses below.

Q1) **In response to your letter (11-40022-463-1310) dated 8 September 2011 and telecon of 21 September 2011, NAVSUP WSS would like to provide you with our clear assessment and decision on the issue of suspect counterfeit parts provided by you under NAVSUP WSS contract N00383-03-D-006A. The Navy considers the five (5) Electro-Magnetic Interference (EMI) Filters, serial numbers: 0487, 0488, 0489, 0490 and 0491, which are a subcomponent of the Electronic Unit (EU), one of the three (3) Weapons Replaceable Assemblies (WRAs) covered the Navy's AN/AAS-44(V) Performance Based Logistics (PBL) contract, as non-conforming material under the contract. As such, three (3) EUs will be returned to you under Product Quality Deficiency Records (PQDRs) for replacement. Because the EMI Filters are considered non-conforming material in accordance with section C2 - 10.11, Configuration Management and Obsolescence Management of the contract, you are asked to replace with new material and return a total of five (5) new EMI Filters at no additional cost to the Government.**

A1) Raytheon will support replacing the five (5) EMI filters with new EMI filters, three (3) of which will got into the EU WRAs, upon receipt, at no additional cost to the Government.

Q2) **Please advise your forecasted shipment date for the replacement material after receipt of the PQDRs as well as the actual date of shipment to the attention of the undersigned. The PQDRs are in process and you are requested to make every effort to ship EUs with new EMI Filters back to the fleet as soon as possible.**

A2) Three (3) EMI filters, with known pedigree, will arrive at FRCSE-Jacksonville no later than Friday, 7 OCT 2011. Upon receipt of the 3 PQDR's EU WRA's, Raytheon will replace the suspect, counterfeit EMI filters with known good EMI filters. The EU WRA receipts will be inducted into repair flow upon receipt and will be treated "as an Over and Above" repair activity to that-month's scheduled repair quantities. Mr. Richard Dell, Reliability Engineer, will be responsible for the

PQDR disposition and will coordinate with FRCSE QA, McKinney DCMA, and Program QA to close out the PQDRs. The suspect counterfeit EMI Filters will be placed on a hold tag pending disposition instructions from program Supply Chain Management (SCM) and Quality Assurance (QA).

Q3) In addition, you were asked during the 21 September 2011 telecon, if Texas Spectrum Electronics (TSE) had procured any other parts from Technology Conservation Group Incorporated (TCGI). Please respond to this request with a list of parts and identify those supplied parts used in support of the AN/AAS-44(V) PBL contract.

A4) Raytheon SCM has conducted an audit against the purchase orders issued against the AN/AAS-44V PBL contract to subcontractors. Our audit indicates the only parts purchased from TSC in support of this programs were these EMI filters. No other parts have been purchased from TSC in support of this program.

Q5) It is my understanding that you have a Raytheon Command/Corporate Counterfeit Parts Plan and Engineering Instructions on "Non Franchised Distributor Procurement" and "Process for Executing Counterfeit (CFP) Detection Analysis". Please provide these plans to me at your earliest convenience.

A5) Provided attached are the Raytheon command media requested with respect to counterfeit parts. Please note these command media are **RAYTHEON PROPRIETARY/BUSINESS DOCUMENTS** and are not to be distributed outside the US Government.

DOCUMENT	COMMAND MEDIA FILE
Raytheon has Corporate Policy 000000243-RP entitled, "Counterfeit Products Risk Mitigation and Prevention"	
Engineering Instruction EI-34-43 Rev. B entitled, "Non Franchised Distributor Procurement"	
Engineering Instruction EN-03-22-20 Rev – entitled, "Process for Executing Counterfeit Part (CFP) Detection Analysis	

If you have any additional questions, please do not hesitate to call [redacted] [w], [redacted] [c], or email at [redacted]@raytheon.com.

Regards,

RAYTHEON COMPANY
Space and Airborne Systems

Daniel B. Forbes
Manager, Contracts
Intelligence, Surveillance, and Reconnaissance Systems (ISRS)

TAB 8

Re: [redacted]

Raquel Supangan to: Jeremy R Bettge 08/22/2011 01:18 PM

From: Raquel Supangan <[redacted]@fairchildsemi.com>

To: Jeremy R Bettge <[redacted]@raytheon.com>

Hi Jeremy,

See below inputs i sent to Michael:

1. The top mark datecode on the units is F N548
Supposedly, this datecode mark would be translated to F = logo; N = assembly / test site code, 5 = year 2005, 48 = Workweek 48 (around end of November or 1st week of December)

However, when i checked this against shipment history and the record of when we obsoleted the part, my assessment is that these parts are suspicious, for the following reasons:

a. This [redacted] device was obsoleted in mid-2004.
In the shipment history, the last shipment we made for this part is of 2004 builds only.There were no shipment records of 2005 year builds.

b. We created a leadfree version that was [redacted] and also created a leaded part number [redacted] during the transition to leadfree, and both part numbers were obsoleted May 2005. However, there are no shipment records of [redacted] and no records of [redacted] for 2005 builds.

c. The surface of the top package appears whitish/grainy, which reminds me of previous cases of counterfeit parts that had the top package re-surfaced and re-marked.
You may be able to compare this better since you have the units on hand, by checking out the top vs bottom package surface, if they have a noticeable difference in the surface finish of the molding compound.

2. The labels you forwarded are not the Fairchild labels, so i can't get more information out of those.

3. The tube photos seem to show an F logo but again, due to the questionable top mark, there is also a question on how these tubes were obtained (could be recycled?)

Based on the available information, i would say that the origin of these parts are questionable.

best regards,
Rocky

Raquel Supangan
Customer Quality Engineering
Fairchild Semiconductor
3030 Orchard Parkway
San Jose, CA 95134
[redacted]

*NOTE: Fairchild also noted in a phone conversation that parts that have made the conversion to Pb-free have the digit for the the year in the date code replaced with a letter that represents the year. XRF

TAB 9

CARL LEVIN, MICHIGAN, CHAIRMAN

JOSEPH I. LIEBERMAN, CONNECTICUT
JACK REED, RHODE ISLAND
DANIEL K. AKAKA, HAWAII
E. BENJAMIN NELSON, NEBRASKA
JIM WEBB, VIRGINIA
CLAIRE McCASKILL, MISSOURI
MARK UDALL, COLORADO
KAY R. HAGAN, NORTH CAROLINA
MARK BEGICH, ALASKA
JOE MANCHIN III, WEST VIRGINIA
JEANNE SHAHEEN, NEW HAMPSHIRE
KIRSTEN E. GILLIBRAND, NEW YORK
RICHARD BLUMENTHAL, CONNECTICUT

JOHN McCAIN, ARIZONA
JAMES M. INHOFE, OKLAHOMA
JEFF SESSIONS, ALABAMA
SAXBY CHAMBLISS, GEORGIA
ROGER F. WICKER, MISSISSIPPI
SCOTT P. BROWN, MASSACHUSETTS
ROB PORTMAN, OHIO
KELLY AYOTTE, NEW HAMPSHIRE
SUSAN M. COLLINS, MAINE
LINDSEY GRAHAM, SOUTH CAROLINA
JOHN CORNYN, TEXAS
DAVID VITTER, LOUISIANA

United States Senate
COMMITTEE ON ARMED SERVICES
WASHINGTON, DC 20510-6050

RICHARD D. DEBOBES, STAFF DIRECTOR
DAVID M. MORRISS, MINORITY STAFF DIRECTOR

October 20, 2011

Mr. Mark Thompson
President and CEO
Fairchild Semiconductor
3030 Orchard Parkway
San Jose, CA 95134

Dear Mr. Thompson:

Counterfeit electronic parts in the Department of Defense's (DOD) supply chain pose a risk to our national security, the reliability of our weapons systems, and the safety of our military men and women. Government and industry share a common interest in ensuring that the DOD supply chain is free from these parts. As part of an inquiry by the Senate Armed Services Committee into suspect counterfeit electronic parts in the DOD supply chain, the Committee is seeking information from defense contractors and subcontractors, independent testing companies, and electronic component manufacturers about suspect counterfeit electronic parts.

The Committee has identified suspect counterfeit electronic parts that entered the U.S. military supply chain. Among those are parts that were sold by an independent distributor in China as new, authentic Fairchild Semiconductor [redacted] transistors [date code F N548]. Enclosed are photos of [redacted] transistors from the suspect lot. Additionally, an independent lab that inspected the suspect parts reported that they exhibited the following anomalies:

External Inspection:

- "Mold markings on the top side of the package showed obvious differences in appearance and also appeared to be 'black-topped'"
- "An indention ring as well as package chipping was observed around the indentation ring as well as package chipping was observed around the mounting hole on S/N 1"
- "The leads had a non-uniform surface appearance; having a smooth shiny appearance at the package egress and transitioning to a rough dull appearance beyond the standoff feature"
- "Metal overlapping and deep scratches characterized the two regions at the stand off"

Radiography

- "The non-uniform areas of the leads noted in the external inspection showed inconsistencies in the density of the metal in these areas"

De-Encapsulation and Visual Inspection

- "The die manufacturer could not be identified due to the lack of die markings on either device"
- "Die markings did not correspond to that of the external package markings"

Conclusion

- "The results of the analysis suggest the devices have possibly been refurbished components or possible counterfeits"
- "The leads may have been cut from solder joints, re-fitted by welds and solder coated"
- "Scrape testing revealed a thin layer of over coat or black-topping"
- "The package surface of both devices flaked off when performing this test revealing a smooth surface beneath"

To assist the Committee with its inquiry, please answer the following questions:

1) Does Fairchild Semiconductor sell refurbished [redacted] transistors or have an agreement with any third party that would permit them to refurbish and sell [redacted] transistors?

2) Did Fairchild Semiconductor use remarking or black-topping in its manufacturing of [redacted]?

3) Would Fairchild Semiconductor recommend the use of [redacted] transistors with the anomalies described above?

4) Would Fairchild Semiconductor warranty [redacted] transistors that exhibited the anomalies described above?

5) Please describe the short-term and long-term reliability and performance risks, if any exist, of using [redacted] transistors with the anomalies described above.

Please provide responsive information by October 27, 2011. Please send your response as an attachment to an email to Ozge_Guzelsu@armed-services.senate.gov and Bryan_Parker@armed-services.senate.gov. If you have any questions or wish to discuss this request, please contact Senate Armed Services Committee majority staff Ozge Guzelsu (202-224-8922) and Bryan Parker (202-224-8265) of the minority staff. Thank you for your cooperation.

Sincerely,

John McCain
Ranking Member

Carl Levin
Chairman

Enclosures

FAIRCHILD SEMICONDUCTOR®

[redacted] direct
[redacted] fax
[redacted] mobile

[redacted]@fairchildsemi.com

Paul D. Delva
Sr. V.P. and General Counsel
Corporate Secretary

Fairchild Semiconductor
82 Running Hill Road
South Portland, ME 04106

www.fairchildsemi.com

VIA EMAIL

October 25, 2011

United States Senate
Committee on Armed Services
Washington, D.C. 20510-6050
Attention: Ozge Guzelsu and Bryan Parker

Dear Ms. Guzelsu and Mr. Parker:

This responds to the Committee's October 20, 2011 letter to Mark Thompson, our Chairman, President and CEO. The Committee's questions and our answers, to the best of our knowledge and belief, are as follows:

1) Does Fairchild Semiconductor sell refurbished [redacted] transistors or have an agreement with any third party that would permit them to refurbish and sell [redacted] transistors?

Answer: No.

2) Did Fairchild Semiconductor use remarking or black-topping in its manufacturing of [redacted]?

Answer: No.

3) Would Fairchild Semiconductor recommend the use of [redacted] transistors with the anomalies described above?

Answer: No.

4) Would Fairchild Semiconductor warranty [redacted] transistors that exhibited the anomalies described above?

Answer: No. According to Fairchild records, the last shipment made for this part number was for parts manufactured in 2004 only. We have no record of parts bearing such a part number being manufactured in 2005. We believe these devices are not genuine Fairchild devices.

5) Please describe the short-term and long-term reliability and performance risks, if any exist, of using [redacted] transistors with the anomalies described above.

Answer: We cannot realistically assess the reliability of the parts in question because we believe they are not Fairchild Semiconductor devices.

We are pleased to assist the Committee's investigation. Please direct further communication about this matter to my attention, and do let me know if you would like to speak with our technical personnel or if you have any additional questions or requests for information.

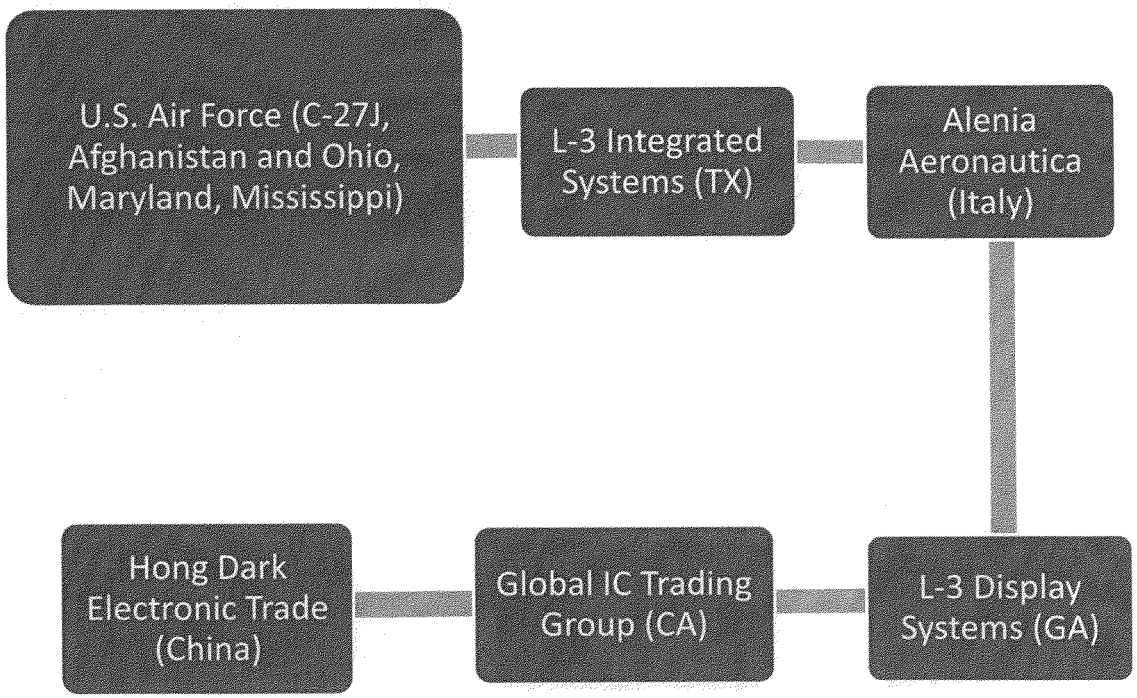
Yours very truly,

FAIRCHILD SEMICONDUCTOR CORPORATION

By: _____
Paul D. Delva
Sr. V.P., General Counsel and Secretary

cc: Mark S. Thompson

Supply Chain for Suspect Counterfeit Parts in Color Multi-Purpose Display Units Installed on U.S. Air Force C-27J

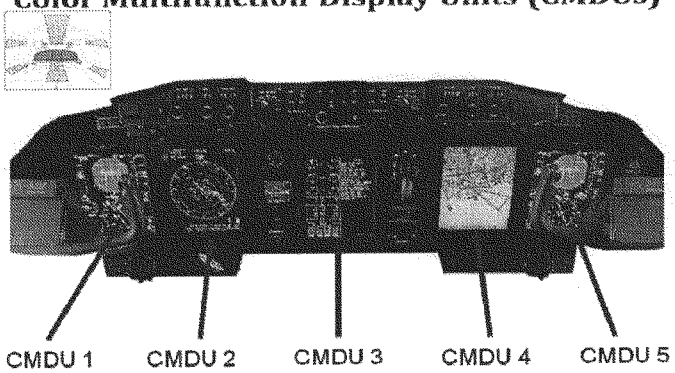


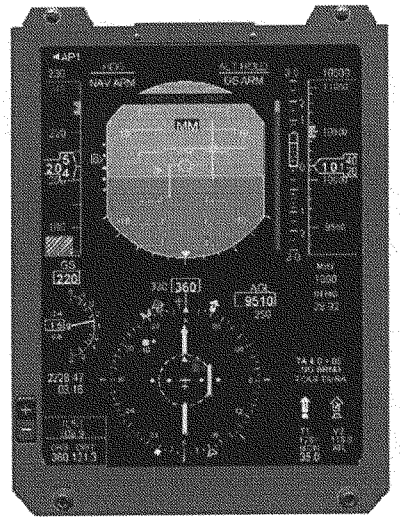
TAB 11

Color Multipurpose Display Unit (CMDU)

The Color Multipurpose Display Unit (CMDU) for the Alenia Aeronautica C-27J and Lockheed Martin (LM) C-130J aircraft is a product of L-3 Displays, PN 9104000-603 (also identified as Lockheed PN 697901-9). There are five (5) CMDUs per plane. These are Primary Flight Displays for the aircraft.

Color Multifunction Display Units (CMDUs)





L-3 Communications Integrated Systems Proprietary Information
© 2011 L-3 Communications Integrated Systems L.P.

TAB 12

CARL LEVIN, MICHIGAN, CHAIRMAN

JOSEPH I. LIEBERMAN, CONNECTICUT
JACK REED, RHODE ISLAND
DANIEL K. AKAKA, HAWAII
E. BENJAMIN NELSON, NEBRASKA
JIM WEBB, VIRGINIA
CLAIRE MCCASKILL, MISSOURI
MARK UDALL, COLORADO
KAY R. HAGAN, NORTH CAROLINA
MARK BEGICH, ALASKA
JOE MANCHIN III, WEST VIRGINIA
JEANNE SHAHEEN, NEW HAMPSHIRE
KIRSTEN E. GILLIBRAND, NEW YORK
RICHARD BLUMENTHAL, CONNECTICUT

JOHN MCCAIN, ARIZONA
JAMES M. INHOFE, OKLAHOMA
JEFF SESSIONS, ALABAMA
SAXBY CHAMBLISS, GEORGIA
ROGER F. WICKER, MISSISSIPPI
SCOTT P. BROWN, MASSACHUSETTS
ROB PORTMAN, OHIO
KELLY AYOTTE, NEW HAMPSHIRE
SUSAN M. COLLINS, MAINE
LINDSEY GRAHAM, SOUTH CAROLINA
JOHN CORNYN, TEXAS
DAVID VITTER, LOUISIANA

RICHARD D. DEBOBES, STAFF DIRECTOR
DAVID M. MORRISS, MINORITY STAFF DIRECTOR

United States Senate
COMMITTEE ON ARMED SERVICES
WASHINGTON, DC 20510-6050

October 31, 2011

Honorable Michael B. Donley
Secretary of the Air Force
United States Department of the Air Force
1670 Air Force Pentagon
Washington, DC 20330-1670

Dear Secretary Donley:

As you may know, the Senate Armed Services Committee is conducting an investigation into counterfeit electronic parts in the Department of Defense's (DOD) supply chain. During the course of its investigation, Committee staff has held two meetings with U.S. Air Force (USAF) personnel regarding suspect counterfeit electronic parts that are installed on aircraft flown by the USAF.

During these meetings, Committee staff shared information collected during the investigation regarding suspect counterfeit parts that were installed on the C-27J and C-130J. The suspect counterfeit electronic parts at issue originated with a company in China, which sold them to an independent distributor in the U.S. That independent distributor sold the parts to L-3 Communications Display Systems, which installed them on Color Multipurpose Display Units (CMDUs). More than 500 of those units were sold to both L-3 Communications Integrated Systems, the prime contractor on the C-27J, and Lockheed Martin, the prime contractor to the C-130J.

It became clear during the staff's meeting with the USAF that Committee staff had more information regarding this suspect counterfeit part than L-3 Communications and Lockheed Martin had provided to the USAF program offices. USAF personnel expressed surprise and disappointment that they had not been provided information they considered critical to judging the severity of the problem and making informed decisions.

The following information about the suspect counterfeit became clear during the course of the meetings:

- Pertinent information regarding the reliability and performance of the suspect counterfeit parts, including an independent test report showing the part to be "suspect counterfeit," was not shared with the USAF by L-3 Communications or Lockheed Martin.

- Despite representations by Lockheed Martin and L-3 Communications Integrated Systems that there had been no increase in CMDU failures attributable to the suspect counterfeit part, according to the USAF, neither of the contractors had reviewed sufficient data to come to that determination.

- Lockheed Martin represented to the USAF that it had conducted six months of "monitoring" of the CMDUs to determine whether the suspect counterfeit parts were causing increased failures. Data provided by Lockheed Martin to the Committee, however, showed that only approximately three months of limited data was reviewed.

- Lockheed Martin told the USAF that the suspect counterfeit parts were "functionally compliant" to authentic genuine parts. The USAF was apparently not informed that the failure rate of the part tripled during acceptance and environmental stress testing.

In addition to the failure to provide sufficient information on the parts, there was also a concern about L-3 Communications' failure to provide timely notification to the USAF about the parts in the C-27J. L-3 Displays, a division of L-3 Communications, learned of the problem in November 2010. Despite being a division of the same company that identified the problem, L-3 Integrated Systems has stated that it did not learn of the suspect counterfeit parts until September 2011. As a result, L-3 did not notify the USAF that the over 30 display units with the suspect counterfeit parts had been installed on eight C-27Js, including two C-27Js deployed to Afghanistan, until September 19, 2011 (one day before the first Senate Armed Services Committee staff meeting with the USAF Program offices).

At their most recent meeting, USAF personnel indicated to Committee staff that they intended to review the new information provided by the Committee and assess a course of action with the contractors. Please inform the Committee by November 7, 2011 regarding what actions the USAF is considering.

If you have any questions or would like to discuss this request, please contact us or have your staff contact Armed Services Committee majority staff Ilona Cohen (202-224-5089) and Bryan Parker (202-224-8265) of the minority staff. Thank you for your prompt attention to this matter.

Sincerely,

John McCain
Ranking Member

Carl Levin
Chairman

DEPARTMENT OF THE AIR FORCE
WASHINGTON DC 20330-1000

OFFICE OF THE SECRETARY

DEC 22 2011

SAF/LL
1160 Air Force Pentagon
Washington, DC 20330-1160

The Honorable Carl Levin
Chairman
Committee on Armed Services
United States Senate
Washington, DC 20510-6050

Dear Mr. Chairman:

Thank you for your October 31, 2011, letter to the Secretary of the Air Force regarding the suspect counterfeit parts on Air Force C-27J and C-130J aircraft. The Air Force shares your concerns and is working quickly to correct the situation and prevent future recurrences.

We are aggressively taking action to rectify the breakdowns in communication, remove the parts in question, audit the associated supply chains, and ensure the responsible parties bear the financial burden of replacement. We believe these actions will help prevent future recurrence and set the tone of increased vigilance for our program offices and industry.

First, we are taking steps to clearly define notification responsibilities and improve communication processes for our defense contractors. We are also working closely with the Defense Contract Management Agency to ensure the program offices and industry communicate effectively. In addition, the L-3 Comm Executive Vice President has agreed to conduct more aggressive quality-assurance monitoring and take steps to improve communications with its subcontractors. Finally, the Air Force Service Acquisition Executive has discussed this issue with executives from both Lockheed-Martin and L-3 Comm, reviewed the communication shortfalls that led to these parts entering the Air Force inventory, and provided direct feedback on Air Force expectations.

Additionally, the Air Force is removing all of the affected parts from the fleet and supply chain. While our engineers remain confident that the parts do not create flight safety risks, they are concerned about long-term reliability and supply chain vulnerability. Thus, in addition to developing a responsive replacement strategy, our teams are also conducting an audit of the C-27J and C-130J supply chains to ensure that no additional parts from suspect suppliers remain in the system.

Finally, we have not yet finalized specific contract remediation actions, but the options under consideration include, but are not limited to, monetary withholds and/or extended warranties until all the parts are replaced. At this time, the prime contractors have agreed to

replace the parts in question at no cost to the government. Our contracting officers will work closely with our program managers to ensure the government's interests are fully protected.

We stand ready to assist your staff in obtaining any additional information they require to support their investigation. A similar letter is being sent to your committee's Ranking Member.

Very respectfully,

ANTHONY P. REARDON, SES, DAFC
Director of Staff, Legislative Liaison

TAB 13

communications

Display Systems
1355 Bluegrass Lakes Parkway
Alpharetta, GA 30004
Telephone (770) 752-7000 Finance/Contracts Fax (770) 752-5516

02 February 2010
CL10-00000-0150/dh

Alenia Aeronautica
Corso Marche 41
10146 Turin
Italy

Attention: Francesco Bucci
Procurement
C-27J Program

SUBJECT: NOTICE OF SUSPECT LATTICE COMPONENTS

Dear Mr. Bucci:

L-3 Communications Display Systems (L-3 DS) has recently discovered that it is in receipt of suspected counterfeit lattice components which may have affected the C27J CMDU XGA (P/N# 104000-603). Please see Attachment A notice.

The serial numbers that may be affected are 4034 – 4073 (Qty 40). Shipments of the CMDU P/N# 104000-603 to Alenia occurred as follows:

January 2009 = 4034, 4035, 4036, 4037, 4038, 4039, 4040, 4041, 4042, 4043
March 2009 = 4044, 4045, 4046, 4047, 4048, 4049, 4050, 4051, 4052, 4053
May 2009 = 4054, 4055, 4056, 4057, 4058, 4059, 4060, 4061, 4062, 4063
July 2009 = 4064, 4065, 4066, 4067, 4068, 4069, 4070, 4071, 4072
August 2009 = 4073

L-3 DS engineering has provided the following analysis regarding component failure:

The component is used on both the Taxi CCA (L-3 DS Part# 104440-603) and the Graphics Processor CCA (L-3 DS Part# 104340-809). On the TAXI, the part is used to decode the TAXI data and generate the video. On the Graphics Processor, the part is used to blend the graphics with the TAXI. A failure of either part would result in video anomalies on the display. If total part failure occurred the display would produce a blank screen. L-3 DS engineering would like the opportunity to discuss with Alenia the affect this condition could have regarding a potential safety concern.

L-3 DS needs to verify if the suspect component is in the delivered units and coordinate replacement of any components determined to be part of the suspect lot. L-3 DS would like

"This technical data is controlled under the U.S. International Traffic in Arms Regulations (ITAR) and may not be exported to a Foreign Person, either in the U.S. or abroad, without the proper authorization by the U.S. Department of State."

to suggest that an L-3 DS team come to Italy to perform an inspection on the above listed units.

In the event that this is an acceptable option; L-3 DS will formulate a plan that will include this on site inspection step.

Please feel free to contact the undersigned if further information or clarification is required.

Sincerely,

Deborah K. Henning

Deborah K. Henning
Sr. Contracts Administrator
Phone: [redacted]
E-mail: [redacted]@L-3com.com

Cc: L. Ream
R. Hunt
D. Parriott

Attachment A – GIDEP Alert

"This technical data is controlled under the U.S. International Traffic in Arms Regulations (ITAR) and may not be exported to a Foreign Person, either in the U.S. or abroad, without the proper authorization by the U.S. Department of State."

Distribution is not authorized outside of the GIDEP participant's organization.

GOVERNMENT - INDUSTRY DATA EXCHANGE PROGRAM

ALERT

1. TITLE *(Class, Function, Type, etc.)* Suspect Counterfeit, Microcircuit, In-System Programmable High Density PLD	2. DOCUMENT NUMBER GG5-A-10-01 3. DATE *(DD-MMM-YY)* 16 December 2009

4. MANUFACTURER AND ADDRESS Lattice Semiconductor Corporation 5555 N.E. Moore Court Hillsboro, Oregon 97124-6421 USA	5. PART NUMBER [redacted]	6. NATIONAL STOCK NUMBER NOT AVAILABLE
	7. SPECIFICATION NOT AVAILABLE	8. GOVERNMENT PART NUMBER NOT AVAILABLE
	9. LOT DATE CODE START A533B07	10. LOT DATE CODE END A533B07
11. MANUFACTURER'S POINT OF CONTACT Thomas J Lawler	12. CAGE 66675	13. MANUFACTURER'S FAX NOT AVAILABLE
14. MFR. POC PHONE [redacted]	15. MANUFACTURER'S E-MAIL [redacted]@latticesemi.com	
16. SUPPLIER NOT AVAILABLE	17. SUPPLIER ADDRESS NOT AVAILABLE	18. SUPPLIER CAGE NOT AVAILABLE

19. PROBLEM DESCRIPTION / DISCUSSION / EFFECT

L-3DS received a total of 3147 pieces of [redacted] from an independent distributor; All components were Lot Code A533B07. Components were subjected to counterfeit inspection and analysis at an independent L-3 approved test facility with no obvious signs of suspect/counterfeit characteristics observed.

During sub-tier re-tinning an unapproved etch process prompted L-3DS to contact Lattice Semiconductors Sales for OEM guidance.

Lattice semiconductor, upon reviewing the data and pictures sent to them, observed inconsistencies with the part marking. The product lot ID A533B07 did not match their data base and the package backside did not have permanent laser markings for seal date and additional lot coding.

L-3DS, in reviewing the attached Lattice letter (5 November 2009), has concluded that the components with Lot Code A533B07 should be considered suspect.

Note: The manufacturer identified in block 4 is the entity whose product may have been counterfeited. This reporting convention is necessary to facilitate GIDEP database searches for suspect counterfeit products and is by no means intended to imply that the manufacturer identified in block 4 is involved with the suspect product.

20. ACTION TAKEN/PLANNED

L-3DS notified its customer of the incident. All 3147 suspect parts have been recalled, quarantined (at L-3), and replaced with known good components. Due to the elusive characteristics of this suspect component, L-3 has requested additional tests be included in the approved independent test facility screening process.

21. DATE MFR. NOTIFIED/ SUPPLIER NOTIFIED 04 Dec. 2009	22. MFR./SUPPLIER RESPONSE [X] REPLY ATTACHED [ ] NO REPLY	23. ORIGINATOR ADDRESS/POINT OF CONTACT Mike Meo L-3Communications Display Systems 1355 Bluegrass Lakes Pkwy Alpharetta GA, 30004 [redacted]

24. GIDEP REPRESENTATIVE Mike Meo	25. SIGNATURE	26. DATE 16 Dec. 2009

GIDEP Form 97-1 (September 2009)

Please refer to the complete distribution policy at the GIDEP member's website.

Lattice Semiconductor Corporation

November 5, 2009

Robert T. Hunt
Director, Quality Assurance
L-3 Communications - Display Systems
1355 Bluegrass Lakes Parkway
Alpharetta, Georgia 30004-8458

Subject: Lattice [redacted] Lot A533B07

Dear Robert,

In reviewing the data and pictures that was sent to us in the Oneida Research Services, Inc report U100188-000 GI.PDF, we observed a number of curious inconsistencies:

1. This product lot ID code is from 1995, 14 years ago. This product lot ID code has the 1990 – 1999 alpha numeric scheme. In 2000, Lattice changed our product lot ID code scheme.

2. The product lot ID A533B07 does not match our manufacturing data base – there is a mismatch of product type and product lot ID.

3. The product lot ID A533B07 represents the A die/foundry code for the [redacted] built in year 1995, during work week 33 at assembly/test site B and the 7th lot built that work week. If this was a valid lot ID, lot A533B07 would have been manufactured in August 1995.

   This manufacturing date implied by the product lot ID code is before the [redacted] mask set was released.

   The earliest [redacted] mask set 03 shipments was in November 1995 with engineering sample material marked with an ES mark designation. The earliest [redacted] 03 mask set production shipment was in March 1996.

4. The package backside – the ejector pins, lack of permanent laser markings for seal date and additional lot coding and plastic surface features - does not match any of our suppliers.

The pictures show that a Lattice [redacted] mask set 03 die is in a package that was not built by any Lattice assembly subcontractors. We have no record of this [redacted] device lot.

We request L-3 Communications, determine the source of this [redacted] device.

Please let me know if you need any additional information.

Regards,

Thomas J Lawler
Director, Quality Assurance
Lattice Semiconductor Corporation
[redacted]

TAB 14

Counterfeit Parts History Card

Date Of Occurrence	Contact Name	Contact Number	Contact E-Mail	Division
15OCT09	Robert Hunt	[redacted]	[redacted]@l-3com.com	Display Systems
Component Type	**Manufacturer**	**Manuf. Part Number**	**L-3 Part Number**	**Country of Origin**
Microcircuit (IC)	Lattice	[redacted]	U100188-000	Korea
Date Code	**Lot Number**	**Defect Quantity**	**Defect Type**	**Impact Category**
9533	A533B07	3147	Lot Traceability	High
Independent Disti.	**Supplier**	**Type of Packaging**	**GIDEP Notification**	**ERAI Report Date**
Global IC	Global IC	Tray	GG5-A-10-01 (17Dec09)	Unknown

Incident Summary:

Subject components were inspected for evidence of suspect/counterfeit characteristics by Global IC, an L-3 approved source of supply. No evidence was detected implicating components. Ref attached report.

GICTG Inspection for PN [redacted]

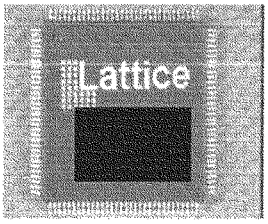
Subject components were independently inspected for evidence of suspect/counterfeit characteristics by Oneida Research, an L-3 approved test facility. No evidence was detected implicating components. Ref attached report.

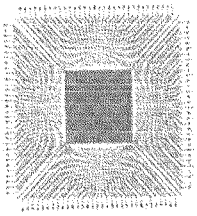
U100188-000 GI.pdf

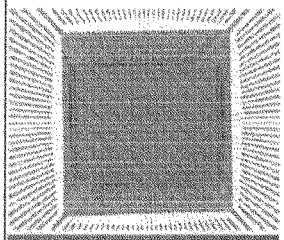
Components were accepted and stocked based on screening information provided.

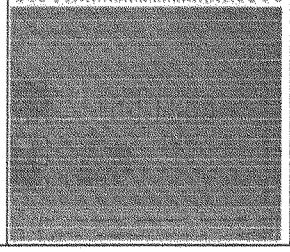
During sub-tier re-tinning an unapproved etch process was performed, requiring disposition of a Vendor Request for Information/Acceptance (VRIA). Lattice was contacted to assist part evaluation and determined this particular Lot number was not consistent for this component.

Pictures:









Resolution Summary:

Opened Case Report with Lattice. Ref attached report.

Lattice [redacted] pdf

Received Case Disposition. Ref attached report.

Lattice response to L-3 Communication is

Initiated internal purge and notified customer (LM Aero) of suspect component concern. Ref attached report.

LPN_U100188-000.pdf

Components have been collected, confiscated, and will be held until further disposition is determined (i.e., scrapped, destroyed, provided as evidence, etc.)

Type "Unknown "in field if information is unavailable. Type "N/A" if information is non-applicable

L-3 Intranet / Material Management / Teams / Counterfeit Parts / CPH Cards

TAB 15

communications

Display Systems
1355 Bluegrass Lakes Parkway
Alpharetta, GA 30004
Telephone (770) 752-7000 Finance/Contracts Fax (770) 752-8516

16 December 2010
CL10-000-1348/MS

Alenia North America
1625 Eye Street NW, Suite 1200
Washington, DC 20006

Attention: David Hope
Procurement
C-27J Program
Alenia North America

SUBJECT: NOTIFICATION OF SUSPECT COMPONENTS – PART NUMBER U100582-000, 4MB IC VRAM CHIP

Dear Mr. Hope:

L-3 Communications Display Systems (L-3 DS) recently identified a concern with the U100582-000 4MB IC VRAM chip utilized in the Color Multipurpose Display Units (CMDU) display assemblies. The initial concern was discovered internally through a perceived increase of failures during testing of the display. Preliminary analysis by L-3 DS lead to the concern that the U100582-000 chip may have been tampered with, indicating the components are suspect. Additional testing by an external laboratory has confirmed the U100582-000 VRAM chip has been remarked.

L-3 DS has taken the following actions concerning the U100582-000 VRAM chip with date code 813:

- Containment
  - Initiation of a purge of all internal stock for the 813 date code to prevent additional assemblies from being produced.
  - Stoppage of any additional shipments of units containing suspect U100582-000 components with an 813 date code.
  - Please refer to the attached list for a complete detail of serial numbers that have shipped from L-3 DS with the U100582-000 VRAM chip with the 813 date code.
    - The first receipt of the U100582-000 with the suspect date code was received 3/24/2009.
    - 98 units have shipped as new production after receipt of these components; possibly containing the suspect component.

- Scope of Concern
  - Suspect parts were delivered to two (2) independent test facilities (SMT & ORS) to complete counterfeit part analysis.
    - SMT confirmed the parts had multiple indications that they have been tampered with; including blacktopping.
      - Parts have been confirmed as having the correct die, indicating the internal circuitry is correct for U100582-000.
    - ORS testing was inconclusive as to the legitimacy of the parts, but confirmed that the components tested are U100582-000.
    - L-3 DS also completed de-encapsulation testing that confirmed the internal die matches that of a non-suspect date code. This indicates the parts in question are U100582-000 parts.
  - The OCM, Samsung, has been contacted for additional verification details of the U100582-000 part with the 813 date code. No response has been received.
  - L-3's supplier has been notified of the issue, and has provided support information concerning the exposure.
    - L-3 received the parts from Global IC Trading Company, a component broker.
    - Global IC received these parts from Hongdark Electronic Trade.
    - Hongdark supplied 1 other component currently in assemblies, which L-3 is confirming. This component is not used in any Alenia assemblies.
  - The failure totals attributed to the U100582-000 has been assessed under those found internally at L-3 DS through our testing, and those found as a result of a customer/ field return. In an effort to avoid failures at the customer, L-3 DS completes 100% testing on all units. The values were determined through analysis of all CMDU's & MFCD's.
    - Internal Failures Corrected Through Screening: 141 (27%; Assemblies where U100582-000 was replaced after testing/ Units Shipped with Suspect Date Code)
    - Field Returned Failures: 1 (0.2%; Return Assemblies for U100582-000 Failure / Units Shipped with Suspect Date Code)
  - L-3 DS' Safety Engineer has reviewed the conditions of this failure and provided the following information:
    - Identification of the original failure was by screening process, not by reduced performance reported or exhibited in the field.
    - No units that have failed the screening process were issued for installation or delivered to the customer.
    - The performance of the field units is not expected to change, nor are any new failure conditions or effects expected.
    - The failure modes that may be exhibited by the displays as related to a failure of the U100582-000 are:
      - Degraded visual imagery on the display
      - Blank screen/ Loss of display
      - BIT Failure (PBIT, CBIT, IBIT)

- The potential rate of single and multiple failures remains consistent with the original safety assessments and FMECA.
- The failure modes are mitigated by redundancy of multiple reconfigurable displays in the aircraft.

In summary, L-3 DS' initial assessment is that the U100582-000 VRAM component with the 813 date code are authentic but have been tampered with for the purpose of remarking them. Based on this analysis, it is determined that the field failure of suspect components is not anticipated to deviate from the current failure percentages, as a result of L-3 DS' internal testing.

Attached is a list of suspect assemblies shipped, should you require additional information or clarification regarding the above subject suspect component, please do not hesitate to contact Chris Durre, Principal Quality Engineer, [redacted] or the undersigned at [redacted]

Sincerely,

Michael Simmons
Contracts Manager

CC: L. Ream
B. Nall
C. Durre

TAB 16

COMPONENT INSPECTION ANALYSIS

00003485

14 High Bridge Road, Sandy Hook, CT 06482
Tel: 203 270-4700 • Fax: 203 270-4799
www.smtcorp.com

Sales Order #	
Customer	L-3 Communications
Customer Part #	
Customer Lot #	FAILED ON CCA
SMT PO #	9995
Vendor Name	
Vendor/Lot #	
Date Received	11/5/10
Manufacturer	SAMSUNG ELECTRONICS INC
Cage Code	N/A
Part Number	KM4216C258G50
Description	Video RAM
Package	64-Pin SOP
Quantity Rec'd	2
Quantity Tested	2
Quantity Rejected	2
Sampling	100%
Lot Code	RMA100CB
Date Code	0813
Inspector	Neil Schultz and Jason Romano
Date	November 9, 2010
Report ID	00003485
Notes	

Analysis Performed

Task	QC Initials	Date	Result
Visual Inspection	NS/JR	11/5/10	FAIL
Resistance to Solvents (RTS) & Scrape Test	NS/JR	11/5/10	FAIL
MFG Spec Sheet Comparison	NS/JR	11/5/10	FAIL
XRF Elemental Analysis	NS/JR	11/7/10	PASS
Real-Time X-Ray Analysis	NS/JR	11/7/10	PASS
Scanning Electron Microscopy (SEM) Analysis			
Scanning Acoustic Microscopy (C-SAM) Analysis			
Solderability Test			
Dynasolve Test			
Decapsulation & Die Microscopy	NS/JR	11/9/10	PASS

Inspector's name (print)	Signature	Date
Neil Schultz		
Jason Romano		

COMPONENT INSPECTION ANALYSIS

00003485

Manufacturer: SAMSUNG ELECTRONICS INC
Part Number: KM4216C258G50
Date Code: 0813 Lot Code: RMA100CB

	QC Initials	Date	Result
Suspect Counterfeit?	**NS/JR**	11/9/10	YES

SUMMARY

Multiple abnormalities were detected while testing these components. Some package measurements do not match the specifications found in the manufacturer datasheet. Foreign material was found on the top surface of one sample. The other sample's part markings are red. The top surface mold cavities of both samples and the bottom mold cavities of one sample were found to contain the same texture as the rest of the component surface, which is an indication of blacktopping. Variations in color and texture were found along the package edge which is further evidence of blacktopping. The bottom surface of one sample exhibits markings while the other sample does not. The condition of the leads is difficult to determine due to the excess solder remaining from having been pulled from a PCB for analysis. Testing these components for marking permanency with acetone lifted a large amount of black material, revealing fine scratches in the original surface and confirming these parts are blacktopped. Based on these abnormalities these components have failed inspection and are not considered to be factory original parts.

COMPONENT INSPECTION ANALYSIS

00003485

Manufacturer: SAMSUNG ELECTRONICS INC
Part Number: KM4216C258G50
Date Code: 0813 Lot Code: RMA100CB

VISUAL INSPECTION

YES	NO	N/A	Leads
X			Corrosion or tarnish on pins
X			Pins have dissimilar gloss, shine, color, or texture
	X		Pin surface is inconsistent with date code
X			Dirty pins or leads
	X		Dents in leads indicate used parts
X			Excess solder on leads indicates used parts
		X	Leads are tinned
		X	Leads/Balls are refurbished
		X	Gold leads have been tinned
			Top Surface
X			Parts appear to be blacktopped and remarked
	X		Surface cracks
X			Directional scratches on top surface of part
			Markings
	X		Part numbers are blurry
X			Inconsistent part marking font, color, or placement
	X		Inconsistent date and lot codes in the package
	X		Inconsistent country of origin within date/lot code
X			Top and bottom markings are inconsistent
X			Colored dots or ink marks on component top
			Component Case
	X		Top and bottom color inconsistent
	X		Tool pull marks
	X		Heat sink witness marks
	X		Burn marks
		X	Parts in package not all facing the same way
	X		Glue or adhesive
	X		Circles on part bottoms are inconsistent
		X	Part does not match known good part

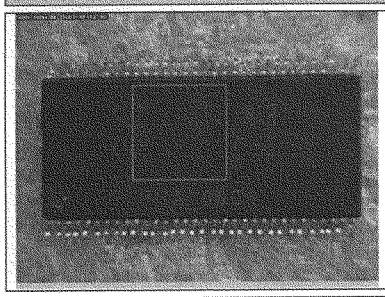
COMPONENT INSPECTION ANALYSIS

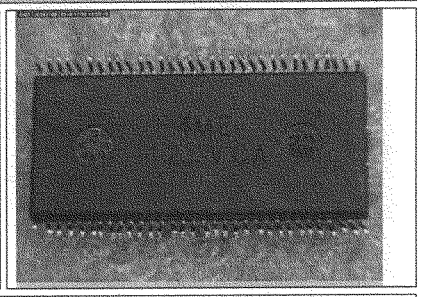
00003485

Manufacturer: SAMSUNG ELECTRONICS INC
Part Number: KM4216C258G50
Date Code: 0813 Lot Code: RMA100CB

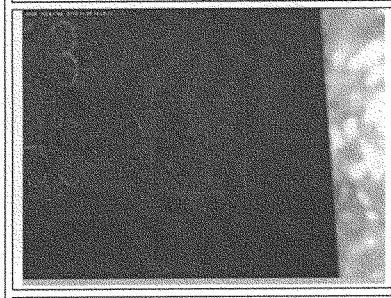
PART PHOTOGRAPHY

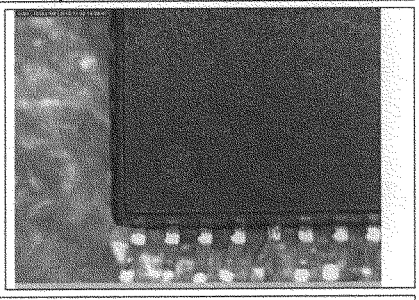
SAMPLE 1



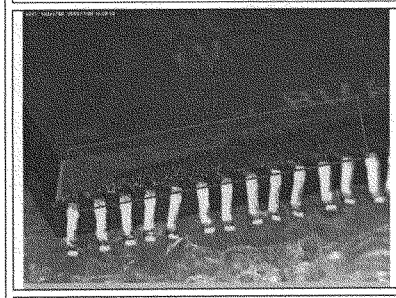


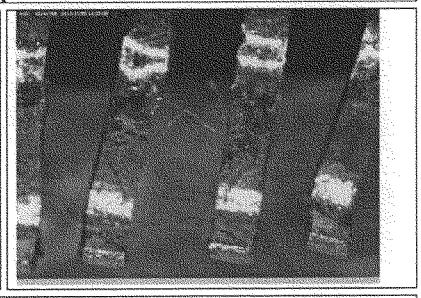
Foreign material was found on the top surface of this sample.





The top surface mold cavity is barely able to be seen and contains the same texture as the rest of the component surface.





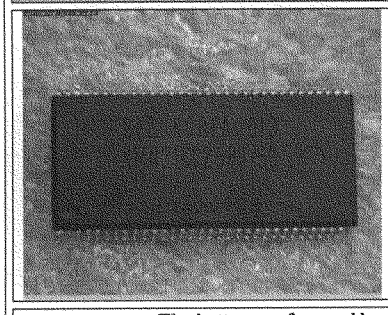
A variation in color and texture was found along the package edges. The condition of the leads is difficult to determine due to the fact that these parts were desoldered from PCBs for inspection.

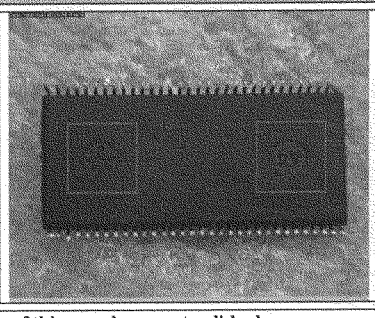
COMPONENT INSPECTION ANALYSIS

00003485

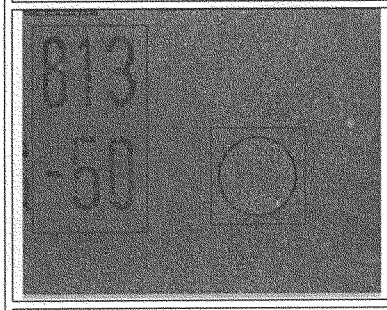
Manufacturer: SAMSUNG ELECTRONICS INC
Part Number: KM4216C258G50
Date Code: 0813 Lot Code: RMA100CB

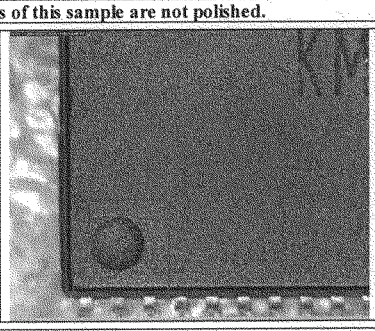
SAMPLE 2



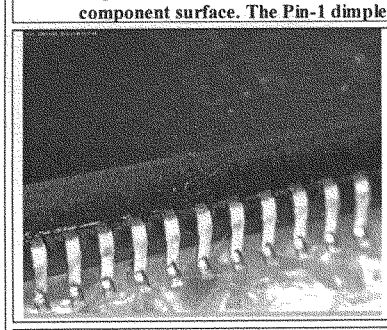


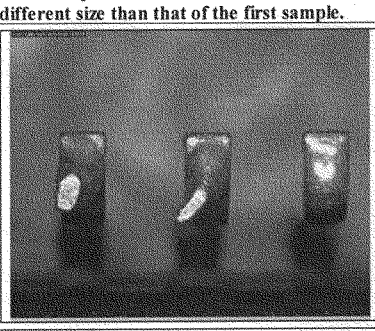
The bottom surface mold cavities of this sample are not polished.





The part markings are red. The top surface mold dimple texture matches the rest of the component surface. The Pin-1 dimple is a different size than that of the first sample.





A variation in color and texture was found along the package edges. The condition of the leads is unable to be determined due to the excess solder that exists on them.

COMPONENT INSPECTION ANALYSIS

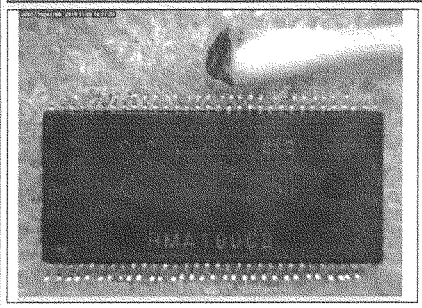
00003485

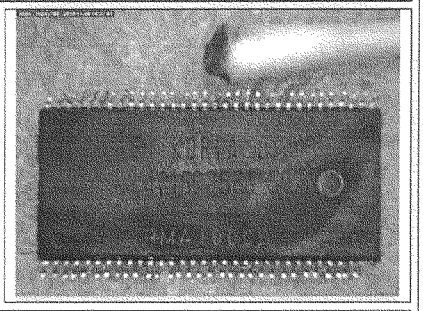
Manufacturer: SAMSUNG ELECTRONICS INC
Part Number: KM4216C258G50
Date Code: 0813 Lot Code: RMA100CB

RESISTANCE TO SOLVENTS & SCRAPE TEST

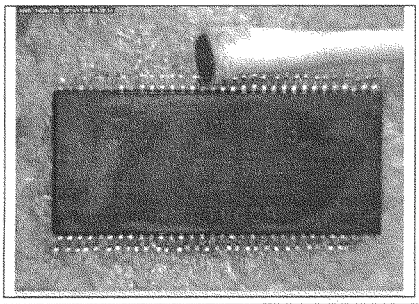
PASS	FAIL	N/A	Wipe test with:
X			3:1 Mineral Spirits/Alcohol Solution
	X		Acetone
		X	Scrape Test

SAMPLE 1





After vigorous wipe testing, the original polish of the top surface mold cavity can be seen.



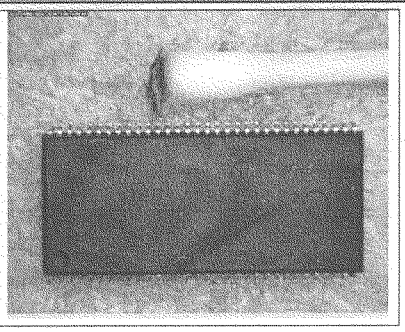
A clear distinction can be made between the original surface and the blacktop coating.

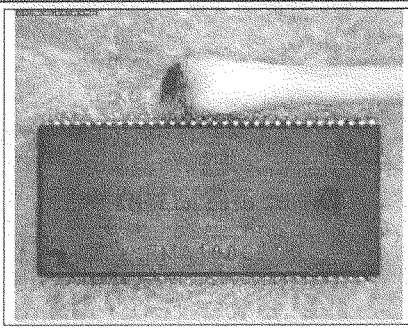
COMPONENT INSPECTION ANALYSIS

00003485

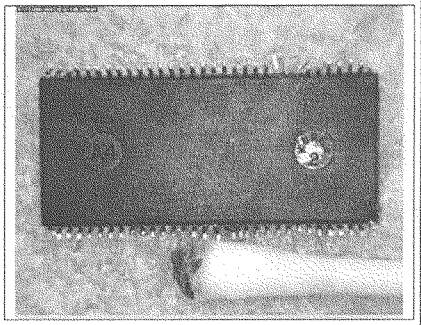
Manufacturer: SAMSUNG ELECTRONICS INC
Part Number: KM4216C258G50
Date Code: 0813 Lot Code: RMA100CB

SAMPLE 2





Testing for marking permanency lifted a large amount of red color from the part markings.



After vigorous wipe testing, the original surface can be seen beneath the blacktop coating. The bottom surface of this sample has also been blacktopped; the original polish of the country of origin dimple can be seen after much wipe testing.

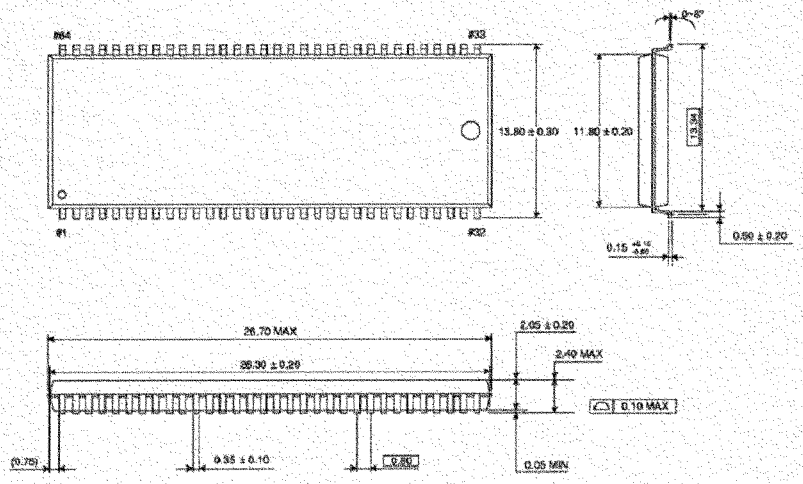
COMPONENT INSPECTION ANALYSIS

00003485

Manufacturer: SAMSUNG ELECTRONICS INC
Part Number: KM4216C258G50
Date Code: 0813 Lot Code: RMA100CB

MANUFACTURER'S SPEC SHEET COMPARISON

64 Pin Plastic Small Out Line Package (Units : Millimeters)



Measured Part dimensions (in mm, unless otherwise noted)

Designation	Spec	Value	In Spec?
Length	26.30 ± 0.20	26.11	Pass
Width	11.80 ± 0.20	11.41	Fail
Width Including Leads	13.80 ± 0.30	13.25	Fail
Package Thickness	2.05 ± 0.20	2.62	Fail
Thickness Including Seating Plane	2.40 Max	2.80	Fail
Lead Width	0.35 ± 0.10	0.29	Pass
Lead Thickness	0.15 +0.10, -0.05	0.15	Pass

COMPONENT INSPECTION ANALYSIS

00003485

Manufacturer: SAMSUNG ELECTRONICS INC
Part Number: KM4216C258G50
Date Code: 0813 Lot Code: RMA100CB

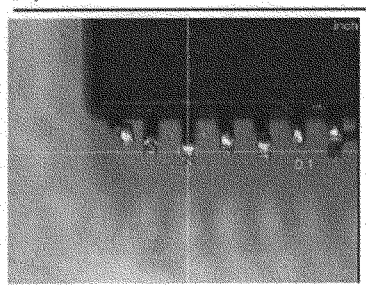
XRF ELEMENTAL ANALYSIS

XRF test results

YES	NO	N/A	Parameter:
		X	RoHS compliant samples meet requirements

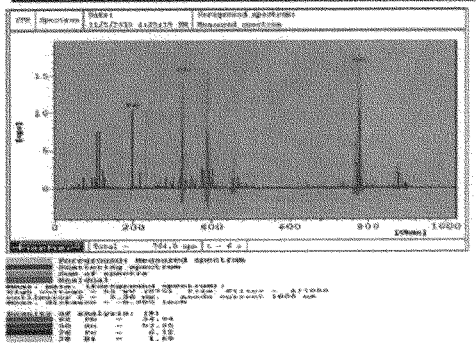
Fischerscope® XRAY XDAL
Calibration: Standard free
Date: 11/5/2010 Time: 4:31:08 PM
Operator: Neil Schultz
Application: 32 / SnPb/CuNiFe

Part Number: KM4216C258G50
Order/PO No: 9995
Date Code: 0813
Lot Code: FAILED ON CCA
Sample: 1



N	Sn 1[ppm] (1000 – 1000000)	Pb 1[ppm] (0.000 – 1000)
1	721286	278714
2	651393	348607
3	717244	282756
4	726751	273249

	Sn 1[ppm]	Pb 1[ppm]
Number of readings	4	4
Min. reading	651393 ppm	273249 ppm
Max. reading	726751 ppm	348607 ppm
Measuring time	60 sec	



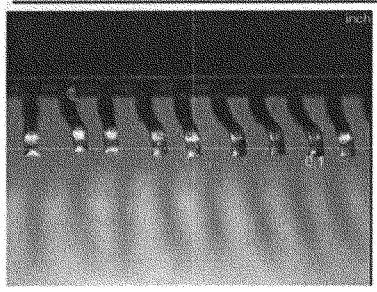
COMPONENT INSPECTION ANALYSIS

00003485

Manufacturer: SAMSUNG ELECTRONICS INC
Part Number: KM4216C258G50
Date Code: 0813 Lot Code: RMA100CB

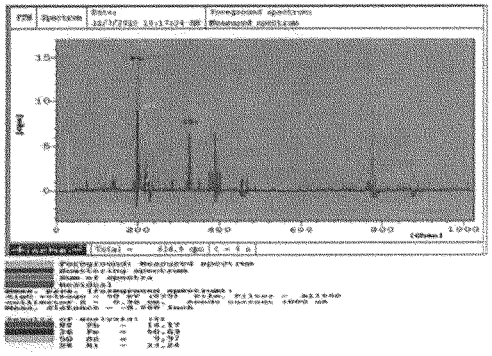
Fischerscope® XRAY XDAL
Calibration: Standard free
Date: 11/7/2010 Time: 10:24:28 AM
Operator: Neil Schultz
Application: 32 / SnPb/CuNiFe

Part Number:	KM4216C258G50
Order/PO No:	9995
Date Code:	0813
Lot Code:	FAILED ON CCA
Sample:	1



N	Sn 1[ppm]	Pb 1[ppm]
1	563961	436039
2	589114	410886
3	529121	470879
4	629169	370831

Number of readings	4	4
Min. reading	529121 ppm	370831 ppm
Max. reading	629169 ppm	470879 ppm
Measuring time	60 sec	



COMPONENT INSPECTION ANALYSIS

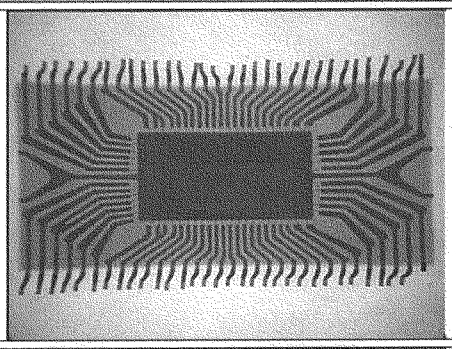
00003485

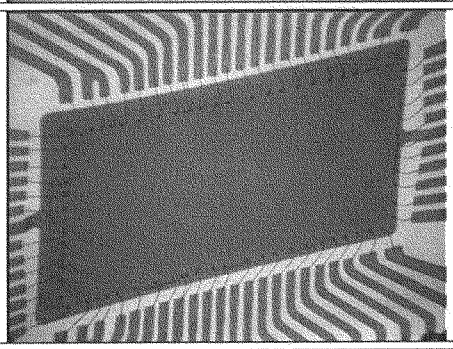
Manufacturer: SAMSUNG ELECTRONICS INC
Part Number: KM4216C258G50
Date Code: 0813 Lot Code: RMA100CB

REAL-TIME X-RAY ANALYSIS

PASS	FAIL	N/A	Check for:
X			Extraneous matter (die attach, burrs, ball bonds)
X			Die attach incorrect (voids traverse die, misalignment)
X			Cracked, split, or chipped electrical elements
X			Broken bond wires or missing bonds
X			Excessive loop or sag in bond wires
X			Taut bond wires
X			Bond wires touch each other or case
			Consistency within:
X			Bond wire gauge
X			Die size and placement

SAMPLE 1



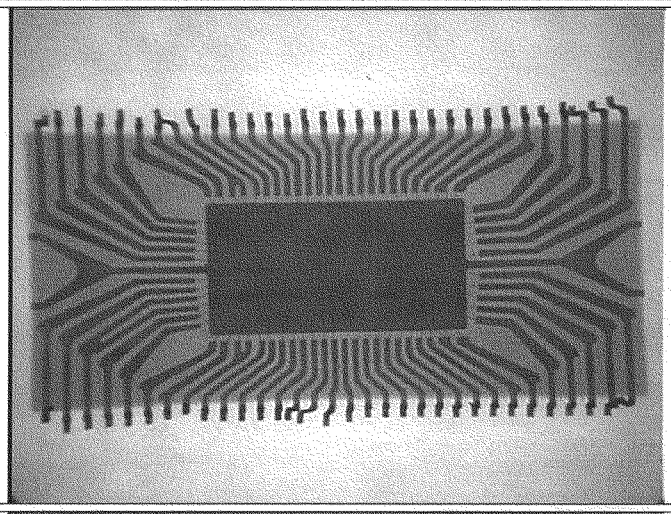


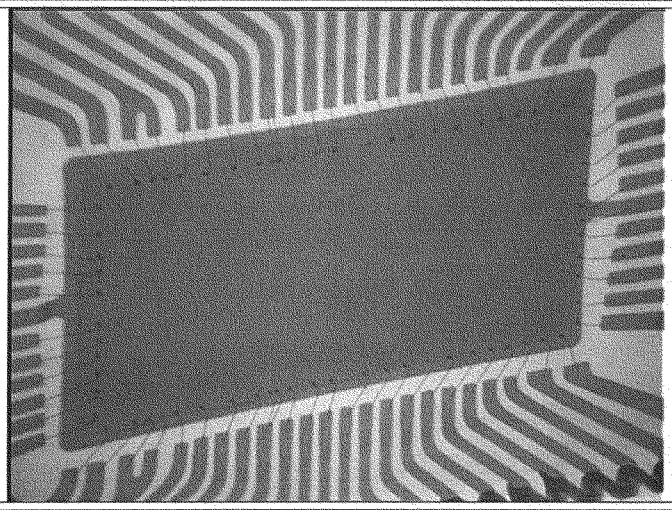
COMPONENT INSPECTION ANALYSIS

00003485

Manufacturer: SAMSUNG ELECTRONICS INC
Part Number: KM4216C258G50
Date Code: 0813 Lot Code: RMA100CB

SAMPLE 2





Die size, substrate type, lead frame design and bond out all match between both samples.

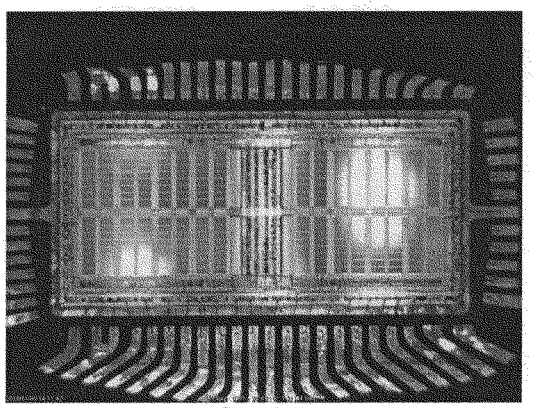
COMPONENT INSPECTION ANALYSIS

00003485

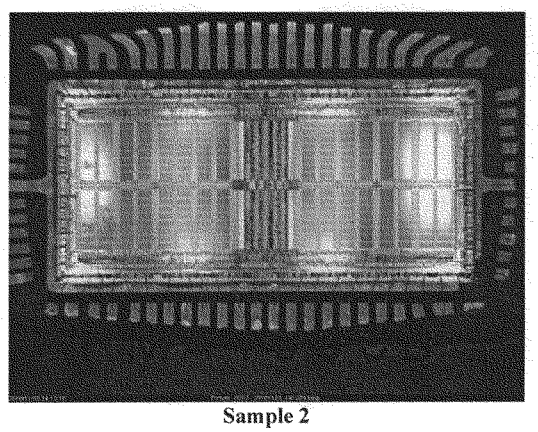
Manufacturer: SAMSUNG ELECTRONICS INC
Part Number: KM4216C258G50
Date Code: 0813 Lot Code: RMA100CB

DECAPSULATION

N/A	Recipe for decapsulation:	Notes			
	Acid:	X	HNO_3	X	H_2SO_4
	Ratio of mixture	9:1			
	Temperature (°C):	100			
	Time (seconds):	60			
	Mode:	X	Pulse		Vortex
	Flow (ml per minute):	3			
	Rinse (seconds):	3			



Sample 1



Sample 2

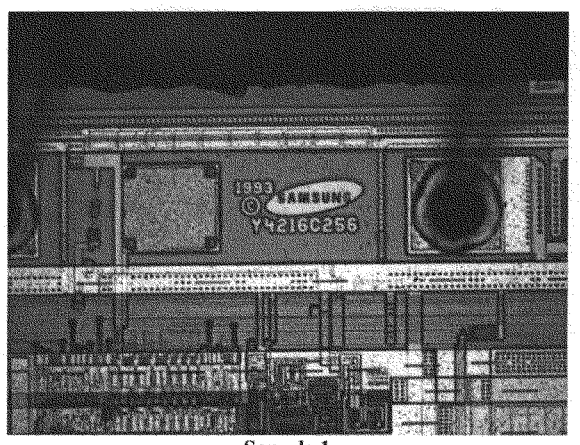
COMPONENT INSPECTION ANALYSIS

00003485

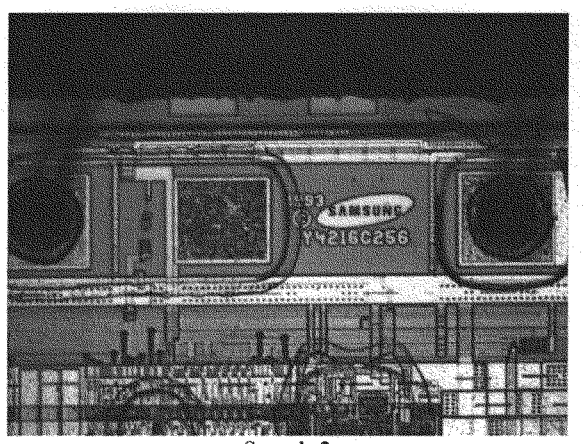
Manufacturer: SAMSUNG ELECTRONICS INC
Part Number: KM4216C258G50
Date Code: 0813 Lot Code: RMA100CB

DIE MICROSCOPY

Look for:	Notes:
Are die consistent between samples?	Yes
Part Number:	Y4216C256
Date:	1993
Manufacturer Logo:	Samsung



Sample 1



Sample 2

COMPONENT INSPECTION ANALYSIS

00003485

Manufacturer: SAMSUNG ELECTRONICS INC
Part Number: KM4216C258G50
Date Code: 0813 Lot Code: RMA100CB

DISCLAIMER: SMT Corp. performs analysis work as a technical service to its customers and extends every effort to report reliable data and an accurate interpretation thereof. However, SMT Corp. agrees only to apply its best professional effort to any work performed. NO WARRANTY IS EXPRESSED OR IMPLIED REGARDING RESULTS OBTAINED.

TAB 17

Distribution is not authorized outside of the GIDEP participant's organization.

GOVERNMENT - INDUSTRY DATA EXCHANGE PROGRAM

ALERT

1. TITLE *(Class, Function, Type, etc.)* Suspect Counterfeit, Microcircuit, 256K x 16 Bit CMOS Video RAM		2. DOCUMENT NUMBER GG5-A-11-001 3. DATE *(DD-MMM-YY)* 20 December 2010
4. MANUFACTURER AND ADDRESS Samsung Semiconductor Inc.	5. PART NUMBER KM4216C258G-50	6. NATIONAL STOCK NUMBER Not Available
	7. SPECIFICATION Not Available	8. GOVERNMENT PART NUMBER Not Available
	9. LOT DATE CODE START 0813	10. LOT DATE CODE END 0813
11. MANUFACTURER'S POINT OF CONTACT Not Applicable	12. CAGE Not Applicable	13. MANUFACTURER'S FAX Not Applicable
14. MFR. POC PHONE Not Applicable	15. MANUFACTURER'S E-MAIL Not Applicable	
16. SUPPLIER Withheld	17. SUPPLIER ADDRESS Withheld	18. SUPPLIER CAGE Withheld

19. PROBLEM DESCRIPTION / DISCUSSION / EFFECT

L-3DS received a total of 10,055 pieces of KM4216C258G-50 from an independent distributor (KM4216C258G-50 is obsolete and not available from an authorized distributor); All components were Date Code 0813. Components were subjected to counterfeit inspection and analysis at an independent L-3 approved test facility with no obvious signs of suspect/counterfeit characteristics observed.

High failure rate during testing prompted L-3DS to conduct further testing. New suspect components with data code 0813 were sent to a different L-3 approved test facility, which detected multiple abnormalities during testing (full report attached). Based on these abnormalities components with date code 0813 have failed inspection and are not considered to be factory original parts.

Note: ***The manufacturer identified in block 4 is the entity whose product may have been counterfeited. This reporting convention is necessary to facilitate GIDEP database searches for suspect counterfeit products and is by no means intended to imply that the manufacturer identified in block 4 is involved with the suspect product.***

20. ACTION TAKEN/PLANNED

All components with the 813 date code have been quarantined at L-3's facility. All parties that have received the suspect components from L-3 Display Systems have been contacted regarding the suspect components. In addition, L-3 will replace all suspect components supplied in fielded units through a process of attrition.

21. DATE MFR. NOTIFIED/ SUPPLIER NOTIFIED Not Applicable	22. MFR./SUPPLIER RESPONSE ☐ REPLY ATTACHED Not Applicable ☐ NO REPLY	23. ORIGINATOR ADDRESS/POINT OF CONTACT Mike Meo, L-3 Communications Display Systems 1355 Bluegrass Lakes Pkwy Alpharetta, GA 30004 [redacted]@L-3com.com [redacted]
24. GIDEP REPRESENTATIVE Mike Meo	25. SIGNATURE Mike Meo	26. DATE 15 Dec. 2010

GIDEP Form 97-2 (September 2009)

Please refer to the complete distribution policy at the GIDEP member's website.

TAB 18

Counterfeit Parts History Card

Date Of Occurrence	Contact Name	Contact Number	Contact E-Mail	Division
11/04/2010	Chris Durre	[redacted]	[redacted]@L-3com.com	Display Systems
Component Type	**Manufacturer**	**Manuf. Part Number**	**L-3 Part Number**	**Country of Origin**
Microcircuit (VRAM)	Samsung	KM4216C258G	U100582-000	Korea
Date Code	**Lot Number**	**Defect Quantity**	**Defect Type**	**Impact Category**
813	RMA100CB	10,055	Marking	Major
Independent Disti.	**Supplier**	**Type of Packaging**	**GIDEP Notification**	**ERAI Report Date**
Global IC	Hongdark	Reel	GG5-A-11-01	12/17/10

Incident Summary:

L-3DS received a total of 10,055 pieces of KM4216C258G-50 from an independent distributor (KM4216C258G-50 is obsolete and not available from an authorized distributor). All of the components were date code 813. A sample of 2 components was delivered to an independent L-3 approved test facility with no obvious signs of suspect/counterfeit characteristics observed in March of 2009.

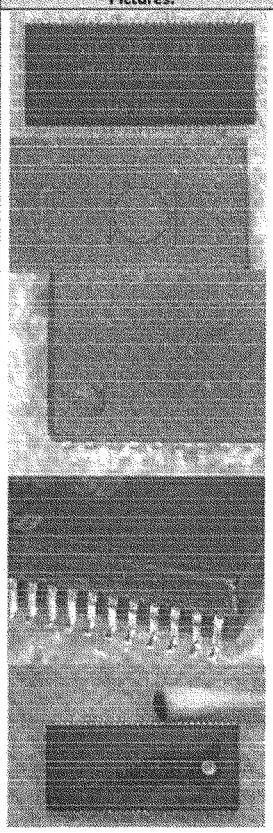
During production testing in November of 2010, a high failure rate at ambient temperature prompted L-3DS to conduct further testing. Another sample of the 813 date code parts were sent to a different L-3 approved test facility. Multiple abnormalities during testing were reported:

- Rough surface in the pin one location and top surface mold cavity location.
- Discoloration/ Inconsistent color on the side of the VRAM.
- Material was removed with acetone.

The samples were confirmed to have the correct internal circuitry:

- X-ray analysis matched a part from a confirmed date code.
- Decapsulation confirmed that the die number, logo, and date match a confirmed date code.

Pictures:



Resolution Summary:

All parts with the 813 date code are considered to be suspect for counterfeit tampering, and have been quarantined within the MRB area.

L-3 has found a replacement part that is not obsolete.

Type "Unknown "in field if information is unavailable. Type "N/A" if information is non-applicable

L-3 Intranet / Material Management / Teams / Counterfeit Parts / CPH Cards

TAB 19

L3 Communications Internal Corrective Action Request

Document Number	CC00003914	**Revision**	D	**Status**	CLS	**Nonconforming**
Assigned To	CAC	Corrective Action Coordinator		**Business Unit**	DIS	

Identification

Summary Assemblies containing a suspect counterfeit part, U100582-000, were delivered to Lockheed Martin.

Supplier		**Part Number**	
Site Code			
Supplier Part Number			
Manufacturer Part Number			
Generated from Module		**Part Revision**	
Sequence Number			
Drawing Number		**Commodity Code**	
Drawing Revision		**Part Criticality Code**	
End Use Part / Model Number			
Location Code			
Factory			
Date Response Due	12/8/2010		
Date Response Received	12/13/2010 8:41:41 AM	**Customer**	
Date Extended	3/24/2011	**Date Identified**	
Buyer		**Lot Quantity**	
Author	durre_c	**Inspected**	
Date Created	11/29/2010 2:41:28 PM	**Nonconforming**	
Date Revised	8/19/2011 7:16:38 AM	**Lot Code**	
Revised By	lybarger	**Planner**	
Revision	30	**Program**	
PO Number		**End Item Serial Number**	
Line		**Repeat Discrepancy**	F
Work Order		**Product Group**	
Work Center		**Product Sub Group**	
FRACAS Identifier		**Customer Due Date**	
Customer CA Number		**Date Submitted To Customer**	
Contract			
Project		**Priority Rating**	
Work Supervisor			

Module	Document Number	Is Master

Associated Part Numbers

Part Number	Description	Part Revision

Processing Dates

Date Discrepancy	2/27/2011 12:51:48 PM	**Date Follow Up**	7/25/2011 2:10:28 PM
Date Cause/CA	2/27/2011 12:51:52 PM	**Date Closed**	8/19/2011 7:16:38 AM
Date Approved	3/21/2011 11:35:55 AM		

D1 Team Members

First Name	Last Name	Subscription Identifier	Title / Occupation

Discrepancy

Letter: A

		Category Code	Process Code	
Revised By	durre_c	Chris Durre	Date Revised	11/29/2010 3:07:19 PM
D2 Problem Defined	T		Revision	3

Discrepancy Description:

During testing, L-3 identified that the U100582-000 VRAM chip with the 813 date code. The components were sent out for testing by an independent lab, and were found to be suspect counterfeit. Refer to the attached report for additional details.

Customer discrepency as reported on CAR 15444 is as follows:

L-3 Display Systems SDL SD00387 indicates an issue with a purchased part, the Samsung U100582-000 4MB IC VRAM chip (date code 813) utilized in the Graphics processor board that goes into both the -11 & -13 CMDUs and the -13 MFCD. Additional testing by an external laboratory has confirmed the U100582-000 VRAM chip has been remarked. Parts are suspect to be counterfeit. L3 indicated the parts were purchased from an L3 Corporate approved source/distributor with receipts beginning in March 2009. The distributor Global IC is not an approved OCM distributor per Para C in above requirement. Additional testing by an external laboratory has confirmed the U100582-000 VRAM chip has been remarked. Parts are suspect to be counterfeit. This is the second occurance of counterfeit parts from Global IC via Hongdark ref. CAR 13554 4 Nov 2009 for the Lattice chip.

Attachment

\\edmund\company\CA Attachments\CC3914 report from SMT.pdf

D0 Emergency Response Action

Letter: A

ERA Implemented T	ERA Performed By durre_c	Date Revised 11/29/2010 3:07:19 PM	Revision 3

ERA Comments

Shipment of all units was stopped until the problem could be evaluated further.

D3 Containment Action

Letter: A

Containment Implemented	T	Containment Performed By	durre_c
Date Containment Complete	11/29/2010 3:07:19 PM	Date Containment Due	11/29/2010 2:41:38 PM

Containment Comments

All assemblies within L-3 display systems containing the suspect U100582-000 VRAM were stopped from shipping. ECN 57322 was implemented to rework the assemblies with the U100538-001 VRAM chip, which is available from the OCM.

A supplier disclosure letter was generated and submitted to Lockheed Martin containing a list of serial numbers that may contain the U100582-000 VRAM. Refer to the attachment for additional details.

Cause/Corrective Action

Letter A

Cause Code V01 Supplier Induced
Corrective Action Code ECN ECN to be generated.
Revised By durre_c Chris Durre **Date Revised** 2/26/2011 7:51:54 AM
Action Due **Revision** 5

Detail Task Planning Required for this line item? F
Preventative Action T **Corrective Action** T

D4 Root Cause Analysis

Supplier Induced:

Counterfeit parts were not pulled from stock previously during lattice chip - Determine the source, and implement a process for reacting to issues. Include the requirement for disclosure of the source in the QA clause.

Parts were approved for usage - Small sample size, and policy allows us to accept a large lot based on a small sample size

Lybarger
During the investigation several areas of concern were detected:

- Supplier (Global IC) supplied parts procured from a source known to have provided counterfeit parts in the past.
- Global IC did not test parts prior to shipping them to Oneida Research Labs for testing.
- A date code sample was slsected by Global IC and sent to ORS for independent testing and found to be acceptable by them.

D5 Permanent Corrective Action Description

ECN to be generated.

ECN 57322 has been initiated to change the VRAM chip on the part to an alternate (U100538-001), and to increase the C/S level of the units. Pending a response from Lockheed, L-3 will replace the U100582-000 units on an attrition basis through the effectivity date on ECN 57322.

If attrition is not accepted as a response, L-3 modify all units through return from the field.

Lybarger

- Global IC has been Disapproved as a vendor for Display Systems and the corporate counterfeit parts team has been notified of the latest issue.
- Testing will require the supplier to send the entire order fo testing and the test house will select the sample
- ORS will no longer be considered for testing. Future testing will be conducted by SMT Corp.

D7 Preventative Corrective Action Description

Modify ENG 010-049 to incorporate changes in sample size, as well as testing requirements. Update QA 122-305A clause 30.0 to communicate the change in requirements to the supply base.

Lybarger
Quality clause 30.0 is being rewritten to address vendor QMS requirements for counterfeit parts mitigation. Until QA 122-305A is revised QAB 609 is in effect, see attached.

D4 Root Cause Analysis

RCA Defined T **RCA Performed By** lybarger **Date RCA Defined** 12/13/2010 8:41:29 AM

D5 Permanent Corrective Action

PCA Defined T **PCA Performed By** lybarger **Date PCA Defined** 12/13/2010 8:41:30 AM

Preventative Action Attachment

\\edmund\company\ISO 9001\QAB\QABs\120710_609.pdf

CA Approvals

Rev	Responsible		Approved By	Date/Time Approved	N/A
A	CAC				
C	CAC				
D	CAC	lybarger	Ron Lybarger	3/21/2011 11:35:55 AM	
A	durre_c				
C	durre_c	durre_c	Chris Durre	2/26/2011 7:52:01 AM	
D	durre_c	durre_c	Chris Durre	3/21/2011 10:56:00 AM	

Approval Comments

Follow Up

Effectivity		Reinspection Results		Follow Up	
Date	3/21/2011	On Hand		Date Action Due	7/15/2011
Quantity		Accepted		Date Verified	7/25/2011
Unit		Discrepant		Verified By	pawar_d
				Verified	T

Followup Comments

ENG 010-049 Rev B issued for circulation on 6/10/11.

D6 Permanent Corrective Action Effectivity

PCA Effectivity Verified T **PCA Verified By** pawar_d **Date PCA Verified** 7/25/2011

D7 Effectiveness

Effectiveness Verified T **Effectiveness Verified By** pawar_d **Date Effectiveness Verified** 7/25/2011

Closure Information

Letter A

Date Revised 8/19/2011 **Revision** 2 **Revised By** lybarger Ron Lybarger

D8 Team Recognition

Team Recognized T **Recognition Performed By** lybarger **Date Recognition Complete** 7/25/2011

TAB 20

communications
Integrated Systems

7500 Maehr Road (76705-1647)
P.O. Box 154580
Waco, Texas 76715-4580
Phone: (254) 867-7868 [redacted]

19 September 2011
11-KAK-125415

Department of the Air Force
866 AESG/JCA
2275 D Street Bldg 16, Rm 149
Wright Patterson AFB, OH 45433-7239

Attention: Mr. James Leighty, Contracting Officer
(via email: [redacted]

Subject: Contract W58RGZ-07-D-0099, Notification of Suspect Electronic Components

Dear Mr. Leighty:

L-3 Communications Integrated Systems (L-3/IS) has been notified today by its major subcontractor and supplier, Alenia Aeronautica, SpA, of the inclusion of suspect electronic components in several avionics items within the Joint Cargo Aircraft C-27J hardware previously delivered to the Government. These involve the Bus Adapter Unit (BAU) Type I provided to Alenia by Goodrich and the Color Multipurpose Display Units (CMDUs) provided to Alenia by L-3 Displays. This information has been received as part of ongoing dialogues and discussions related to queries from the SPO and other US Government agencies in the past week. The details as we know them are as provided below.

Bus Adapter unit (BAU) Type I (Goodrich Part Number 30106-01)

Alenia Aeronautica has reported to L-3 Communication Integrated Systems that it was notified by Goodrich of suspect, unapproved parts in several of the Type I BAU in August 2009. Although Alenia issued internal instructions to locate the affected BAU serial numbers and to return them to Goodrich, these parts were not retrieved prior to the delivery of the C-27J aircraft to L-3 Communication Integrated Systems and subsequently to the Government. Before 19 September 2011, no notification of this issue in the C-27J program has ever been provided by Alenia to L-3 Communications Integrated Systems nor, to the best of Alenia's knowledge, to the US Government.

Goodrich communications indicated that the use of the suspect parts would not constitute a safety issue. Alenia performed an engineering assessment of the nonconformity configuration as installed on C-27J and determined that there is no safety of flight issue associated with this discrepancy, and that no critical failure modes which would compromise the safe operation of the aircraft have been identified (i.e., there are no catastrophic hazards associated to a failure of the Bus Adapter Unit Type I). Alenia believes that this conclusion is consistent with the engineering analysis performed by Goodrich.

Goodrich advised that the affected BAUs can be recalled for rework/replacement/repair at the Government's convenience. A Service Bulletin is being prepared by Alenia to provide directions for this removal and processing of the affected BAUs. The details of the release dates and processing will be coordinated with the Government to minimize disruption to the JCA C-27J fleet operations.

Color Multipurpose Display Units (CMDU) L-3 Part Number 104000-603

In December 2010, L-3 Display Systems issued a formal Alert via the Government Industry Date Exchange Program (GIDEP) for a series of Samsung 4 MegaByte Integrated Circuit Video Random Access Memory (VRAM) chips used in CMDUs and Multi-Function Control Displays (MFCDs) installed on the Alenia C-27J and other aircraft.

The initial issue was discovered internally in L-3 Displays through a perceived increase of failures during testing of the displays. Subsequent detailed investigation and additional testing imposed by L-3 Displays and performed by external laboratories confirmed that in numerous instances the VRAM chips had been remarked. This was traced to a single lot code.

A failure assessment was performed, and safety assessments of the results ensure that no reduced performance has been reported or exhibited in the field operation. The types of failure possible from failures of the VRAM chips include degraded visual imagery on the display or blank screen/loss of the display. No CMDU components that failed the L-3 Displays internal screening process were ever issued for installation or delivery to Alenia Aeronautica or any other customer.

In the same month, L-3 Displays notified Alenia that it had identified a series of suspect electronic component installations involving CMDUs previously delivered for the Alenia C-27J aircraft program. The occurrence of the suspect part included nearly 100 CMDUs delivered to Alenia Aeronautica for use in the C-27J product line, which includes aircraft, spares, flight simulator and test rig units.

Alenia performed engineering/safety assessment using all available information and test results provided by L-3 Displays and concluded that no inspection on the suspect assembly was necessary. Also, no recall action on the items was requested by L-3 Displays. No Service Bulletin was issued by Alenia Aeronautica, since no recall was requested. Prior to 19 September 2011, no notification was ever made to L-3 Communications Integrated Systems nor to the US Government regarding the suspect items in the L-3 Displays CMDU delivered for the C-27J program.

Monitoring in services CMDUs was performed and no relevant changes in failure percentages were noticed (the failure rate of CMDUs in operation has remained unchanged).

The table below identifies the serial numbers of the CMDUs containing the suspect VRAM chip that are installed on, or intended for use in, the US Government JCA C-27J program. This information reflects what was installed on each aircraft at the time of delivery to L-3 Communications Integrated Systems. There have been very few changes to the installed configurations since delivery to the US Government.

CMDU Serial Number	Installed on C-27J Aircraft
4093	Spare Part
4106	USAF 8
4044	USAF 3
4045	USAF 3
4049	USAF 3
4053	USAF 3
4054	USAF 4
4060	USAF 4
4061	USAF 4
4062	USAF 4
4074	USAF 10
4076	USAF 7
4077	USAF 7
4079	USAF 6
4081	USAF 8
4082	USAF 10
4083	USAF 8
4085	USAF 10
4086	USAF 7
4087	USAF 10
4088	USAF 10
4091	USAF 7
4092	USAF 7
4100	USAF 6
4101	USAF 6
4102	USAF 6
4104	USAF 8
4105	USAF 6
4121	USAF 11
4122	USAF 11
4123	USAF 9
4126	USAF 9
4127	USAF 9
4128	USAF 9
4130	USAF 9
4137	USAF 11
4139	USAF 11
4140	USAF 11

We are working to determine more of the exact details regarding this issue and will provide additional dialogue and materials to the C-27J SPO in the near future. For questions regarding this matter, please contact Greg Bruich at [redacted]/e-mail [redacted]@l-3com.com. For contractual correspondence, please contact Kimberly Kachura at [redacted]/e-mail [redacted]@l-3com.com.

Sincerely,

L-3 Communications
Integrated Systems
Platform Integration Division

Kimberly Kachura

Kimberly Kachura
Contracts Manager
C-27J Programs

TAB 21

[redacted]

From: Paul Meyers <[redacted]@gictg.com>
Sent: Wednesday, November 10, 2010 2:50 PM
To: [redacted]@l-3com.com; [redacted]@L-3com.com; [redacted]@L-3com.com; [redacted]@l-3com.com; [redacted]@L-3com.com
Cc: Lori Leroy; Nick Cirocco
Subject: L-3 display info
Attachments: InspectionPics.pdf; Rec_7249_7326.pdf; Rec_7436.pdf; InspectionPics.pdf; FRM7402-B_Inspection_List.pdf; FRM7402-B_Inspection_List_Cover.pdf; FRM7402 _Product_Receiving_Report_Cover.pdf; FRM7402_Product_Receiving_Report.pdf; CAR_ 48.pdf

Greetings-

First, I would like to apologize for this unfortunate situation. Per our conversation earlier today we have attached two receiving reports along with inspection photos for your p/n U100582-000 that we received. The visual inspection process follows IDEA STD1010A and our inspection process has evolved as follows:

8-2008 Implemented in-house X-Ray and Decapsulation and detailed inspection - no sample quantity requirements unless specified by customer; Inspector discretion
6-2009 Lead inspector obtained IDEA ICE 3000 certification
11-2009 Implemented Sampling Plan that requires 100% visual inspection of package and product inspection per Sampling Chart (attached).
8-2010 Changed Sampling Plan to reflect new sampling quantities based on supplier approval level
11-2009 Changed Receiver/Inspection report to include sampling quantities
7-2010 Changed Receiver/Inspection report and process to include a pass/fail at every step of inspection which includes the inspector's name (attached).
7-2010 Changed L-3 Inspection criteria (all facilities) to include 100% microscope inspection

The name of our supplier is Hongdark Electronic Trade in China. The vast industry references checked by our purchasing staff revealed multiple positive comments and solid references including 2 from other IDEA members and zero negative references which our process allows for a provisional supplier.

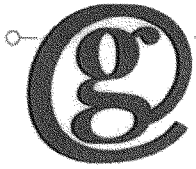
Per our SCAR # 48 (attached) issued on 12/2/09 we disqualified this supplier. That said, this supplier is in fact the same supplier for your p/n U100188-000. All of the purchases made for the parts listed above were made prior to the disqualification of the supplier. All product from this supplier passed our visual, X-ray, and decap as well as the third party inspection done by Oneida.

Further after a review of Display's sales history we feel it is our responsibility to share than we found one other part that we purchased from this supplier in October of 2009, (89 pcs of your p/n U100802-000) on your PO A99032. Again, this product went through the same process that all product goes through for Displays (Global IC Trading Group visual, X-ray, and decap as well as independent inspection from Oneida).

From our conversation this morning, we did sense your frustration with Global IC Trading Group not sharing supplier information. Please understand that this is usually not something that independent distributors participate in. However, we wanted to gather all the information and present all the data accurately. Our intention was in no way meant to be misleading or lacking integrity.

Paul Meyers
Global IC Trading Group
26051 Merit Circle #106
Laguna Hills CA 92653
www.gictg.com
[redacted]
AS9120 & ISO 9001 Certified
ANSI/ESD S20.20 Certified

TAB 22



GLOBAL IC TRADING GROUP
26051 Merit Circle, #106
Laguna Hills, California 92653
Phone 949.421.1140
Fax 949.421.1151
www.gictg.com

Via FedEx[redacted]

June 24, 2011

Ilona R. Cohen
Counsel
U.S. Senate Armed Services Committee
228 Russell Senate Office Building
Washington, D.C. 20510

Re: Response to U.S. Senate Armed Services Committee letter dated June 7, 2011

Dear Ms. Cohen

Pursuant to the letter dated June 7, 2011 from the U.S. Senate Armed Services Committee requesting information and documents regarding counterfeit electronic parts entering the DOD supply chain, we have enclosed on two separate thumb drives (one for the majority and one for the minority) a total of 817 pages (excluding this cover letter) as follows:

Question 1 – pages 1 -396
Question 2 – pages 397 - 746
Question 3 – pages 747 -813

We hope that this information is useful in your investigation. Global IC Trading Group has been in business for 11 years and we have witnessed the counterfeit problem grow rapidly. As you can see, our company has been the victim of suspect material, and we have taken great strides to improve our processes and avoid suspect material entering the supply chain.

Since joining the IDEA organization in May of 2009, we have learned a great deal from our competitors/fellow IDEA members in detection methods and best practices. We will continue to improve in all aspects of our business and maintain our status of a preferred independent distributor in our industry.

Sincerely,

Lori LeRoy
Global IC Trading Group

enclosure

Global IC Trading Group
Response to Questions #2

Supplier to Global IC Trading	Manufacturer, Part # and Date Code	Quantity Bought by Global IC Trading	Purchase Date	Customer	Quantity Sold by Global IC Trading	Date of Sale	Testing and Date of Test Report
Hong Dark Electronic Trade	IC Designs, KD2001SC1, DC 9811	202	3/23/2009	L-3 Communications Cincinnati Electronics	200	4/16/2009	Yes - Global IC Trading dated 6/9/09
Hong Dark Electronic Trade	Lattice, [redacted] DC 9533	6	9/26/2008	L-3 Communications Corp Display Systems	0	n/a	Yes - Oneida dated 10/27/2008
Hong Dark Electronic Trade	Lattice, [redacted] DC 9533	2315 4	11/12/2008	L-3 Communications Corp Display Systems	2314 4	11/24/2008 12/3/08	Yes - Global IC Trading dated 11/24/2008
Hong Dark Electronic Trade	Lattice, [redacted] DCc 9533	831	3/4/2009	L-3 Communications Corp Display Systems	829	3/2/2009	Yes - Global IC Trading dated 3/26/09
Hong Dark Electronic Trade	Micron, MT28F400B5SG-8TET, DC 0450	4000	10/7/2009	L-3 ACSS	0	n/a	Yes - Anloy 12/7/09
Hong Dark Electronic Trade	Samsung, KM4216C258G-50, DC 0813	3500 1000	2/12/2009	L-3 Communications Corp Display Systems L-3 Communications Corp Display Systems	3500 1000	3/20/2009 4/9/09	Yes - Oneida. 2/24/09 report attached
Hong Dark Electronic Trade	Samsung, KM4216C258G-50, DC 0813	6057	3/14/2009	L-3 Communications Corp Display Systems	6055	6/24/2009	Yes, Global IC Trading dated 11/22/10
Hong Dark Electronic Trade	TI, TPS79028DBVR, 0836	9000	5/7/2009	ABX Engineering	9000	5/12/2009	accepted, photos only
Hong Dark Electronic Trade	Agilent, HDMP-1024, 0504	21	8/27/2009	L-3 Communications Systems West	0	n/a	rejected, photos on file
Hong Dark Electronic Trade	Agilent, HDMP-1024, 0504	20	5/21/2009	L-3 Communications Systems West	12	5/29/2009	Yes - Global IC Trading dated 5/29/09
Hong Dark Electronic Trade	Atmel, AT29C040A-20TI, 9810	501	2/25/2009	L-3 Communications Cincinnati Electronics	500	3/5/2009	Yes - Global IC Trading dated 03/04/09
Hong Dark Electronic Trade	Freescale, MC34119EFR2, 0812	20000	2/19/2009	Lockheed Martin Material Acquisition	19990	2/26/2009	Yes - Global IC Trading dated 2/23/09
Hong Dark Electronic Trade	Freescale, MC34119EFR2, 0918	20000	6/2/2009	Lockheed Martin Material Acquisition Center Mid Atlantic	19998	6/11/2009	Yes - Global IC Trading Group dated 6/11/09
Hong Dark Electronic Trade	Freescale/Mot, MRF9060LSR1, 04+	101	2/12/2009	ORI Services Corporation		2/19/2009	accepted, X-Ray and decap done; photos only

398

GLOBAL IC TRADING GROUP
26051 Merit Circle #106
Laguna Hills, CA 92653 USA
www.gictg.com

Global IC Trading Group
Response to Questions #2

Supplier to Global IC Trading	Manufacturer, Part # and Date Code	Quantity Bought by Global IC Trading	Purchase Date	Customer	Quantity Sold by Global IC Trading	Date of Sale	Testing and Date of Test Report
Hong Dark Electronic Trade	Hynix, HY5DU283222BFP-28, 0621	20	3/23/2009	Thomson Inc dba-Grass Valley	12	4/6/2009	accepted, X-ray done; photos only
Hong Dark Electronic Trade	Hynix, HY5DU283222BFP-28, 0621	168	6/10/2009	Thomson Inc dba-Grass Valley	168	6/22/2009	accepted, X-ray done; photos only
Hong Dark Electronic Trade	Hynix, HY5DU283222BFP-28, 621A	672	9/29/2010	Thomson Inc dba-Grass Valley	0	n/a	accepted, X-ray done; photos only
Hong Dark Electronic Trade	IC Designs / Cypress, ICD2051SC1, 9918	23	5/1/2009	L-3 Communications Telemetry West	25	6/10/2009	Yes - Anloy 5/27/09; dated Global IC Trading 6/9/09
Hong Dark Electronic Trade	Intel, E28F016SV65, 0505	200	6/16/2009	L-3 Communications Corp. Display Systems	0	n/a	rejected, photos on file
Hong Dark Electronic Trade	Intel, RC28F128K3C-115, 03+	900	11/10/2009	L-3 Communications Systems West	898	12/2/2009	Yes - Global IC Trading Group dated 11/30/09
Hong Dark Electronic Trade	Intel, TB28F400BV-T60, 0320	60	10/2/2009	L-3 ACSS	0	n/a	rejected, photos on file
Hong Dark Electronic Trade	Intel, TE28F128J3C150, 05+	501	2/26/2009	L-3 Communications Cincinnati Electronics	500	3/12/2009	Yes - Global IC Trading Group dated 3/12/09
Hong Dark Electronic Trade	LSI Logic/Cisco, L2A1285, 0035/0539	110	2/17/2009	Flextronics International Technologia LTDA	110	2/25/2009	accepted, X-ray done; photos only
Hong Dark Electronic Trade	LSI LOGIC/CISCO, L2A1919, 0423	40	2/12/2009	Flextronics International Technologia LTDA	40	2/25/2009	accepted, X-ray done; photos only
Hong Dark Electronic Trade	Micron, MT28F800B5SG-8BET, 0522, 0948	5010	1/9/2009	L-3 ACSS	5000	2/18/2009	Yes - (2) Global IC Trading Group dated 1/26/09
Hong Dark Electronic Trade	Micron, MT28F800B5WG- 8T, 01+	20	4/29/2009	CTS	10	5/5/2009	Yes - Global IC Trading Group dated 5/5/09
Hong Dark Electronic Trade	MICRON, MT48LC1M16A1TG-7S, 0040	2160	3/3/2009	L-3 Communications Corp. Display Systems Div	2138	4/24/2009	Yes - Oneida dated 3/27/09
Hong Dark Electronic Trade	MICRON, MT48LC1M16A1TG-7S, 0040	48	4/29/2009	L-3 Communications Corp. Display Systems Div.	43	5/21/2009	accepted, X-ray done; photos only
Hong Dark Electronic Trade	MICRON, MT48LC1M16A1TG-7S, 0040	62	7/27/2009	L-3 Communications Corp. Display Systems Div.	50	8/31/2009	accepted, X-ray done; photos only
Hong Dark Electronic Trade	Motorola, MC14490L, 9816	54	7/20/2009	L-3 Ruggedized Command & Control	50	9/8/2009	Yes - Global IC Trading Group dated 8/5/09
Hong Dark Electronic Trade	Motorola, MC9S12D64MFUE, 0723	802	4/9/2009	ABX Engineering	800	4/21/2009	accepted; X-ray, decap done; photos only

399

GLOBAL IC TRADING GROUP
26051 Merit Circle #106
Laguna Hills, CA 92653 USA
www.gictg.com

Global IC Trading Group
Response to Questions #2

Supplier to Global IC Trading	Manufacturer, Part # and Date Code	Quantity Bought by Global IC Trading	Purchase Date	Customer	Quantity Sold by Global IC Trading	Date of Sale	Testing and Date of Test Report
Hong Dark Electronic Trade	Motorola, MC9S12D64MFUE, 0723	631	9/21/2009	ABX Engineering	618	9/28/2009	accepted, X-ray done; photos only
Hong Dark Electronic Trade	Philips, SA5205AD, 0029	1010	3/17/2009	L-3 ACSS L-3 ACSS	313 687	/2009G1/15/10	Yes, Global IC Trading 4/17/09
Hong Dark Electronic Trade	Phillips, SA7025DK, 9944	2555	2/12/2009	Lockheed Martin Material Acquisition Center Mid Atlantic Region	2550	2/23/2009	Yes, Global IC Trading dated 2/20/09
Hong Dark Electronic Trade	Samsung, KM684000BLR-5L, 9949	505	5/14/2009	L-3 Communications Cincinnati Electronics	500	5/28/2009	Yes - Global IC Trading dated 5/28/09
Hong Dark Electronic Trade	Samsung, KM68V4002BLT-15, 9913	1002	2/23/2009	L-3 Communications Cincinnati Electronics	1000	3/5/2009	Yes - Global IC Trading dated 3/4/09
Hong Dark Electronic Trade	Samsung, KM68V4002BLT-15, 9913	305	5/14/2009	L-3 Communications Cincinnati Electronics	300	5/29/2009	Yes - Global IC Trading dated 5/29/09
Hong Dark Electronic Trade	Samsung, KM68V4002BLT-15, 9913	235	7/16/2009	L-3 Communications Cincinnati Electronics	234	8/6/2009	Yes - Global IC Trading dated 8/5/09
Hong Dark Electronic Trade	ST Micro, 25P64V6P, 0821	50	5/11/2009	Intel Technology (US) LLC	50	5/14/2009	accepted, X-ray done; photos only
Hong Dark Electronic Trade	ST Micro, SD8257-01, 00+	21	5/18/2009	L-3 ACSS	21	5/27/2009	Yes - Global IC Trading dated 5/27/2010
Hong Dark Electronic Trade	TI, MSP430F415IPM, 08+	320	9/2/2009	KESP Sdn Bhd	320	9/11/2009	Yes - Global IC Trading dated 9/14/2010
Hong Dark Electronic Trade	TI, TMS320DM642AZDK7, 07+	250	5/8/2009	ABX Engineering	250	5/26/2009	accepted, X-ray done; photos only
Hong Dark Electronic Trade	Xilinx, [redacted]	28	3/23/2009	L-3 Communications Corp. Display Systems	0	n/a	rejected due to date code, photos on file
Hong Dark Electronic Trade	Xilinx, [redacted] 0321	93	3/23/2009	L-3 Communications Corp. Display Systems	92	10/1/2009	Yes - Oneida 4/2/09
Hong Dark Electronic Trade	Xilinx, XC2V4000-4BF957C, 0545	2	3/18/2009	EMLinQ, LLC	2	3/19/2009	Yes - Global IC Trading, dated 4/3/09
Hong Dark Electronic Trade	Xilinx, XC2V4000-4BF957C, 0545	249	3/23/2009	EMLinQ, LLC	38 42 21 90 57	4/3/2009 4/15/09 4/16/09 4/29/09 5/29/09	accepted, photos only

(400)

GLOBAL IC TRADING GROUP
26051 Merit Circle #106
Laguna Hills, CA 92653 USA
www.gictg.com

Global IC Trading Group
Response to Questions #2

Supplier to Global IC Trading	Manufacturer, Part # and Date Code	Quantity Bought by Global IC Trading	Purchase Date	Customer	Quantity Sold by Global IC Trading	Date of Sale	Testing and Date of Test Report
Hong Dark Electronic Trade	Xilinx, XC2V4000-4BF957C, 0545	10	5/18/2009	EMLinQ, LLC	4	10/15/009	Yes - Global IC Trading, dated 5/29/09
Hong Dark Electronic Trade	Xilinx, XC2VP4-6FG456C, 0518	15	2/7/2009	EMLinQ, LLC	14	2/18/2009	Yes - Global IC Trading, dated 2/18/09
Hong Dark Electronic Trade	Xilinx, XC4006E-2PQ160I, 0145	505	3/30/2009	L-3 ACSS	500	4/23/2009	Yes - Global IC Trading, Dated 4/23/09
Hong Dark Electronic Trade	Xilinx, XC95144XL-10TQG100C, 0901	1350	3/27/2009	VSS Monitoring	450 450 450	3/2/09 5/29/09 7/30/09	accepted, photos only
Hong Dark Electronic Trade	Xilinx, XCR3128XL-7CS144I, 0509	1600	2/24/2009	L-3 Communications Interstate Electronics	1597	2/11/2009	Yes - Global IC Trading, Dated 3/11/09
Hong Dark Electronic Trade	Zarlink, GP2021/IG/GQ1N, 9918	156	2/7/2009	Sigmatron International	155	2/20/2009	Yes - Global IC Trading, Dated 2/20/09

[redacted]

GLOBAL IC TRADING GROUP
26051 Merit Circle #106
Laguna Hills, CA 92653 USA
www.gictg.com

Global IC Trading Group
Response to Questions #2

Supplier to Global IC Trading	Manufacturer, Part # and Date Code	Quantity Bought by Global IC Trading	Purchase Date	Customer	Quantity Sold by Global IC Trading	Date of Sale	Testing and Date of Test Report
[redacted]							

Notes:
92sd was disqualified 10/17/09 and removed as a supplier
Hongdark Electronics was disqualified 12/10/09 and removed as a supplier after the second quality related concern with product supplied by Hongdark
Nagono was disqualified 6/22/10 and removed as a supplier
TCG - Technology Conservation Group supplier status was demoted to "elevated risk" on 6/20/11

(402)

GLOBAL IC TRADING GROUP
26051 Merit Circle #106
Laguna Hills, CA 92653 USA
www.gictg.com

TAB 23

CARL LEVIN, MICHIGAN, CHAIRMAN

JOSEPH I. LIEBERMAN, CONNECTICUT
JACK REED, RHODE ISLAND
DANIEL K. AKAKA, HAWAII
E. BENJAMIN NELSON, NEBRASKA
JIM WEBB, VIRGINIA
CLAIRE McCASKILL, MISSOURI
MARK UDALL, COLORADO
KAY R. HAGAN, NORTH CAROLINA
MARK BEGICH, ALASKA
JOE MANCHIN III, WEST VIRGINIA
JEANNE SHAHEEN, NEW HAMPSHIRE
KIRSTEN E. GILLIBRAND, NEW YORK
RICHARD BLUMENTHAL, CONNECTICUT

JOHN McCAIN, ARIZONA
JAMES M. INHOFE, OKLAHOMA
JEFF SESSIONS, ALABAMA
SAXBY CHAMBLISS, GEORGIA
ROGER F. WICKER, MISSISSIPPI
SCOTT P. BROWN, MASSACHUSETTS
ROB PORTMAN, OHIO
KELLY AYOTTE, NEW HAMPSHIRE
SUSAN M. COLLINS, MAINE
LINDSEY GRAHAM, SOUTH CAROLINA
JOHN CORNYN, TEXAS
DAVID VITTER, LOUISIANA

RICHARD D. DeBOBES, STAFF DIRECTOR
DAVID M. MORRISS, MINORITY STAFF DIRECTOR

United States Senate
COMMITTEE ON ARMED SERVICES
WASHINGTON, DC 20510-6050

October 20, 2011

Mr. Charlie Bae
President and CEO
Samsung Semiconductor, Inc.
3655 N. First Street
San Jose, California 95134

Dear Mr. Bae:

Counterfeit electronic parts in the Department of Defense's (DOD) supply chain pose a risk to our national security, the reliability of our weapons systems, and the safety of our military men and women. Government and industry share a common interest in ensuring that the DOD supply chain is free from these parts. As part of an inquiry by the Senate Armed Services Committee into suspect counterfeit electronic parts in the DOD supply chain, the Committee is seeking information from defense contractors and subcontractors, independent testing companies, and electronic component manufacturers about suspect counterfeit electronic parts.

The Committee has identified suspect counterfeit electronic parts that entered the U.S. military supply chain. The parts were sold by an independent distributor in China as new, authentic Samsung Video Random Access Memory KM4216C258G-50 parts. Enclosed with this letter is a test report from an independent testing company. The independent test report states the following:

- "Multiple abnormalities were detected while testing these components."
- "Some package measurements do not match the specifications found in the manufacturer datasheet."
- "Variations in color and texture were found along the package edges."
- "The bottom surface of one sample exhibits markings when the other two samples do not."
- "Testing these components for marking permanency with acetone lifted a large amount of black material, revealing fine scratches in the original surface and confirming these parts are blacktopped."
- "The size of the Pin-1 dimple is different than that of the other samples."
- "Based on these abnormalities these components have failed inspection and are not considered to be factory original parts."

To assist the Committee with its inquiry, please answer the following questions:

1) Does Samsung sell refurbished KM4216C258G-50 parts or have an agreement with any third party that would permit them to refurbish and sell KM4216C258G-50 parts?

2) Did Samsung use remarking or black-topping in its manufacturing of KM4216C258G-50?

3) Would Samsung recommend the use of KM4216C258G-50 parts with the anomalies described above?

4) Would Samsung warranty KM4216C258G-50 parts that exhibited the anomalies described above?

5) Please describe the short-term and long-term reliability and performance risks, if any exist, of using KM4216C258G-50 with the anomalies described above.

Please provide responsive information by October 27, 2011. Please send your response as an attachment to an email to Ilona_Cohen@armed-services.senate.gov and Bryan_Parker@armed-services.senate.gov. If you have any questions or wish to discuss this request, please contact Senate Armed Services Committee majority staff Ilona Cohen (202-224-5089) and Bryan Parker (202-224-8265) of the minority staff.

Thank you for your cooperation.

Sincerely,

John McCain
Ranking Member

Carl Levin
Chairman

Enclosures

SAMSUNG SEMICONDUCTOR, INC.
Office of the General Counsel
3655 North First Street
San Jose, CA 95134-1713
Tel: (408) 544-4000 Fax: (408) 544-4914

November 7, 2011

The Honorable Carl Levin, Chairman
The Honorable John McCain, Ranking Member
Committee on Armed Services
United States Senate
Washington, D.C. 20510-6050

Re: Inquiry re Samsung Video Random Access memory KM 4216C258G-50 parts

Dear Senators:

I am Vice President and General Counsel of Samsung Semiconductor, Inc., the North American sales, marketing and distribution arm for components made by Samsung Electronics Co., Ltd. I am writing in response to the questions posed in your letter dated October 20, 2011 and addressed to SSI President Charlie Bae. Please consider the following responses, and let me know if you have any further questions.

Question No. 1: Does Samsung sell refurbished KM4216C258G-50 parts or have an agreement with any third party that would permit them to refurbish and sell KM4216C258G-50 parts?

Answer: No.

Question No. 2: Did Samsung use remarking or black-topping in its manufacturing of KM4216C258G-50?

Answer: No.

Question No. 3: Would Samsung recommend the use of KM4216C258G-50 parts with the anomalies described above?

Answer: No. Semiconductor components have limited useful lives. Without knowing the conditions under which the components were used and/or stored, it is not possible to project the reliability of a semiconductor that was manufactured over ten years previously, even if the part was good and merchantable when it came from the factory.

Question No. 4: Would Samsung warranty KM4216C258G-50 parts that exhibited the anomalies described above?

Answer: No. As stated above, semiconductor components are life limited, and their functionality after an extended period of time depends on how they have been stored and/or used.

Question No. 5: Please describe the short-term and long-term reliability performance risks, if any exist, of using KM4216C258G-50 with the anomalies described above.

Answer: One cannot expect such parts to function properly, or at all. It is difficult to predict the various failure modes that might occur. The most likely scenario is that the part would not respond to commands and would simply fail to operate, and there would be no data output. In the case of a video memory or processor chip, the image on the device display may be absent or degraded in quality.

Samsung Semiconductor and Samsung Electronics are dedicated to providing the highest quality electronic components to our customers. We do not endorse or support any modification, reconditioning or refurbishment of our factory original components.

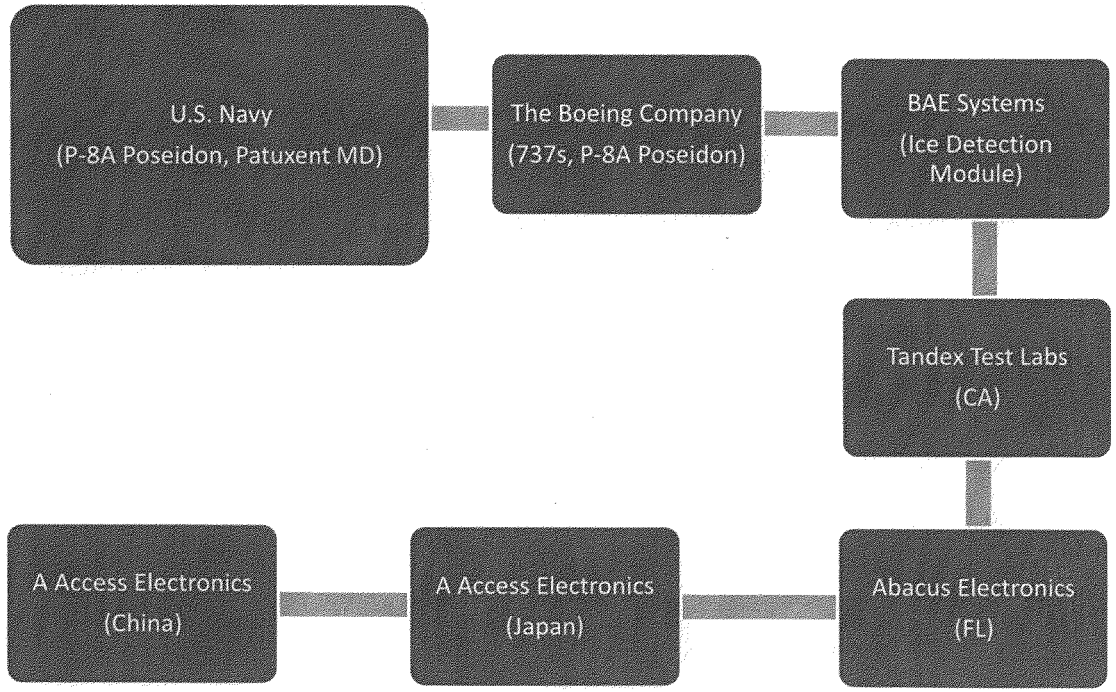
Please let us know if you have any further questions regarding these components.

Very truly yours,

Terrence H. Cross
Vice President and General Counsel

SAMSUNG SECONDUCTOR, INC. 3655 North First Street • San Jose, CA 95134-1713 • Tel: (408) 544-4000 • Fax: (408) 544-4980

Supply Chain for Suspect Counterfeit Parts in Ice Detection Module Installed on U.S. Navy P-8A Poseidon



TAB 25

BAE SYSTEMS PLATFORM SOLUTIONS

BAE SYSTEMS

Supplier Corrective Action Request (SCAR)

CAR ID: 2195

Part Number: 906-60069-149

Created By: CLARKCL

Serial Number: NA

Created Date: 12-JAN-10

Quantity Rejected: 300

Issue Title:
Refurbished Parts - 906-60069-149

Problem Description:
Brian,

I hate to be the bearer of bad news, but it appears as though we received refurbished parts from Tandex, which resulted in a field failure on a flight critical piece of hardware. In order to understand the scope of the issue, we would appreciate your help in determining the specifics surrounding the parts, as well as, the process breakdown that allowed these parts to pass the screening measures requested.

Here is the timeline...

November 2008
Sonia notified Rex that Tandex had found 300 more pcs of 906-60069-149, which was obsoleted in 2002. This is Xilinx PN XC3042A-7PG84M. Rex requested that PSPP Flow Sheet Step 1 be completed along with pictures.

December 2008
Rex got engineering to provide an Advanced Sales Order to procure these parts as a Lifetime Buy (LTB) to support several modules. The Step 1 information and pictures were passed to engineering, who completed Step 2 of the flow sheet requesting 100% visual inspection, including physical dimensions and marking permanency, along with some other testing. (See attached.) Rex then placed PO 128235 for 250 pcs (Irving) and PO 128245 for 100 pcs (50 eventually shipped to Fort Wayne & the other 50 were cancelled). PO 128235 included a $1500 charge for screening.

January – June 2009
PO 128235 50 pcs were received every month. (Jan. – May)
PO 128245 50 pcs were received in June. (Ft Wayne)

November – December 2009
BAE received word that an Ice Detector module failure at Boeing was root caused to U46 (PN 906-60069-149). The technician noted that he could hear something rattling around inside the module when it was removed from the plane. When he opened the box, the part had actually fallen out of the socket. The factory purged the remaining stock to DCA and the parts were reviewed for any potential non-conformances. The results of which are as follows:

Visual inspection was performed on 249 parts currently in QA Review. (We have an additional 50 pcs in Fort Wayne that are being sent to Irving.)

We have parts with multiple date codes:

D/C 0239 Lot X30008M Qty 90 pcs
D/C 0237 Lot X30008M Qty 8 pcs
D/C 0226 Lot X30008M Qty 86 pcs
D/C 0218 Lot X30008M Qty 15 pcs
D/C 9920 Lot X29627M Qty 8 pcs
D/C 9925 Lot X23528M Qty 39 pcs
D/C 9933 Lot X32175M Qty 3 pcs

Parts with date codes 0239, 0237, 0226, 0218 have the following inconsistencies: (See attached pics for examples.)
- different ceramic body size

The information contained in this document is the property of BAE SYSTEMS Platform Solutions and further dissemination is prohibited without the written permission of BAE SYSTEMS Platform Solutions.

BAE SYSTEMS PLATFORM SOLUTIONS

BAE SYSTEMS

Supplier Corrective Action Request (SCAR)

- different size of metal tab
- repainted metal tab (traces of masking, dull gold color, traces of sprayed paint on sides of ceramic body)
- same date code, same lot parts come with different ceramic body shape
- same lot code is used for all four different date codes (for parts manufactured in both USA and Philippines)
- signs of resurfacing
- bent leads
- bent shoulders on corner pins
- peeling coating (suspecting that pins were repainted)
- different length of pins (not meeting manufacturer's datasheet min specification)
- nicks and dents on surface of pins, evidence of reshaping/straightening pins)
- minor chips on sides of ceramic body

All these symptoms are very characteristic for refurbished/counterfeit parts.

To:

Date: 12-JAN-10
Supplier Contact Name: Brian Peale
E-Mail: [redacted]@tandexlabs.com
Supplier Name: TANDEX TEST LABS
Supplier Site: IRWINDALE CA 91706
E-mail2:
Supplier RMA #:
Response Due: 11-FEB-10

A non-conformance has been discovered on product or services provided by your company or subcontractor and is described above. Please provide corrective action response to the BAE Systems Supplier Representative identified below.

The response must be received, reviewed for adequacy and approved by BAE Systems on or before the documented due date. Your company status as a supplier may be placed in a delinquent state if this corrective action request is not received by that date.

If your investigation determines that BAE Systems is at fault, please indicate that in your corrective action response.

CORRECTIVE ACTION RESPONSE

Please address the following items in your written response by the requested due date.

1. Confirmation of issue description stated above
2. Root cause of issue
3. Reason issue was not detected
4. Immediate action(s) taken to correct issue
5. Proposed corrective action(s) to detect and prevent future occurrence
6. Detailed implementation plan of the proposed corrective action(s)
7. The date and/or serial number effectivity

The information contained in this document is the property of BAE SYSTEMS Platform Solutions and further dissemination is prohibited without the written permission of BAE SYSTEMS Platform Solutions.

BAE SYSTEMS PLATFORM SOLUTIONS

BAE SYSTEMS

Supplier Corrective Action Request (SCAR)

Originator Site: Irving TX

BAE SYSTEMS Contact Name: Carrie Mizell

Email: [redacted]@baesystems.com

Phone Number: [redacted]

The information contained in this document is the property of BAE SYSTEMS Platform Solutions and further dissemination is prohibited without the written permission of BAE SYSTEMS Platform Solutions.

Notification of Escape

(Form Instructions Included)

* * * BOEING PROPRIETARY * * *

1. DOCUMENT IDENTIFICATION

1.1. Identification of Customer: Boeing Commercial Supplier Code #:

1.3. Document Reference Number: Customer #: 578121

1.5. Category*:

1.2. Identification of Supplier/Subcontractor: BAE SYSTEMS Controls, Inc.

1.4. Document Issue: Rev New

1.6 Number of Sheets:

2. IDENTIFICATION OF PRODUCT AFFECTED

2.1 Model of Product/Program:

Replacement Parts	Spares
B717	B767
B737	B777
B747	B787
B757	Aircraft

2.2 Part Number(s): 908-60069-149

2.3 Part Description: Programmable Gate Array

2.4 Part /Serial Number/Batch/Effectivity Number Lot Number: See Attached

2.5 Quantity: See Attached

2.8 Assembly Serial Number *: See Attached

2.6 Product Number *: See Attached

2.7 Work/Purchase Order Number *: See Attached

2.9 Assembly Drawing Number *: See Attached

3. DESCRIPTION ON NONCONFORMITY

3.1 Detailed Description of Nonconformity:

The noted FPGA is an obsolete part. There is evidence that the components purchased by BAE Systems beginning in December 2008, are reworked parts and unacceptable for use. Inconsistencies include:

- Repainted metal tabs
- Signs of resurfacing
- Bent leads
- Peeling coating
- Nicks and dents on surface of pins

4. DESCRIPTION OF CAUSE/CORRECTIVE ACTION:

5. PROPOSED DISPOSITION OF NONCONFORMITY

5.1 Proposed Disposity by Supplier/Subcontractor:

BAE systems recommends replacement of the suspect components. It is notable that none of the modules have failed in service.

5.2 Limitations Imposed on the Part Design Decision:

Quality Decision *:

5.3 Flight Operaations That are Affected *: Describe Below Unknown

6. SIGNATURE

ORIGINATOR

Name: Murry Hall

Phone: [redacted]

Date: 1/7/2010

7. ADDITIONAL INFORMATION

7.1 Which Regulatory(ies) Have Been Notified:

7.2 Availability of Replacement Parts:

7.3 Availability of Personnel to Perform Work:

7.4 In-Service Units Affected:

8. DISTRIBUTION LIST:

9. HOW DEFICIENCY WAS DISCOVERED: Internal Investigation

10. RESPONSIBLE PQA REPRESENTATIVE: LeRoy Anderson

10.1 Responsible Procurment Agent/ Contract Administrator: Theo Rozario

Notification of Escape

Parts Listing

Part Number	Part Name	Part Identification	Quantity	Boeing PO	Ship Date	AssemblyDrawing	LineUnits
69-78533-1 MOD A	Module Assy - Ice Detection	D00078	1	614-000235217	06-23-2009	69-78533	Unknown
69-78533-1 MOD A	Module Assy - Ice Detection	D00079	1	614-000235217	06-23-2009	69-78533	Unknown
69-78533-1 MOD A	Module Assy - Ice Detection	D00080	1	614-000235217	06-20-2009	69-78533	Unknown
69-78533-1 MOD A	Module Assy - Ice Detection	D00081	1	614-000242510	07-15-2009	69-78533	Unknown
69-78533-1 MOD A	Module Assy - Ice Detection	D00082	1	614-000242510	08-07-2009	69-78533	Unknown
69-78533-1 MOD A	Module Assy - Ice Detection	D00083	1	614-000247118	08-13-2009	69-78533	Unknown
69-78533-1 MOD A	Module Assy - Ice Detection	D00084	1	614-000247118	08-21-2009	69-78533	Unknown
69-78533-1 MOD A	Module Assy - Ice Detection	D00085	1	614-000247118	11-09-2009	69-78533	Unknown

TAB 27

SDR Closure Template (delete answers that are not applicable)

SDR RFA Number: A6750001850
SDR Subject: ICE DETECTION MODULE ASSEMBLY
Supplier NOE: (Yes)
RFA Originator: Rohrbach
Liaison Engineer: Rohrbach
COSP Number (if applicable):
Service Engineer: Robert Kertesz Phone Number: [redacted]
Project Engineer: Jeff Look
Estimated/actual number of airplanes or spares affected by issue:
Cost impact of issue to operator: (High) (Medium) (Low/None)
Safety Determination: (Airplane Safety) (Personal Safety) (Not Safety)
(if applicable) (Addressed by existing action, Reference:)
Safety Board (if applicable): (EIB) (SRB) (Cross-Model SRB)
Safety Process Reference Number:
SRP Number (if applicable):
Basis for safety/not safety determination:

Planned In-Service Action(s): (provide complete description of in-service corrective action(s), such as inspection service bulletin, parts replacements, etc. and the method to implement the corrective actions)

NAR

Change Process: (MRR) (PRR) (BCS message) (None)
Change Process reference(s):

Reason for In-Service Action(s): (provide complete justification and/or analyses, if no in-service action is needed, please provide justification for no action)

Components may have a somewhat lower reliability, the engineering consensus is that the units can remain on the airplane and be repaired on an atrition basis.

SDR Data Quality Feedback: (missing information, wrong part numbers, incomplete problem description, etc.)

Would earlier SE involvement in the investigation of this issue helped speed resolution of this issue? (Yes) (No)

If yes, why?

TAB 28

BOEING

P-8A

Item Number: ZVD-P-8-TR-KSEA-11-0389

Subject: ICE DETECTION MODULE ASSEMBLY
Date Created: 08/17/2011 18:58 GMT **Inquiry Date Approved:** 08/18/2011 13:25 GMT
Status: Create Response

Priority: Critical **Date Due:** 08/22/2011
Location: Seattle (KSEA)
ATA: (2400-00) Electrical Power - General
Asset Number: YP004 **Model:** P-8A (Line: 2931 BUNO: 167954)
Cycles: 0 **Hours:** 0

Inquiry Type: Airplane **External Document #**
Requestor: **Operator:**
Organization:

Part Number:
Part Nomenclature:
Serial Number:
Suitable Sub/Vendor Part Number:
Software Version:
Cage:

References:

REF DES: **Recurring Condition:** Yes √ No

Reason for Inquiry:
Affected Unit: YP004
At the next available opportunity please replace the electrical equipment P5 overhead module installation, P/N 69-78533-1 from BAE. It is suspected that the module may be a re-worked part that should not have been put on the airplane originally and should be replaced immediately. Please contact BAE for an acceptable replacement part.

Inquiry Author: Avila,Steve **Phone:** [redacted]

Inquiry Approver: Johnson, Dan **Phone:** [redacted]
Date: 08/18/2011 13:25 GMT
Inquiry Approval Comments:

Inquiry Assigner: Johnson, Dan **Phone:** [redacted]
Date Assigned: 08/18/2011 13:25 GMT
Assigned To: McDowell,Joel **Phone:** [redacted]
Comments:

Export Notice: The information disclosed hereunder may include United States origin technical data. Accordingly, the receiving party is responsible for complying with and assures the disclosing party that it will comply with all export regulations of the United States, including the U.S. Department of State International Traffic in Arms Regulations (Title 22 CFR Parts 120-130), the U.S. Department of Commerce Export Administration Regulations (Title 15 CFR 768-799), and any other U.S. Government regulations applicable to the export or disclosure of such controlled technical data (or the products thereof) to Foreign Nationals, whether within or without the U.S, including those employed by or otherwise associated with the receiving party.

Note: Printed version is reference only Master record and all electronic approvals for this TR are archived in VECTOR Printed on: 08/18/2011 16:11 GMT

TAB 29

DEPARTMENT OF THE NAVY
NAVAL AIR SYSTEMS COMMAND
RADM WILLIAM A. MOFFET BUILDING
47123 BUSE ROAD, BLDG 2272
PATUXENT RIVER, MARYLAND 20670-1547

IN REPLY REFER TO:
Ser AIR-2.3.E.1/11-088
31 Oct 2011

The Boeing Company
Attn: Ms. Maureen Carlson
7755 East Marginal Way
P. O. Box 3707
Seattle, WA 98124-2499

Subject: CONTRACTOR USE OF "COUNTERFEIT" PARTS

Ref: (a) N00019-09-C-0022
(b) N00019-04-C-3146

Dear Ms. Carlson:

1. This letter serves to remind The Boeing Company of its obligation to ensure that deliverables made under references (a) and (b) are in conformance with contractual requirements and do not contain any "counterfeit" material.

2. Reference (a), N00019-09-C-0022, Statement of Work (SOW) paragraph 3.1.4.1.2, Material Review, states "The contractor shall construct records of nonconforming material. All nonconforming material shall be identified and kept separate from the production process until disposition. The contractor shall conduct a Material Review Board (MRB) to disposition nonconforming material. The contractor shall obtain Government approval for "use as is" or repair dispositions when the nonconforming material affects safety, health, performance, interchangeability, reliability, maintainability, function, or weight. "Use as is" and repair dispositions that require MRB review shall be documented and provided at the time of acceptance as supporting documentation."

3. Contract clause 252.246-7003, Notification of Potential Safety Issues, which is part of reference (a) requires the contractor to notify the cognizant Administrative Contracting Officer (ACO) and the Procuring Contracting Officer (PCO) as soon as practicable but not later than 72 hours after discovery of all nonconformances or deficiencies that may result in a safety impact.

4. The Government's position is that any "counterfeit" material received in conjunction with the execution of the above referenced contracts is nonconforming material and shall be immediately reported to the Government.

5. In the event The Boeing Company is made aware of any "counterfeit" materials present on any aircraft and/or aircraft system prior to or after delivery to the Government is made, immediate notification should be made to the cognizant ACO and the PCO.

6. This letter should not be construed as an obligation or commitment on the part of the Government of any kind. This letter constitutes no authorization for increase or decrease in cost or schedule to reference (a) and (b), or any other contract in force between the Government and The Boeing Company. If you have any questions pertaining to this notification, please contact the undersigned at [redacted], email [redacted]@navy.mil.

Sincerely,

Clare C. Carmack
Contracting Officer

Copy to:
PMA-290; CAPT S. Dillon
AIR-11.3; Robert McCall
DCMA Seattle; Debra Hafert

TAB 30

CARL LEVIN, MICHIGAN, CHAIRMAN

JOHN McCAIN, ARIZONA
JAMES M. INHOFE, OKLAHOMA
JEFF SESSIONS, ALABAMA
SAXBY CHAMBLISS, GEORGIA
ROGER F. WICKER, MISSISSIPPI
SCOTT P. BROWN, MASSACHUSETTS
ROB PORTMAN, OHIO
KELLY AYOTTE, NEW HAMPSHIRE
SUSAN M. COLLINS, MAINE
LINDSEY GRAHAM, SOUTH CAROLINA
JOHN CORNYN, TEXAS
DAVID VITTER, LOUISIANA

RICHARD D. DEBOBES, STAFF DIRECTOR
DAVID M. MORRISS, MINORITY STAFF DIRECTOR

United States Senate
COMMITTEE ON ARMED SERVICES
WASHINGTON, DC 20510-6050

October 20, 2011

Mr. Moshe N. Gavrielov
President and CEO
Xilinx, Inc.
2100 Logic Drive
San Jose, CA 95134

Dear Mr. Gavrielov:

Counterfeit electronic parts in the Department of Defense's (DOD) supply chain pose a risk to our national security, the reliability of our weapons systems, and the safety of our military men and women. Government and industry share a common interest in ensuring that the DOD supply chain is free from these parts. As part of an inquiry by the Senate Armed Services Committee into suspect counterfeit electronic parts in the DOD supply chain, the Committee is seeking information from defense contractors and subcontractors, independent testing companies, and electronic component manufacturers about suspect counterfeit parts.

The Committee has identified suspect counterfeit electronic parts that entered the U.S. military supply chain. Among those are parts that were sold by an independent distributor in China as new, authentic Xilinx XC3042A-7PG84M programmable gate arrays. The purchaser of the suspect parts reported that they exhibited the following anomalies:

- "Different ceramic body size"
- "Different size of metal tabs"
- "Repainted metal tab (traces of masking, dull gold color, traces of sprayed paint on sides of ceramic body)"
- "Same date code, same lot parts come with different ceramic body shape"
- "Signs of resurfacing"
- "Bent leads"
- "Peeling coating (suspecting that pins were repaired)"
- "Different length of pins (not meeting manufacturer's datasheet min specification)"
- "Nicks and dents on surface of pins, evidence of reshaping/straightening pins"
- "Minor chips on sides of ceramic body"
- "Noticeable major scuffs on a couple of parts on the marking area"
- "Some parts have different color and font written of 'Philippines' on the backside of the part"
- "Noticeable major scuffs on a couple of parts on the marking area"
- "One part is completely missing a lead"
- "Philippines text on back of several parts were off centered from the rest of the date code"

To assist the Committee with its inquiry, please answer the following questions:

1) Does Xilinx sell refurbished XC3042A-7PG84M programmable gate arrays or have an agreement with any third party that would permit them to refurbish and sell XC3042A-7PG84M programmable gate arrays?

2) Did Xilinx use remarking or black-topping in its manufacturing of XC3042A-7PG84M programmable gate arrays?

3) Would Xilinx warranty XC3042A-7PG84M programmable gate arrays that exhibited the anomalies described above?

4) Please describe the short-term and long-term reliability and performance risks, if any exist, of using XC3042A-7PG84M programmable gate arrays with the anomalies described above.

Please provide responsive information by October 27, 2011. Please send your response as an attachment to an email to Ozge_Guzelsu@armed-services.senate.gov and Bryan_Parker@armed-services.senate.gov. If you have any questions or wish to discuss this request, please contact Senate Armed Services Committee majority staff Ozge Guzelsu (202-224-8922) and Bryan Parker (202-224-8265) of the minority staff.

Thank you for your cooperation.

Sincerely,

John McCain
Ranking Member

Carl Levin
Chairman

XILINX.

October 26, 2011

Honorable Carl Levin and Honorable John McCain
United States Senate
Committee on Armed Services
Washington, DC 20510-6050

Dear Senators Levin and McCain:

This letter is in response to your letter dated October 20, 2011 asking us to assist you with your inquiry into the risk that counterfeit electronic parts pose to the military supply chain. Provided below are our answers to your questions.

Question: Does Xilinx sell refurbished XC3042A-7PG84M programmable gate arrays or have an agreement with any third party that would permit them to refurbish and sell XC3042A-7PG84M programmable gate arrays?

Answer: Xilinx does not sell refurbished materials nor do we authorize any third party to refurbish or sell devices that have been refurbished.

Question: Did Xilinx use remarking or black-topping in its manufacturing of XC3042A-7PG84M programmable gate arrays?

Answer: Xilinx did not perform black-topping in its manufacturing of XC3042A-7PG84M but Xilinx did occasionally remark this part type with a manufacturing qualified demark process followed by a remark using qualified black ink. A given part can be remarked as another part as long as it is the same device type and it meets required specifications for speed, power, and temperature grades. The remark process, which enables more effective inventory management, can only be performed by Xilinx or an authorized supply chain partner.

Question: Would Xilinx warranty XC3042A-7PG84M programmable gate arrays that exhibited the anomalies described above?

Answer: Xilinx would not extend warranties to any device that was not purchased directly from Xilinx or an authorized distributor as stated in our standard Terms of Sale. This information is detailed on our public website as follows:

Authorized distributor list: http://www.xilinx.com/company/contact/auth-disti-table.htm
Warranty: http://www.xilinx.com/warranty.htm
Terms of Sale: http://www.xilinx.com/legal.htm#tos

TEL 408.559.7778 FAX 408.559.7114
2100 LOGIC DRIVE SAN JOSE, CA 95124-3400

XILINX.

Question: Please describe the short-term and long-term reliability and performance risks, if any exist, of using XC3042A-7PG84M programmable gate arrays with the anomalies described above.

Answer: Based on the description provided on the subject device, we would consider the devices to be of dubious origin. The devices may have been reclaimed and potentially exposed to excessive heat in order to dismount them from a circuit board. These cases pose a significant reliability risk owing to the potential exposure to excessive solder heat and electro-static discharge (ESD) damage. With respect to ESD, there are many potential damage mechanisms that could have affected the devices. Some of these could be catastrophic; others may create a damage mechanism that is latent for an undetermined amount of time. With the descriptions provided in this letter, we believe that excessive solder heat was likely used in conjunction with mechanical removal techniques. The combination of these events calls into question the integrity of the devices and would have exposed them to potential ESD damage as well. Though the devices may initially function, it would be next to impossible to predict what amount of life is remaining, or what damage may have been caused to the circuitry.

We hope that this information will help you in your inquiry. Should you need any further assistance, please contact me directly; alternatively, your staff can contact Craig Taylor (email: [redacted]@xilinx.com and telephone: [redacted]) from our corporate quality organization.

Sincerely,

Moshe Gavrielov
President and Chief Executive Officer
Xilinx, Inc.

TEL 408.559.7778 FAX 408.559.7114
2100 LOGIC DRIVE SAN JOSE, CA 95124-3400

TAB 31

1635254 *MAR-08-11 06:32 PM*

BOEING PROPRIETARY - DISTRIBUTION LIMITED TO BOEING PERSONNEL ONLY

[redacted] IBA - Boeing Proprietary

Document Number 1635254	**Status:** Open	**Owner:** IBA IDS	

[redacted]

Initiation Date: 23-DEC-2010 11:38	**Response Due:** 22-JAN-11	**Technical Contact :** Jeff Mitroka	**Phone:** [redacted]
Originator: Joann Beihl (339808)	**Site:** MO002 / **Dept:** ZE6	**Mfg POC:** Ed Cashmere	
Title: Suspect Counterfeit, Microcircuit, Xilinx FPGA		**Mfg Name:** Honeywell International Inc.	
Rep: Jeff Mitroka		**Mfg Address:** 111South 34th Street, Phoenix, AZ 85034	
Original Document Nbr:		**Mfg Cage Code:** 97896	

☐ Supplier ☐ In-House ☐ Other

Description of Problem

As is / Should Be Condition:

C-17 subcontractor Honeywell has reported that Xilinx XC4006/XC4006E FPGAs procured from independent brokers Zelcon and Serenity in 2008 are suspect counterfeit parts. Some packages had incorrect die, others had delamination failures, numerous packages were marked with incorrect lot date codes and some were relabeled. Honeywell stated that all of the FPGAs procured from both Serenity and Zelcon showed evidence of having been remarked. Reference attached Honeywell White Paper and Failure Analysis Report for Details and pictures.

The FPGAs are used on the Video Processor Module which is a circuit card assembly in the Honeywell DME-37B. The Distance Measuring Equipment (DME) was engineered at Redmond, WA and manufactured in Malaysia. In March of 2009 DME manufacturing was transferred from Olathe, Kansas to Penang, Malaysia.

Honeywell part number 12051388-0008 (Xilinx XC4006-6PC84I or (XC4006E-4PC84I)) lot date codes considered suspects are:

Serenity
0046
0421
0221

Zelcon
0313
0308 (investigation not complete)

Actions Taken to Prevent Recurrence:

Short term Honeywell will add new processes such as electrical testing and possibly upscreening to their existing processes in place to detect counterfeiting (Reference attached Procedure #SPOC 419 on Honeywell Part Authenticity Testing). Long term is to replace the part with the still OEM procurable Xilinx component XC4010E. Note: Actions are being reviewed and updated so future White Paper revisions will further detail actions to prevent recurrence.

Suggestions / Recommendations:

Please respond back to the C-17 Program if you have used any of these parts, since Boeing wants to capture any other product that might be impacted.

Attachments

White Paper ? Honeywell DME-37B Xilinx Parts Issue ? Boeing Applications ? Rev J dated December 3, 2010

Failure Analysis report # 501331-1 (dated 2 Dec 2010, date code: 0421, Xilinx P/N: XC4006E-4PC84I) from Honeywell on the Xilinx Suspect Parts Issue

Honeywell Part Authenticity Testing Procedure SPOC 419

Modified By: Joann Beihl (339808)	**Date Modified:** 23-DEC-10 12:07

Page 1 of 2

Boeing Proprietary
Distribution Limited to: Authorized Boeing IQDS Users who understand their personal responsibility and accountability for the proper handling of this information in accordance with Procedure PRO-2227 requirements, and non-Boeing Users specifically approved by the IQDS Systems Administrator.

Special Flags			
Current Assignment Information			
Work Message:			
Queue:	IBA IDS	**Assignee:**	**Dept:**

[redacted]

1635254_501331-1_Xilinx_0421_lot.pdf	Joann Beihl (339808)	23-DEC-10 11:48
1635254_DME_Scan001did_12_03_2011_white_paper_rev_J.pdf	Joann Beihl (339808)	23-DEC-10 11:48
1635254_SPOC_419_-_SOW_template.pdf	Joann Beihl (339808)	23-DEC-10 11:49

Boeing Proprietary
Distribution Limited to: Authorized Boeing IQDS Users who understand their personal responsibility and accountability for the proper handling of this information in accordance with Procedure PRO-2227 requirements, and non-Boeing Users specifically approved by the IQDS Systems Administrator.

[Whereupon, at 3:07 p.m., the committee adjourned.]

○