PRESS RELEASE
U.S. Senate Committee on Armed Services
Carl Levin, Chairman
John McCain, Ranking Member
http://armed-services.senate.gov

FOR IMMEDIATE RELEASE
May 21, 2012
Contacts:
Tara Andringa (Levin) 202-228-3685
Brian Rogers (McCain) 202-224-2235

Senate Armed Services Committee Releases Report on Counterfeit Electronic Parts

WASHINGTON -- A Senate Armed Services Committee investigation discovered counterfeit electronic parts from China in the Air Force's largest cargo plane, in assemblies intended for Special Operations helicopters, and in a Navy surveillance plane among 1,800 cases of bogus parts, a committee report released today [pdf] shows.

The year-long investigation launched by Sen. Carl Levin, D-Mich., the committee's chairman, and Ranking Member Sen. John McCain, R-Ariz., found a total number of suspect counterfeit parts involved in those 1,800 cases exceeding 1 million.

"Our report outlines how this flood of counterfeit parts, overwhelmingly from China, threatens national security, the safety of our troops and American jobs," Levin said. "It underscores China's failure to police the blatant market in counterfeit parts – a failure China should rectify."

"Our committee's report makes it abundantly clear that vulnerabilities throughout the defense supply chain allow counterfeit electronic parts to infiltrate critical U.S. military systems, risking our security and the lives of the men and women who protect it," said McCain. "As directed by last year's Defense Authorization bill, the Department of Defense and its contractors must attack this problem more aggressively, particularly since counterfeiters are becoming better at shielding their dangerous fakes from detection."

The investigation's findings point to China as the dominant source of counterfeit electronic parts and the Committee concluded that the Chinese government has failed to take steps to stop counterfeiting operations that are carried out openly in that country. The Chinese government denied visas to Committee staff to travel to mainland China as part of the Committee's investigation.

The Committee's report includes detailed descriptions of how counterfeits are flooding the supply chain, risking the performance and reliability of critical defense systems. In just one example described in the report, the U.S. Air Force says that a single electronic parts supplier, Hong Dark Electronic Trade of Shenzhen, China, supplied approximately 84,000 suspect counterfeit electronic parts into the DOD supply chain. Parts from Hong Dark made it into

Traffic Alert and Collision Avoidance Systems (TCAS) intended for the C-5AMP, C-12, and the Global Hawk. In addition, parts from Hong Dark made it into assemblies intended for the P-3, the Special Operations Force A/MH-6M, and other military equipment, like the Excalibur (an extended range artillery projectile), the Navy Integrated Submarine Imaging System, and the Army Stryker Mobile Gun.

While the investigation focused on the risk that counterfeit parts pose to U.S. national security and the safety of military personnel, the rampant theft of U.S. intellectual property also severely impacts the U.S. economic security. According to the Semiconductor Industry Association (SIA), counterfeits cost U.S. semiconductor companies more than $7.5 billion annually in lost revenue, a figure SIA says results in the loss of nearly 11,000 American jobs.

In November 2012, the Committee held a hearing on the investigation's preliminary findings. Following that hearing, Committee Chairman Carl Levin and Ranking Member John McCain offered an amendment to the FY 2012 National Defense Authorization Act to address weaknesses in the defense supply chain and to promote the adoption of aggressive counterfeit avoidance practices by DOD and the defense industry. The amendment was adopted in the Senate and a revised version was included in the final bill signed by President Barack Obama on December 31, 2011.

ARMED SERVICES COMMITTEE CONCLUSIONS

Source of Counterfeit Parts

Conclusion 1: ***China is the dominant source country for counterfeit electronic parts that are infiltrating the defense supply chain.*** The U.S. Trade Representative (USTR) has said that China's global manufacturing capacity "extends to all phases of the production and global distribution of counterfeit goods." The Committee's investigation uncovered overwhelming evidence that that is the case with electronic parts infiltrating the defense supply chain. The Committee tracked well over 100 cases of suspect counterfeit parts back through the supply chain. China was found to be the source country for suspect counterfeit parts in an overwhelming majority of those cases, with more than 70 percent of the suspect parts traced to that country. The next two largest source countries were the United Kingdom and Canada. The Committee identified instances in which both countries served as resale points for suspect counterfeit electronic parts from China.

Conclusion 2: ***The Chinese government has failed to take steps to stop counterfeiting operations that are carried out openly in that country.*** One Committee witness described visiting China and seeing public sidewalks covered with electronic components that had been harvested from e-waste. Another witness said he saw whole factories in China of 10,000 to 15,000 people set up for the purpose of counterfeiting. Counterfeit electronic parts are sold openly in public markets in China. Rather than acknowledging the problem and moving aggressively to shut down counterfeiters, the Chinese government has tried to avoid scrutiny, including denying visas to Committee staff to travel to mainland China as part of the Committee's investigation.

Department of Defense Actions on Counterfeits

Conclusion 3: ***The Department of Defense lacks knowledge of the scope and impact of counterfeit parts on critical defense systems.*** In a March 2010 report, the Government Accountability Office stated that "DOD is limited in its ability to determine the extent to which counterfeit parts exist in its supply chain." The Committee's findings support that statement. Reporting into the Government-Industry Data Exchange (GIDEP) program, which would allow DOD to track instances of counterfeit parts, is woefully lacking. During the period reviewed by the Committee, the Defense Logistics Agency (DLA), which is responsible for supplying DOD with most of its spare parts, neither consistently reported to GIDEP nor maintained a list of instances in which they had been supplied counterfeit electronic parts. And, in each of the three cases that the Committee investigated in depth, DOD was unaware that counterfeit electronic parts had been installed on certain defense systems until the Committee's investigation.

Conclusion 4: ***The use of counterfeit electronic parts in defense systems can compromise performance and reliability, risk national security, and endanger the safety of military personnel.*** The investigation uncovered dozens of examples of suspect counterfeit electronic parts in critical military systems, including 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 a large number of military airplanes. The potential impact of suspect parts on the performance and reliability of defense systems is significant. For example, according to MDA, if suspect counterfeit devices installed on the THAAD mission computers had failed, the THAAD missile itself would likely have failed. According to the Navy, had counterfeit parts contained in electromagnetic interference filters failed on an SH-60B helicopter, the aircraft's ability to conduct night missions and surface warfare missions involving hellfire missiles would have been compromised.

Conclusion 5: ***Permitting contractors to recover costs incurred as a result of their own failure to detect counterfeit electronic parts does not encourage the adoption of aggressive counterfeit avoidance and detection programs.*** Taxpayers should not be burdened with covering the costs of a contractor's failure to detect counterfeit electronic parts in their own supply chain. Moreover, government contracts that permit cost recovery in such circumstances contrast with agreements that some contractors enter into with their own suppliers. Raytheon's General Terms and Conditions relating to nonconforming material states that the "[c]ost of repair, rework, replacement, inspection, transportation, repackaging, and/or reinspection by Buyer shall be at Seller's expense." Similarly, BAE's General Provisions state that, in cases where a supplier delivers non-conforming work, BAE may "make, or have a third party make all repairs, modifications, or replacements necessary to enable work to comply in all respects with Contract requirements and charge the cost incurred to the SELLER."

Defense Industry

Conclusion 6: ***The defense industry's reliance on unvetted independent distributors to supply electronic parts for critical military applications results in unacceptable risks to national security and the safety of U.S. military personnel.*** The Committee identified approximately 1,800 cases of suspect counterfeit parts in the defense supply chain. Those parts were supplied by more than 650 companies, each of which relied on their own network of suppliers. DOD and defense contractors are frequently unaware of the ultimate source of electronic parts used in defense systems. The suspect counterfeit parts that were used in Electromagnetic Interference Filters (EIF) destined for the Navy's SH-60B helicopters, for example, changed hands five times before the parts were bought by the Raytheon subcontractor who built the EIFs. Those parts

originated with Huajie Electronics in Shenzhen, China, a fact that neither DOD nor Raytheon was aware of prior to the Committee's investigation.

Conclusion 7: ***Weaknesses in the testing regime for electronic parts create vulnerabilities that are exploited by counterfeiters***. The Committee reviewed test reports associated with the approximately 1,800 cases of suspect counterfeit parts identified in the investigation. Those reports reveal wide disparities in testing used by companies in the defense supply chain. Some companies require a range of testing, for example, exposing a part to aggressive solvents to determine whether markings are authentic or delidding part samples to examine their die. Other companies, however, are willing to accept parts that have only been subject to basic functional testing. The investigation also revealed deficiencies in the process used to determine whether and how parts are tested. For example, in the case of the counterfeit memory chips sold to L-3 Communications, the supplier in China selected and sent L-3 Communications' U.S.-based distributor a sample of 18 parts to test. Once those parts were tested and validated as authentic, the China-based supplier sold the company more than ten thousand of the chips. L-3's process at the time allowed the company to accept those chips without additional testing from an independent laboratory.

Conclusion 8: ***The defense industry routinely failed to report cases of suspect counterfeit parts, putting the integrity of the defense supply chain at risk.*** The vast majority of the approximately 1,800 cases of suspect counterfeit parts identified in the investigation appear to have gone unreported to DOD or criminal authorities. For example, in the case of the suspect counterfeit part contained in the Navy's P-8A airplane, Boeing failed to notify the Navy of the problem until the Committee began inquiring about the suspect counterfeits. Similarly, in the case of the suspect counterfeit memory chip contained in the C-27J, L-3 Communications did not notify the Air Force until the day before Committee staff was scheduled to meet with the Air Force program office responsible for that aircraft. Many cases also go unreported to the Government-Industry Data Exchange Program (GIDEP), a DOD program where government and industry participants can file reports about suspect counterfeits. While one industry witness told the Committee that sharing information on counterfeit parts through GIDEP "can help stop suppliers of counterfeit parts in their tracks," only 271 total reports were submitted to GIDEP during all of 2009 and 2010.

.