

Electronic Waste Rules Could Help Thwart Flow of Counterfeit Parts

February 2015

By Jim Burger, Henry Livingston and Tom Sharpe



As highlighted in a report by the U.S. Senate Armed Services Committee, a flood of counterfeit electronic parts from China threatens the reliability of sophisticated defense technologies from thermal weapon sights to advanced missile systems and from aircraft to submarines.

The committee found more than 1,800 cases of counterfeit parts in defense systems. But like the proverbial tip of the iceberg, what we can see is only a small part of the problem.

From our respective vantage points in the defense and computer industries, we have observed that the problem has continued to grow in recent years. While the federal government and the defense industry are implementing prevention and detection measures, additional action is needed by Congress.

Counterfeits threaten reliability because advanced defense systems require sensitive electronic components manufactured in ultra-clean environments. Employees must wear “bunny suits” to prevent skin or hair being shed into the environment because even a small flake of dandruff can ruin a microchip and potentially compromise the performance of the hardware it drives. Moreover, legitimate semiconductor companies subject all of their chips to electronic testing to ensure they perform properly. Military chips are subject to additional environmental testing.

By contrast, counterfeiters re-process used electronic components pulled from e-waste — the source of their feedstock. As the Armed Services Committee report found, “much of the material used to make counterfeit electronic parts is electronic waste, or e-waste, shipped from the United States and the rest of the world to China.”

The used parts are subjected to harsh re-processing practices that add to the performance risks before they are re-sold as “new.” E-waste is shipped by boat across the Pacific Ocean, smuggled into China and trucked to Guangdong Province, the epicenter of counterfeiting activities. There, workers pull apart the e-waste by hand, often in backyards and dump sites. The e-waste is often heated over open fires to loosen electronic components so they are easier to remove from the circuit boards to which they are soldered. Because e-waste contains toxins, these processes create serious health and environmental hazards for the workers and the community at large.

The parts are then dumped on sidewalks for sorting. The process is messy, so the components are washed in a river

or left outside in the rain.

After drying in the open air, the parts are shipped to larger facilities that are set up for counterfeiting. The parts may be sanded or put through an acid wash to remove part numbers, then re-coated in a process known as "blacktopping" to hide identifying product information. Because chips are sensitive to moisture and static electricity incurred from improper handling, packaging and storage, the counterfeit process threatens already unreliable used components. In addition, the acid eventually eats away at a microchip's internal parts.

Obviously, microchips handled in this way will be prone to failure — sooner rather than later. Yet even to a trained eye, the chips look factory fresh. These counterfeit parts are represented as "new" by the counterfeiters and sold to U.S. companies that are unaware of their origins and incorporate the counterfeit parts into their products.

While national security is a primary concern, these counterfeits also find their way into technologies across a wide range of industries, including telecommunications, health care, air travel and nuclear power. One might also find counterfeits in items you rely on every day, such as your alarm clock and your home PC as well as your car's airbags and automatic braking systems.

This raises the critical question: What can we do to stop this flow?

The federal government and the defense industry are enacting new policies and practices that prevent the introduction of such components into supply chains and detect them should they slip through. While prevention and detection measures are important, we believe we must also choke off the counterfeiters' feedstock: e-waste exports.

Legislation that promotes responsible electronics recycling would be a major step in halting the flow of e-waste from the United States that undermines our national security. Such legislation would require domestic recycling of all untested, nonworking electronics. By keeping these materials in the United States, we will keep them out of the hands of counterfeiters.

There is a strong network of responsible recyclers already established in the United States that is capable of scaling up to meet the additional demand. By recycling these materials responsibly on American soil, we can also reduce the global environmental impacts caused by exports to developing countries that lack appropriate safeguards. These dangers can easily be contained within the controlled processes already in place at many U.S. e-scrap processing sites.

Because of its national security implications, legislation promoting responsible electronics recycling has attracted bipartisan support in this session of Congress. The Congressional co-sponsors include chairs of committees and subcommittees related to intelligence, homeland security, rare earths and other relevant issues who recognize the national security threat posed by counterfeits.

By allowing an unchecked flow of e-waste exports, the United States is contributing to the feedstock used to create counterfeit electronic parts that can find their way into the DoD supply chain and can also present a public health and safety risk. Congress must go on the offensive against counterfeiters by enacting a comprehensive policy on e-waste exports. ND

Henry Livingston is a technical director and Engineering Fellow at BAE Systems, a global defense, security and aerospace company. Tom Sharpe is vice president at SMT Corp., an electronics distributor to the defense and aerospace industries and counterfeit mitigation laboratory. Jim Burger, a partner at the law firm Thompson Coburn LLC, is an advisor to the computer industry.

Photo Credit: Thinkstock