Counterfeits Can Kill U.S. Troops. So Why Isn't Congress and DoD Doing More to Stop it?

By Jim Burger and Kimberly Heifetz

Sometime in the not-to-distant future, a submarine will sink. An air defense missile will detonate far from its intended target. A Seahawk helicopter will intercept a suicide speed boat headed for an aircraft carrier only to see its infrared targeting system goes dark.

These chilling scenarios won't be the result of human error or terrorist plots: They will directly result from a $2 counterfeit electronic tucked deep within a billion-dollar military technology.

It's not a matter of if, but when. Just last month, the Department of Justice indicted a Massachusetts man for selling counterfeit semiconductors to Navy contractors. Some of the fake parts were intended for nuclear submarines.

The vast majority of counterfeits discovered in military equipment are semiconductors, the stamp-sized silicon wafers that act as the "brains" of nearly every type of modern electronic system. The U.S. military is a huge consumer of these tiny products; a single F-35 Joint Strike Fighter jet is controlled by more than 2,500 semiconductors.

That huge military demand has fueled a rampant — and quite sophisticated — counterfeit network that spans the globe. It starts in China and ends in the weapons systems and aircraft used by our service personnel every day. Congress and the Administration have known about this threat for years, but have not done enough to stop counterfeit electronics from entering the country and ending up in critical military systems.

The Treasury Department has hindered the ability of Customs and Border Protection officers to seize counterfeit semiconductors at the border. At the same time, the Defense Department has proposed band-aid rules to prevent counterfeits from being incorporated into military systems.

Counterfeits semiconductors are generally not manufactured. Instead, laborers in foreign markets, chiefly in China's Guangdong Province, "recycle" millions of tons of e-waste. In their backyards, workers separate boards from used tech products, "cook" the boards over a fire, then slam them to remove the chips. Foreign intermediaries buy the chips and use lasers to etch fake trademarks, part numbers and production codes onto the surface before selling them to unscrupulous U.S importers and brokers.

Statistics about the widespread infiltration of counterfeits are frightening. A 2012 Senate Armed Services Committee investigation report uncovered 1,800 cases of suspect counterfeit electronic parts in the defense supply chain, with the total number of suspect parts exceeding one million. A senior Naval Air Systems official estimated "that as many as 15 percent of all spare and replacement microchips the Pentagon buys are counterfeit."

These counterfeits have been found in all kinds of critical military systems, including helicopter forward-looking infrared, F-16 hostile tracking radar, portable nuclear identification tools, and aircraft pilot display units.

The good news is that the threat of counterfeits can be drastically reduced by effective border enforcement. Customs officers would routinely take digital photographs of detained suspect semiconductors. They sent the pictures to manufacturers whose names appeared on the chips to see if they are real or fake. This streamlined process worked without a single complaint until 2008, when the Treasury Department abruptly ordered Customs agents to redact all numbers when sending the digital snapshots to manufacturers, hobbling a system that had proved remarkably effective in seizing counterfeits. Treasury made this change to protect "gray market goods," lower-priced items legitimately sold overseas but that often end up back in the U.S. supply chain in breach of the foreign distributor's license with the U.S. manufacturer.

To remedy this problem, Congress enacted Section 818 of the 2012 National Defense Authorization Act. Unfortunately, instead of requiring that Customs agents disclose the codes to manufacturers, the legislation only gave Treasury "permission" to do so, stripping the measure of its teeth. Following the passage of the law, Customs wrote to manufacturers saying: "While the NDAA authorizes sharing of unredacted samples, it is consistent with current regulations which do not permit sharing of unredacted samples prior to seizure." Yet when pushed to demonstrate which "current regulations" forbid pre-seizure disclosures, Customs couldn't provide an answer.

A later regulation, issued in April 2012, essentially allows criminal importers to verify the authenticity of their own shipments, which they are more than happy to do using fake certificates of authenticity. After all, what's a perjury charge compared to the felony they face for selling counterfeits to the government? The rule also adds a significant burden to already overtaxed Customs officers. Disclosures and seizures of semiconductors fell dramatically in the first eight months after the rule was enacted.

Reps. Ted Poe (R-Texas) and Zoe Lofgren (D-Calif.) have introduced H.R. 22, which would require Customs officers to immediately disclose to manufacturers unredacted photographs of suspect aircraft or automotive parts, or semiconductors. This bipartisan bill, co-sponsored by 17 Representatives (including the chairmen of the House Armed Services and Homeland Security Committees), has been referred to the House Judiciary Committee.

The counterfeit threat looms so large that the executive branch is also scrambling for solutions. The Defense Department is poised to alter its federal acquisition regulations to directly target counterfeit electronics. But the agency's proposed rule, announced in May, is riddled with ambiguities and loopholes. Part of the problem is that DoD created a proposed rule full of terms that don't line up with the Congress' language in Section 818. The DoD rule is intended to kick-start the implementation of Section 818, but that's going to be nearly impossible if the two measures are incongruous in their approach to a number of basic terms and concepts.

For example, the DoD rule defines a "counterfeit part" as an item that has been altered by a someone other than a "legally authorized source." The term "legally authorized source" — which doesn't appear anywhere in Section 818 — is defined as either the original manufacturer of the item (plus its authorized suppliers) or "current design activity."

A number of industries are struggling with that second term, "current design activity." Some have no clue what it means. Others have ventured guesses based on the only other place the term appears — a 71-page manual governing DoD labeling standards for military products. But even then, it's just an educated guess.

Leaving such a critical term open to interpretation creates vulnerabilities. Without a definition, all segments of the military

supply chain will be forced to come up with their interpretations. That kind of uncertainty will not only allow the continued entry of counterfeit parts into DoD's supply chain — it will guarantee it.

A better definition of "legally authorized source" would be "the original manufacturer and authorized distributors, authorized resellers, and authorized aftermarket distributors and manufacturers, that the original manufacturer authorizes to produce an item through distribution, resale or manufacture (current design activity). All other sources are non-authorized."

But what if a contractor needs a part that is not available from an original manufacturer or its authorized distributers? In those instances, the proposed rule says a contractor may purchase a part from a "trusted supplier." But that term, too, is undefined. How should DoD vet distributers before qualifying them as "trusted suppliers"? What do these companies need to do to disclose about the parentage of a semiconductor to prove it's not a counterfeit? These questions still need to be answered.

Also, DoD's rule only applies to contractors and subcontractors covered by the federal government's Cost Accounting Standards, a set of rules for procurements in excess of $700,000. Many counterfeit electronic parts enter the military supply chain through small companies that would not be covered by this rule. In fact, at a June public hearing on the proposed rule, one government attendee noted that the rule would only cover roughly 10 to 15 percent of its contractors. That figure is unacceptable. Every contractor and subcontractor that supplies parts that end up in military devices should obey the rules. For that reason, the rule should apply to all tiers of military contractors and subcontractors.

It's not too late to create strong, effective barriers to the swell of counterfeit electronics currently flooding the military supply chain. First, Congress should pass H.R. 22. This simple legislative fix will stop counterfeit semiconductors before they even come near our military systems.

Second, before moving forward on any rulemaking, DoD needs to issue another proposed rule regarding counterfeit electronics. In its current form, the rule simply doesn't work. But it's still possible to craft a regulation that will allow all tiers of the military supply chain to detect and avoid counterfeit parts. Semiconductor companies, industry groups and universities can help enormously in this process. Like the government, they want nothing more than to ensure our military is working every day with the best equipment possible.

***Jim Burger** is a partner at Thompson Coburn LLP. He has represented semiconductor companies before Congress, the White House and the Homeland Security, Defense and Treasury departments on the anti-counterfeiting issue. He and Kimberly Heifetz prepared comments for the semiconductor industry in recent rulemaking asking DoD to more aggressively respond to counterfeits in the military supply chain. Jim is also Vice Chair of the Intellectual Property Owners Association's Anti-Counterfeiting and Anti-Piracy Committee. He has helped IPO draft comments to the Pentagon on preventing counterfeits in DoD procurement. Jim has also spoken directly to military leaders about the dangers of counterfeit parts, including a recent speech before the Naval Sea Systems Command.*

***Kimberly Heifetz** is counsel at Thompson Coburn LLP and former in-house counsel for BAE. She has extensive experience analyzing federal regulations on behalf of clients who contract with the government or who support government contractors. Her understanding of the proposed counterfeit parts regulations stems from years of working with government-wide regulations, including those unique to Department of Defense agencies.*