New Rule Addresses Supply Chain Assurance

Companies in the defense supply chain know well the threat of counterfeit parts. Clark Silcox wrote about this threat in his June National Defense article, "New Strategies to Combat Counterfeit Parts," and outlined two strategies for averting the hazard of such items.

The first strategy focuses on the source of the supply — principally China — and presents methods for increasing anti-counterfeit enforcement. Silcox's second strategy focuses on curtailing demand for counterfeits by improving industry efforts to assure receipt of authentic articles.

There are some new rules on counterfeit parts that defense contractors must now abide. Last November, the Defense Department issued an interim rule that empowers it to exclude sources deemed to represent "the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert a system."

The interim rule specifically focuses on counterfeits that harbor malicious code that could enable a cyber attack. When national intelligence agencies detect an "attack vector" capable of being exploited, the new rules empower the department to exclude a supplier without informing the company planning to use its part.

Every producer of sensitive defense equipment is cautioned to carefully scrutinize its supply chain. While Chinese-sourced parts should receive special scrutiny, especially if a supplier's ownership is connected to the People's Liberation Army, contractors should confirm the identity of whoever owns or controls key suppliers for mission critical items obtained from any location. For such trusted systems, the department expects that its contractors will be able to establish the provenance of key parts, to allay concern of interception or manipulation.

The notice and comment period for this interim rule has ended and a final rule is expected soon.

In May, the Defense Department issued a final Defense Acquisition Regulation System rule on counterfeit electronic parts. It implements, in part, Section 818 of the fiscal year 2012 National Defense Authorization Act, which was passed into law shortly after extensive hearings by the Senate Armed Services Committee that revealed the defense industry's failure to adequately self-protect against counterfeit electronics and report counterfeit incidents.

The rule applies directly only to about 1,200 government contractors that are governed by the cost accounting standards in whole or in part. These covered contractors, applying 12 criteria, must establish and document compliant systems to detect and avoid counterfeit electronic parts.

These criteria include: the use of trusted suppliers, preferably the original source of a component or an authorized distributor; improving traceability of parts back to the original manufacturer; additional inspection and testing of parts using risk-based assessment methods; and new obligations with regards to reporting and quarantining parts, so that counterfeits do not re-enter the supply chain.

Additionally, as part of the contractor purchasing system review, the government will evaluate the adequacy of the system. For covered contractors, the new rules present challenging implementation issues, in part because of the incomplete or ambiguous nature of the rules themselves, as well as the great diversity of contractor facts and circumstances. Nonetheless, the new rules are in effect and are appearing through new contract clauses in solicitations. The Defense Contract Management Agency has the principal responsibility for oversight and administration.

While they directly apply only to large defense contractors, the new rules also impact many smaller suppliers. Covered contractors are obligated to flow down the requirements to "all levels in the supply chain" without exception, and therefore to all suppliers, regardless of size and regardless of whether the part is commercial or commercial, off-the-shelf. The mandatory flow-down presents a very difficult implementation issue because commercial and COTS sources are unlikely to accept all the requirements and potential liabilities — particularly for parts where defense uses or customers represent only a tiny fraction of sales. Many smaller companies that sell to the Defense Department will also object to the full range of the requirements as either impracticable or too costly.

The department recognizes this problem. At a public forum in mid-June, a defense official confirmed that the department was working on a new and even broader regulation to cover all 13,000 companies that sell to it. This new rule also would extend beyond electronic parts to include other forms of counterfeit material and mechanical parts. Another rulemaking action would expand reporting requirements as to nonconformities of "common items" that have multiple applications.

Notably, large contractors are working to improve their existing anti-counterfeit practices, but smaller contractors, COTS vendors, and commercial sources are not legally obligated to accept the flow-down or to agree to all of the new requirements. Such obligations arise solely as a matter of contract, and only to the extent a flow-down is accepted. Some companies will decline the flow-down as neither feasible nor prudent, while others will accept only some of the obligations. This does not mean they cannot sell to the Defense Department or to "covered contractors."

Responsible companies should evaluate the new rules, conduct a risk-based assessment of their supply chain, consider the consequences to their customers should a counterfeit escape occur, adopt improved practices to control sources of supply and respond to new demands for inspection, testing, training and reporting.

Prudent suppliers not directly subject to the new regulations will ensure they are able to demonstrate the adequacy and viability of their tailored counterfeit prevention systems, and document their systems to assure parts' authenticity.

Higher tier companies, where covered by the new regulations, will seek complete flow-down. But they cannot compel acceptance of the flow-down. It is expected that "covered contractors" and the department will recognize that business must continue with the necessary sources of supply that decline the full flow-down. Both purchasers and suppliers will need to act responsibly to implement effective surrogates to avoid counterfeits.

The Defense Department recognizes that its supply chain is enormous in breadth and depth and that it must proceed carefully with administration and enforcement of the new rules. Simultaneously, companies that intend to remain in the defense supply chain must take prudent proactive measures to adopt and improve systems to detect and avoid counterfeits.

Robert S. Metzger, a law partner with the Washington, D.C., office of Rogers, Joseph O'Donnell, P.C., and vice chair of the supply chain assurance subcommittee of TechAmerica, has written extensively on supply chain assurance and related cyber security matters.