THE GOVERNMENT CONTRACTOR®

WEST®

Information and Analysis on Legal Aspects of Procurement

Vol. 54, No. 23 **June 20, 2012**

Focus

¶ 189

FEATURE COMMENT: Preparing For New Rules To Combat Counterfeit Parts

Many defense electronic contractors will face yet another challenge in this year of shrinking federal defense budgets. On Dec. 31, 2011, President Obama signed into law the National Defense Authorization Act for Fiscal Year 2012 (NDAA). P.L. 112-81, 125 Stat. 1298 (2011). Section 818 of the NDAA focuses on detection and avoidance of counterfeit electronic parts in the defense supply chain. It imposes new obligations on the Department of Defense and the private sector, onto which it shifts much of the responsibility to detect counterfeit parts. The full scope of these obligations will become clear by September 26, the date by which the secretary of defense must issue new anti-counterfeit regulations.

Although the new regulations are still several months away, the NDAA identifies a variety of requirements that contractors may have difficulty meeting without advance planning. For instance, new sourcing and traceability requirements may necessitate fundamental changes in the way some contractors design products and procure parts. Further, § 818's reporting safe-harbor provisions will protect only contractors that have reasonable quality procedures in place to identify counterfeit or suspect counterfeit electronic parts. Assessing your company's existing anti-counterfeit procedures before the issuance of the new regulations will better prepare you to comply with the new anti-counterfeit requirements.

Understanding the Risk: Counterfeit Parts in the Defense Supply Chain—Counterfeit parts in the defense supply chain are a persistent and growing issue. "Almost anything is at risk of being counterfeited including fasteners used on aircraft, electronics used on missile guidance systems, and materials used in body armor and engine mounts." Government Accountability Office report, *Defense Supplier Base: DOD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Counterfeit Parts* (GAO-10-389), available at *www.gao.gov/new.items/d10389.pdf*.

The term counterfeit generally refers to goods for which the origin or pedigree is misrepresented. Counterfeit includes bogus parts—that is, parts manufactured by one manufacturer that uses the name or trademark of another without authorization. Counterfeit parts under the NDAA also include genuine parts that have been recycled, but are offered as new. See NDAA § 818(b)(1) (requiring DOD to establish definitions for "counterfeit electronic part" and "suspect counterfeit electronic part" to include used parts misrepresented as new); SAE International, "SAE Aerospace Standard 5553, Counterfeit Parts; Avoidance, Detection, Mitigation and Disposition" (April 2009) (setting forth definition of counterfeit used in aerospace industry and endorsed by DOD in 2009). Suspect counterfeit parts are parts believed to be counterfeit, although a determination is not yet confirmed.

The problem of counterfeit parts in the defense supply chain is driven by obsolescence—the scarcity or unavailability of parts from original equipment manufacturers (OEMs) or their authorized dealers as defense systems age and, in many cases, are employed far beyond their anticipated life span. The issue is particularly acute for electronic parts, for which Government purchases account for only a small portion of the market, and the rapid turnover in technology drives OEMs to shift production to next generation parts at a seemingly ever-increasing pace. Contractors, which often need older parts to deliver or repair systems for existing platforms, frequently cannot obtain the parts directly from the OEM or its authorized dealers, and must purchase the parts

from independent distributors or brokers, leaving the contractors vulnerable to purchasing bogus or reworked parts.

In the defense supply chain, much of the attention to date has focused on counterfeit electronic parts, although the problem is much broader. Incidents of counterfeit parts more than doubled from approximately 3,868 in 2005, to 9,356 in 2008. See Department of Commerce, Defense Industrial Base Assessment: Counterfeit Electronics i–ii (2010). In 2011, the Senate Armed Service Committee investigated counterfeit electronic parts in the defense supply chain and found more than one million incidents of suspect counterfeit parts. See Committee on Armed Services, United States Senate, 112th Cong., Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain (May 12, 2012).

The demand for obsolete electronics is only part of the explanation for this increase. Counterfeiters also have found relative safe havens in certain countries, providing stability to an iniquitous industry. Consequently, counterfeiters have become more sophisticated in their trade, investing in better equipment and producing better fakes. A contractor that receives a counterfeit part may not question its origins if the part bears an authentic OEM name and part number, arrives with documentation of authentication, and passes inspection and testing.

Most counterfeit goods found in the U.S. come from China, and counterfeit electronic parts in the defense supply chain are no exception. Given the multi-billion-dollar size of the counterfeit parts market, the profits to be made from counterfeiting, and the absence of any significant deterrent, a decrease in counterfeit electronic parts is unlikely.

New Requirements for Contractors: § 818 Requirements—On Nov. 17, 2011, Sens. Carl Levin (D-Mich.) and John McCain (R-Ariz.) proposed an amendment to the NDAA "to bolster the detection and avoidance of counterfeit electronic parts." S. 1867, Amendment No. 1092, 112th Cong. (2011). The amendment, enacted as § 818, both imposes new requirements on DOD and the Department of Homeland Security, and requires DOD to impose new requirements on defense contractors that supply products or weapon systems with electronic components. The requirements include new counterfeit part prevention, detection and mitigation obligations. Failure to adhere to these requirements may have significant consequences such as increased costs, suspension, debarment, and even civil and criminal liability.

New DOD Requirements: DOD must assess its acquisition policies and systems for the detection and avoidance of counterfeit electronic parts. DOD must establish by June 28 department-wide definitions for "counterfeit electronic part" and "suspect counterfeit electronic part." NDAA § 818(a), (b)(1). As of the date of publication of this article, DOD has yet to issue proposed or final definitions. Further, DOD must issue internal guidance to minimize the incidence and risk of counterfeit electronic parts. Id. § 818(b)(2)–(5). The internal guidance must address, among other things, remedial actions to be taken against contractors that repeatedly fail to detect or avoid counterfeit parts, or that have "otherwise failed to exercise due diligence in the detection and avoidance of such parts." Id. § 818(b)(3).

New Homeland Security Requirements: DHS, in consultation with DOD, must establish an enhanced inspection program for parts imported into the U.S. Id. § 818(d).

New Contractor Requirements: Of most importance to contractors, the legislation requires that, no later than September 26, DOD revise the Defense Federal Acquisition Regulation Supplement to address the detection and avoidance of counterfeit electronic parts. Id. § 818(c)(1). The new DFARS regulations will place responsibility for detecting and avoiding counterfeit parts on contractors, and, where counterfeit parts are used, will assign remedial costs to contractors without allowing for recovery under DOD contracts. As discussed below, contractors should begin formulating internal policies and procedures to ensure that they are ready to comply with the forthcoming regulations.

- Covered contractors, which are subject to the Cost Accounting Standards under § 26 of the Office of Federal Procurement Policy Act, 41 USCA § 422, and supply electronic parts or products that include electronic parts, will now be responsible for not only detecting and avoiding counterfeit and suspect counterfeit parts, but also for any rework or corrective action necessary to remedy the inclusion of such parts. The regulations will make the cost of any such rework or corrective action unallowable. Id. § 818(c)(2).
- Contractors at all tiers will be required, whenever possible, to procure parts from the original

component manufacturers (OCMs) or their authorized dealers, or from trusted suppliers that obtain such parts exclusively from the OCMs or their authorized dealers. If electronic parts are no longer in production nor available in stock, contractors can purchase from "trusted suppliers." Notably, § 818 does not define "trusted suppliers." DOD is to establish qualification requirements pursuant to which it may identify trusted suppliers and authorize contractors and subcontractors to identify and use additional trusted suppliers under certain circumstances set forth in the legislation. Id. § 818(c)(3) (stating that the trusted-supplier qualification requirements are to be consistent with 10 USCA § 2319, which sets forth procedures for establishing qualification requirements in DOD procurements).

- The new regulations will impose certain reporting requirements. Contractors will need to notify DOD, and inspect, test and authenticate parts obtained from any source other than the OCM, authorized supplier or trusted supplier. If contractors become aware or have reason to suspect that counterfeit parts have entered the supply chain, they must file a report within 60 days to both the appropriate Government authorities and the Government-Industry Data Exchange Program (GIDEP). Id. § 818(c)(4).
- Section 818 creates a "safe harbor" from civil liability for reporting if the contractor has made a reasonable effort to determine whether the component at issue contained counterfeit or suspect counterfeit parts. Id. § 818(c)(5).
- Section 818 requires DOD to implement a program to "enhance contractor detection and avoidance of counterfeit electronic parts." Under this program, contractors will be required to adopt internal policies and procedures "to *eliminate* counterfeit electronic parts from the defense supply chain" (emphasis added). The legislation then lists the various areas that these internal systems should address, such as the training of personnel, inspection, traceability and testing of parts, use of trusted suppliers, reporting and quarantining of counterfeit parts, implementation of systems to detect and avoid counterfeit parts, and the flowdown of counterfeit avoidance and detection requirements to subcontractors. DOD must establish processes for the review and approval of contractor systems, which will be comparable to the processes now used for contractor business systems. Id. § 818(e).

New Criminal Liability: Finally, the legislation amends 18 USCA § 2320 to add criminal liability for intentionally trafficking in counterfeit goods or services, knowing that such a good or service is for military use and is likely to cause injury or death, disclosure of classified information, impairment of combat operations, or other significant harm to a combat operation, a member of the Armed Forces or national security. Penalties include fines of up to $5 million for individuals and $15 million for persons other than individuals, and 20 years imprisonment. Id. § 818(h).

Preparing for the New Requirements—Defense contractors can and should begin preparing for the new requirements. They will need lead time to, at the very least, assess existing systems and identify gaps. Moreover, proposed amendments to the NDAA may provide an exception to the cost-shifting provisions if a contractor has "an operational system to detect and avoid counterfeit parts and suspect counterfeit electronic parts that has been reviewed and approved by the Department of Defense." FY 2013 NDAA, H.R. 4310, 112th Cong. § 816 (2012).

For those contractors that do not have an existing counterfeit mitigation plan, there are many roadmaps in the existing literature, although policies and systems should be specific to each company and its particular issues and risks. See, e.g., SAE International, "Aerospace Standard 5553, Counterfeit Parts; Avoidance, Detection, Mitigation and Disposition" (April 2009). Designing a company-specific plan will require a review of internal systems to identify areas of risk. The plan should address procurement processes, inspection and testing procedures, mitigation procedures in the event a counterfeit part enters the supply chain, reporting systems, and training.

In preparing for the new requirements, contractors should consider not only the best practices in the defense industry, but also those from other industries with similar issues and risks. The below list sets out some of the steps that defense contractors should consider before the new requirements take effect.

- Establish a supplier plan for all departments purchasing electronic parts. The requirements in § 818 provide the foundation for such a plan. Section 818 requires that, whenever possible,

contractors should purchase parts from the OEM, its authorized dealer, or a trusted supplier that purchases from the OEM or authorized dealer. If a part is not available from these sources, contractors may purchase from another trusted supplier. If even that is not possible, contractors may purchase from another supplier, but must notify DOD and inspect, test and authenticate the electronic part.

- Determine best practices for inspecting, testing and authenticating the particular parts used in the relevant industry. Assess the company's current testing methods for any gaps compared to best practices and counterfeiting practices. Reassess testing methods on a periodic basis, as counterfeiters will revise their methods to avoid existing tests. In addition, contractors should assess the capabilities and availability of outside firms to conduct testing, as needed.
- Assess and begin to plan for long-term parts requirements. Contractors facing unavailability of parts from trusted sources may need significant lead time to redesign a system or find an aftermarket manufacturer. Product life-cycle management software can assist with this.
- Establish a plan for quarantining and destroying suspect and counterfeit parts. Contractors should not return counterfeit parts to the supplier because the supplier may reintroduce the parts into the supply chain.
- Establish internal reporting requirements for suspect and counterfeit parts that include reporting to GIDEP. The regulations under the NDAA will require reporting to GIDEP and to other Government authorities (to be determined by regulation).
- Train key employees on up-to-date information on counterfeit avoidance, detection and reporting.
- Review anti-counterfeiting requirements of existing subcontract and supplier agreements for adequacy, and monitor developments in this area. DOD recently directed its components to identify appropriate industry standards for anti-counterfeiting and include those standards in contracting requirements, with flowdown to appropriate lower-tier subcontracts. See Memorandum from the Under Secretary of Defense, Dep't of Defense, to Secretaries of the Military Departments Directors of the Defense Agencies, Overarching DoD Counterfeit Prevention Guidance (March 16, 2012).
- Join industry groups to share information on counterfeit parts and best practices and to advocate for workable solutions. In a recent report by the House Committee on Armed Services, the Committee noted that it is

> imperative that the Department engage industry in a consistent and meaningful dialogue as it continues to craft and implement policies and procedures for meeting this challenge [of preventing counterfeit parts]. The committee considers close and continuing communication between industry and policy makers to be instrumental to effecting sound policies and procedures, throughout the defense industrial base, and for avoiding costly or ineffectual missteps in mitigating the threat of counterfeit electronic parts.

H. Comm. on Armed Servs., National Defense Authorization Act for Fiscal Year 2013, H.R. Rep. No. 112-479, at 186 (2d Sess. 2012).

Conclusion—To be certain, § 818's requirements will make it more difficult to introduce counterfeit electronic parts into the defense supply chain. However, § 818 leaves unaddressed many of the structural issues that have given rise to counterfeiting opportunities. A long-term, cooperative effort by governments, OEMs, distributors and contractors will be required to solve this problem. For now, defense electronic contractors must focus on preparing for the new anti-counterfeit rules.

✦

***This Feature Comment was written for The Government Contractor by* Craig Holman, Evelina Norwinski *and* Dana Peterson. *Craig Holman is a partner and Dana Peterson is an associate in Arnold & Porter LLP's Government contracts group. Evelina Norwinski is a partner in Arnold & Porter's litigation group and co-author of* Brand Integrity: Strategies for Fighting Contraband and Counterfeit Goods.**