Bloomberg BNA

Federal Contracts Report™

DOD

Counterfeit Electronic Parts: What to Do Before The Regulations (and Regulators) Come?

Part 1: New Requirements

BY ROBERT S. METZGER AND JEFFERY M. CHIOW

Late in 2011, Congress enacted new legislation – section 818 of the FY 2012 National Defense Authorization Act (2012 NDAA) – that requires the Department of Defense to impose on contractors new and very strict obligations to detect and avoid counterfeit electronic parts in the defense supply chain. DOD already has taken significant, interim measures to act on the intent of the legislation [1] and is obligated to produce rules governing contractors by September 26, 2012. Owing to the urgency of the situation, it is widely expected that the regulations will be issued without prior notice and comment, on an ''interim'' but nonetheless binding basis.

Incidents of reported counterfeit parts continue to rise. In 2011, there were more than 1,300 counterfeit incidents reported from around the world to the Electronic Resellers Association International (ERAI) – more than double the number reported in 2010 and 2008, and quadruple the number reported in 2009.[2] Even these statistics greatly understate the problem, however. Until enactment of section 818, even highly regulated U.S. defense contractors were subject only to ''voluntary'' reporting obligations, and there is considerable evidence that many companies did not report experience with known or suspect counterfeit parts.[3] The Senate Armed Services Committee, in an investigative

[1] DOD Instruction 4140.01, issued on December 14, 2011, requires DOD personnel to report ''all occurrences of suspect and confirmed counterfeit parts. . .in the appropriate reporting system to include the GIDEP.'' A March 16, 2012 DOD Memorandum, ''Overarching DOD Counterfeit Prevention Guidance'' by Frank Kendall, undersecretary of defense for acquisition, technology, and logistics, also requires GIDEP reporting and provides guidance relative to several other requirements of section 818.

[2] ''Counterfeit Chips on the Rise,'' IEEE Spectrum (June 2012), *available at* http://spectrum.ieee.org/computing/hardware/counterfeit-chips-on-the-rise.

[3] *Id.* A representative of one company commented that in the past there was simply no financial reason to report fraudulent chips. With the new legal responsibilities imposed by section 818, that is changing.

Robert S. Metzger is a partner and Jeffery M. Chiow an associate in the Washington, D.C. office of Rogers Joseph O'Donnell, P.C., a San Francisco, Calif.-based law firm with 30 years commitment to public contracting matters.

 ISSN 0014-9063

report released on May 21, 2012, identified approximately 1,800 cases of suspect counterfeit parts in the defense supply chain in 2009 and 2010 – of which only 15 percent had been reported on GIDEP.

Section 818 will have a global impact. Although the law requires regulations that will govern DOD's suppliers, those suppliers depend upon many tiers of vendors that combine to represent the ''global supply chain'' for electronic parts. Companies that become subject to new laws, regulations, and sanctions will flow down these requirements to every level of their supply chain and to their sources around the world.[4]

Part I of this article provides an assessment of the current controversy surrounding electronic counterfeit parts and an analytic framework for understanding the objectives and operation of section 818 of the 2012 NDAA. In Part II, to be published next week, we focus on specific actions prudent companies should take now to prepare themselves for the new requirements and reduce exposure and costs.

Recent Events: The Senate Armed Services Committee Investigative Report & Action on the FY 2013 National Defense Authorization Act. Counterfeit electronic parts have been much in the public eye in recent weeks. On May 21, 2012, the Senate Armed Services Committee (SASC) released a final report following its two-year investigation of the threat posed by counterfeit electronic parts to the defense supply chain.[5] Although many of the findings were previewed in testimony at hearings the SASC held in 2011,[6] the report has drawn media attention[7] – and for good reason. The report shows counterfeit electronic parts to be a pernicious problem that threatens the operability and reliability of U.S. weapon systems and could endanger our troops and allies.[8] The making of counterfeit electronic parts has become a very big business, conducted by unscrupulous but sophisticated operators, sometimes enjoying a degree of state protection (if not sponsorship). Counterfeit electronic parts produce great costs and risks to the U.S. government.

U.S. military systems are vulnerable to counterfeit electronic parts for reasons that are easy to understand but difficult to combat. Many U.S. systems, of course, depend upon electronic assemblies that use a great variety of individual electronic parts. Over a period of years, commercial sources have been relied upon increasingly for a great majority of the component electronic parts.[9] Electronic systems built for defense applications often have lengthy product life cycles, sometimes measuring in decades. In contrast, the production cycle for representative commercial electronic parts may be measured in months.[10] As a result, too frequently it proves difficult for contractors to obtain the parts they need, for system maintenance and support, from original device manufacturers or their authorized distributors. Facing a demand for parts, but shortage of supply from the most reliable sources, contractors and DOD itself have taken to purchasing electronic parts from distributors, broker, or other suppliers whose corporate credentials are ''irregular'' at best.[11] As described in the SASC report, when an electronic part is no longer available from the manufacturer or an authorized distributor, buyers are often forced to rely on ''independent distributors,'' of which there are thousands just in the United States [12] While some of these distributors are reputable, the SASC investigation and earlier GAO studies spotlight the use of shadowy brokerages and on-line sales of electronic parts via Internet trading platforms.[13]

The SASC report used ''case studies'' of aircraft programs of the Air Force and Navy, and a missile defense system of the Missile Defense Agency, to show how counterfeit electronic parts have come into the defense supply chain, to demonstrate the risks posed to system reliability, and to illustrate the adverse cost and mission consequences.[14] There is no reason to believe that these

---

[4] One estimate is that non-U.S. based suppliers accounted for more than $2 billion of U.S. government procurement spending between 2007-2011 and an estimated 362 non-U.S. companies, worldwide, have supplied parts that could be directly impacted by the new law. ''US counterfeit parts crackdown will be felt in Europe,'' *ElectronicsWeekly.com* (April 30, 2012), *available at http://www.electronicsweekly.com/Articles/30/04/2012/53553/us-counterfeit-parts-crack-down-will-be-felt-in-europe.htm*.

[5] ''Inquiry Into Counterfeit Electronic Parts in the Department of Defense Supply Chain: Report of the Committee on Armed Services United States Senate'' hereinafter the ''SASC report,'' available at http://www.armed-services.senate.gov/Publications/Counterfeit percent20Electronic percent20Parts.pdf.

[6] Video of the SASC Hearing and related materials are available at http://armed-services.senate.gov/e_witnesslist.cfm?id=5254..

[7] *See e.g.* Lee Ferran, ''Counterfeit Chinese Parts Slipping Into U.S. Military Aircraft: Report'', ABC News, May 22, 2012 available at http://abcnews.go.com/Blotter/counterfeit-chinese-parts-slipping-us-military-aircraft-senate/story?id=16403599 and Larry Shaughnessy, ''Probe finds 'flood' of fake military parts from China in U.S. equipment,'' CNN News, May 22, 2012 available at http://security.blogs.cnn.com/2012/05/22/probe-finds-flood-of-fake-military-parts-from-china-in-u-s-equipment..

[8] DOD responded to the SASC report by citing stepped up, aggressive action to address the problem of counterfeit parts. However, Pentagon Press Secretary George Little told reporters that he was ''unaware to date of any loss of life or catastrophic mission failure that has occurred because of counterfeit parts.'' ''DOD Combats Counterfeit Parts Threat,'' Armed Forces Press Service, May 23, 2012, available at http://www.defense.gov//News/NewsArticle.aspx?ID=116456.

[9] The Federal Acquisition Streamlining Act of 1994 (''FASA''), Pub. L. No. 103-355, 108 Stat. 3243 (1994) and the Federal Acquisition Reform Act of 1996 (''FARA''), Pub. L. No. 104-106, 110 Stat. 186 (1996) introduced a preference for increasing commercial acquisitions in federal procurements..

[10] *See* SASC report, at 9-10 (discussing declining defense industry market influence and shorter production lifecycles among other causes of defense industry parts obsolescence).

[11] *See* SASC report, at 10; *see also* ''Dangerous Fakes: How Counterfeit, Defective Computer Components from China Are Getting into U.S. Warplanes and Ships,'' *Business Week* (Oct. 2, 2008) (quoting the commanding General of the Defense Supply Center in Columbus, OH in 2008 as supporting electronic parts purchases from internet or ''kitchen-table'' parts brokers based on the belief that ''less than one-quarter of 1 percent of what we buy is compromised.'')

[12] *See* SASC report, at 10.

[13] *See, e.g.,* SASC report, at 20, *DOD Supply Chain: Suspect Counterfeit Electronic Parts Can Be Found on Internet Purchasing Platforms*, GAO-12-375 (February 2012).

[14] The case studies in the SASC report included the Navy's SH-60B helicopters and P-8A anti-ship and submarine aircraft, the Air Force's C-130J and C-27J cargo aircraft and the Missile Defense Agency's Terminal High Altitude Area Defense (THAAD) missile system.

  FCR ISSN 0014-9063

case studies are unique or isolated examples of the problem. To the contrary, as supported by the SASC report, there are causes for concern that the problem is replicated elsewhere but presently unknown and unremedied.[15]

"U.S. military systems are vulnerable to counterfeit electronic parts for reasons that are easy to understand but difficult to combat."

The publication of the SASC report and attendant publicity has increased the public pressure upon the whole of the defense supply chain to find and exorcise counterfeit electronic parts. This will be an extraordinarily challenging undertaking, not because there is any opposition to the principle, but because of the great difficulties that exist between the *condition* (proliferation of counterfeit or suspect parts in the supply chain) and the *objective* (their elimination). The obligations of section 818 –while they apply directly to large DOD contractors, who are ''covered''[16] in that they perform work for DOD under CAS-covered contracts – also must flow down to subcontractors, vendors and suppliers.[17] The threat extends to the very ''lowest'' level of the supply chain where counterfeit discrete microelectronic devices and parts can be introduced, and extends upward, across a very broad universe of higher tiers, reaching ultimately large companies that manufacture and integrate systems. Exposure to counterfeit electronic parts thus extends to device makers, distributors and other sources of parts supply, to commercial and military suppliers of hardware in which electronic parts are installed, and even to service or solution providers who rely entirely upon commercially-sourced electronic equipment (as even that is not absolutely immune from infiltration of counterfeit components).

This is why section 818, though it addresses directly prime contractors to DOD and high-tier subcontractors, undoubtedly will have an impact upon commercial companies, worldwide, who make or distribute electronic parts. Even though some of these devices are essentially commodities, where the cost and price of piece parts are very low, the new law will affect the global sources of such devices because higher-tier users must ensure sources of genuine part supply throughout product or system life cycle. The new law does not distinguish between counterfeits of special-purpose military electronic parts and counterfeits of lower-level commodity devices utilized in commercial equipment that is employed in systems sold to the military. Indeed, even contractors that sell no hardware to DOD but deliver services or solutions dependent upon electronic hardware must take cognizance of the law's intentions, even though it does not appear to apply directly.[18]

Even before official implementation of section 818, and months before the date by which DOD must produce new regulations, there has been some distress and considerable speculation in the contractor community about the potential costs and consequences of the new law and the expected regulations. These efforts led industry groups to seek to amend section 818 via revisions included in what will become the FY 2013 NDAA. The House Armed Services Committee responded positively with amendments that would offer a qualified ''safe harbor'' to contractors.[19] Under the House-passed version, the costs of confirmed or suspect counterfeit electronic parts, and for rework or corrective action, would not be unallowable if the contractor had an operational system to detect and avoid counterfeit parts that DOD had reviewed and approved, *and* if the parts in question had been procured from an approved source or provided as government-furnished property (GFP), *and* if the contractor had provided ''timely notice'' of the identification of a counterfeit or suspect part.[20]

Industry organizations have endorsed the House-proposed changes as encouraging contractors to swiftly implement effective systems to detect and avoid counterfeit parts. The SASC, nonetheless, declined to adopt the House language, leaving the subject to be resolved by the full Senate or in Conference Committee.

As is evident from the SASC investigation report, the SASC's perspective likely is that contractors should not have been paid for parts, or for correction and rework, that, being counterfeit, did not comply with specifications and requirements in the first place. As explained in the committee's report, making these costs *unallowable* was seen as a powerful incentive to contractors to implement systems that would detect and avoid such parts, and therefore minimize the occurrence of replacement or corrective costs.[21]

Responsible and equitable allocation of the incentives and burdens of detecting and avoiding counterfeit parts implicates many complex considerations – and presents many ''unknowns'' that ought to prompt due caution in implementation of the new law's mandates.[22] Making

[15] The SASC identified over 1,800 incidents involving more than 1,000,000 parts based upon responses to its requests for information, but those requests only went to a small sector of the defense supply chain, specifically: DLA, 10 large defense contractors and 22 companies that had conducted testing for at least three of the defense contractors. *See* SASC report, at 12. Also, the fact that there was little to no reporting of those 1800 incidents in GIDEP, suggests that identified suspect counterfeit parts outside the narrow swath of the SASC's investigation also went unreported. *Id.* at 17-19.

[16] *See* section 818(f)(1), which cites Section 893(f)(2) of the 2011 NDAA, defining covered contracts for purposes of the so-called ''business systems rule.''

[17] *See* section 818(e)(2)(A).

[18] section 818(c)(2) requires DOD to issue new regulations covering contractors who ''supply electronic parts or products that include electronic parts.''

[19] *See* HR 4310 § 816, Contractor Responsibilities in Regulations Relating to Detection and Avoidance of Counterfeit Electronic Parts.

[20] *Id.*

[21] *See* SASC report, at 71-72. The SASC, however, has signaled its appreciation of industry concerns. In its Report on the 2013 NDAA, it encouraged DOD to solicit the views of both independent experts and interested parties – including representatives of original equipment manufacturers, DOD prime contractors, and lower-tier contractors in affected industries – to address implementation issues. *See* ''National Defense Authorization Act for Fiscal Year 2013, Report To Accompany S.3254'', Report 112-173, Committee on Armed Services, United States Senate, at p. 152.

[22] Practical concerns about the implementation of section 818(c)(2), making costs of counterfeit parts, suspect parts, and

costs of remediation unallowable raises concerns about fairness and risks of unintended consequence. The contractors whose costs are to be disallowed cannot be said to have the whole responsibility for the introduction of counterfeit parts into the supply chain. Indeed, the contractors at greatest risk of disallowed costs may be the victims of unscrupulous business practices, or sloppy inspection and testing, at many levels below their visibility or control. Some responsibility resides with DOD because of its decisions to increase reliance upon inexpensive, commercially-sourced items rather than pay higher prices for specialized, high reliability parts. In point of fact, DOD itself may be the source — for example through its depots — of counterfeit parts furnished to DOD contractors. Moreover, experts say that it is impossible to entirely eliminate counterfeit parts from the supply chain.[23] Should industry find that the financial consequence of the new law and DOD regulations is too great to bear, some companies might choose not to participate in supply to DOD. Should this occur at lower levels of the supply chain where microelectronic parts are sourced, or among commercial device suppliers whose products are regularly employed in systems sold to DOD, the higher-tier DOD suppliers might find it impossible to support existing products or even to supply DOD's needs for new items. For these and related reasons, industry has sought to moderate the financial consequence of the new law by proposing remediation costs be allowed as a cost of doing business where a contractor has a compliant detection system, purchased parts from an OEM or ''trusted supplier,'' and promptly fulfilled reporting obligations once a fraudulent part was found. Industry also has sought the opportunity to inform DOD of its implementation concerns before new regulations are released and made effective.

The Law: Section 818 NDAA 2012. Originally introduced by SASC Chairman Carl Levin (D-Mich.) and Ranking Member John McCain (R.-Ariz.), following the SASC's investigation, section 818 of 2012 NDAA takes aim at counterfeit electronic parts at several ''junctures'' in the supply chain:

■ **Detection.** The law strengthens the inspection regime for imported electronic parts.[24] The secretary of homeland security, after consulting with the secretary of defense, is to establish and implement a ''risk-based methodology'' for enhanced targeting of electronic parts imported from any country. Customs and Border Protection (CBP), which is under the authority of the Department of Homeland Security, previously had expressed concern about sharing unredacted product information from suspect counterfeit products.[25] The law explicitly authorizes CBP to share unredacted information from and samples of suspect products, their packaging and labels, with the company whose product is suspected of being counterfeited, in order to better identify and exclude counterfeit parts at our borders.[26] Already, new regulations have been issued with immediate effect to allow CBP to make limited disclosure of information appearing on merchandise for the purpose of assisting in determining whether the merchandise bears a counterfeit mark.[27]

■ **Exclusion.** The combination of additional and clarified detection authority and increased enforcement sanctions clearly is intended to deter foreign sources from attempting to export counterfeit electronic parts to the U.S. and to discourage would-be importers of such parts. The SASC investigation indicates that virtually all counterfeit electronic parts originate outside of the United States – the great majority from China.[28] Thus, better enforcement at the border should help to stem the flow. Cutting off the *supply* of counterfeit parts from China is an obvious and compelling strategy to deal with this threat. However, counterfeit electronic parts have been routed through Canada and the United Kingdom, and they may originate or flow through any country. The *demand* for counterfeit electronic parts, in any event, originates not with the countries where they are made but with the countries (like the United States) where there is a market to purchase needed parts.[29] In

---

rework and corrective action unallowable, are further discussed below.

[23] *See e.g.*, KPMG Study: Managing the Risks of Counterfeits in the IT Industry (on file with the authors) available at: http://www.agmaglobal.org/press_events/press_docs/Counterfeit_WhitePaper_Final.pdf (''No anticounterfeiting effort is entirely foolproof, but the better ones can make a significant difference.'')

[24] *See* section 818(d) and SASC report, at 67.

[25] CBP expressed concern that the Trade Secrets Act ''prohibits the disclosure prior to seizure of confidential business information found on merchandise suspected of [being counterfeit].'' As a matter of policy, based upon the CBP's concerns about its obligation to protect confidential business information, CBP had refused to share unredacted product information with the companies whose trademarks were suspected to have been infringed. By making explicit the authorization to share such information, Congress intended to have CBP exercise authority that it arguably already possessed. *See* SASC report, at 67.

[26] *See* section 818(g)(1). The influx of counterfeit electronic parts may be abated by tougher CBP measures. Section 818 also requires the secretary of defense, by September 26, 2012, to implement a program to ''enhance contractor detection and avoidance'' of counterfeit electronic parts. While the law requires DOD to conduct an ''assessment'' of its acquisition policies and systems, for the ''detection and avoidance'' of counterfeit electronic parts, there is no specific mandate that DOD implement a program to *enhance* detection, like that required of its contractors. Rather, DOD is obligated to improve its ''guidance'' and implement improved approaches to ''minimize the impact'' of counterfeit parts.

[27] ''Disclosure of Information for Certain Intellectual Property Rights Enforced at the Border,'' Interim Rule, 77 Fed. Reg. 24375 (Apr. 24, 2012)(to be codified at 19 C.F.R. Parts 133, 151). The new regulations, while open for comment until June 25, 2012, were given immediate effect. As explained in the *Federal Register*, the changes will ''enhance CBP's enforcement capability against increasingly sophisticated counterfeit products that threaten the public health and safety and national security.'' *Id*. at 24,376.

[28] The SASC report claims that China was responsible for more than 70 percent of the greater than one million suspect parts identified in its investigation. SASC report, at 14. While 80 percent of first tier suppliers that provided counterfeit parts had a U.S. presence, the country of origin for the 126 cases the Committee investigated were all outside the U.S. *Id*. at 14-15.

[29] China may be a principal ''source'' of counterfeit parts, but the United States and other countries in the developed world generate the electronic waste (''e-waste'') from which semiconductors and other microelectronic parts are extracted by counterfeiters. At a recent conference, Bob Braasch, Senior Director, Supply Chain, for HIS, observed that 58 percent of e-wasted generated by the United States is shipped to developing countries. Counterfeit parts represent an unfortunate, and

  FCR ISSN 0014-9063

government-to-government dealings, the U.S. government could encourage China to suppress the flourishing and notorious counterfeit electronic parts industry. Many observers are very skeptical that China will be receptive to U.S. initiatives to suppress its industry of counterfeiting electronic parts, in part because China generates revenues from the 17 percent value added tax when paid by enterprises engaged in import-export, production, distribution or retailing activities.[30]

■ **Enforcement.** Section 818 amended 18 U.S.C. § 2320 to add a criminal offense for trafficking in military goods or service known to be counterfeit where use, malfunction or failure is likely to cause serious injury or death, impairment of combat operations or other ''significant harm'' to national security, and broadened the definition of the ''trafficking'' offense to include attempts or conspiracy.[31] For an offense involving counterfeit military goods or service, a fine of not more than $5 million, and imprisonment of not more than 20 years, are imposed for individuals, and a fine of not more than $15 million applies to corporations. Second or subsequent offenses face larger fines and longer maximum jail terms. New definitions are added; for example, a ''counterfeit military good or service'' is one that is falsely identified or labeled as meeting a military specification, or intended for use in a military or national security application.

■ **Purchasing Practices.** Although section 818 operates at many junctures, where it will likely have its greatest success is in changing purchasing practices. The new law requires DOD suppliers ''where possible'' to purchase electronic parts from original manufacturers or their authorized dealers, or from ''trusted suppliers'' that obtain such parts exclusively from the OEM or their authorized dealers. As to parts not currently in production or in stock from ''trusted suppliers,'' procedures are to be established for notification to DOD, inspection, testing and authentication. Also to be established is a system to ''qualify'' trusted suppliers, i.e., requirements to demonstrate appropriate policies and procedures.[32] Purchases from sources other than the OEM or authorized dealer, such as distributors, are allowed only on an ''exception'' basis and subject to specific notification and authentication requirements. These requirements are to apply to DOD itself – the U.S. federal government is the largest purchaser of information technology in the world[33] – and to ''contractors and subcontractors at all tiers.''[34] Through these changes, the law undoubtedly will cause defense suppliers and their lower tier vendors to forego, if not abandon entirely, purchases from brokers and limit purchases from independent distributors to those with demonstrable and documented controls, possessing appropriate certifications, and whose business record justifies confidence in the authenticity of supplied parts.

■ **Inspection & Testing.** If some aspects of section 818 are aimed at the *supply* side and are intended to prevent or deter further importation of counterfeit electronic parts and to punish those who attempt or do so, other aspects of the law emphasize *detection* to address the presently unknown quantity of bogus parts already are in the defense supply chain. As to its own purchasing activities, DOD is to issue new guidance that includes new requirements for inspecting and testing parts (and reporting and quarantining parts found to be counterfeit or suspect).[35] Obligations imposed upon contractors, again, are much more rigorous. Initially, where necessary parts are unavailable from OEMs or authorized dealers, ''inspection, testing and authentication'' is required when another source is used.[36] The regulations that are due on September 26, 2012, governing defense contractors, also require implementation of a program with attendant policies and procedures that address ''inspection and testing'' of electronic parts.[37] Also required are ''methodologies to identify suspect counterfeit parts'' and systems to detect and avoid counterfeit and suspect electronic parts. The law states that a compliant program, to detect and avoid counterfeit electronic parts, will cause these ''counterfeit avoidance and detection requirements'' to flow down to subcontractors. There is no restriction on how far down the requirement is to flow. Imposition of these additional inspection and test requirements will be costly and DOD will bear at least some of these costs where they are allocated to overhead of contractors under cost-type and flexibly-priced contracts and when they affect forward-pricing rates for fixed-price contracts.

■ **Reporting.** Accompanying the new inspection and testing systems will be requirements to identify parts as

---

unintended, form of ''recycling'' back to the United States of this waste. ''Counterfeits' Widespread Effects the Focus of Conference,'' (May 18, 2012), *available at* http://www.pcbdesign007.com/pages/zone.cgi?a=84222. The Congress may be encouraged to strengthen waste management laws to reduce or cut off the shipment of e-waste from the U.S.

[30] *See* ChinaWTO.com, ''Trade Regulations, Customs and Standards,'' at http://chinawto.com/wto/index-e.asp?sel=info&info=regulation.

[31] section 818(h).

[32] Section 818(c)(3)(D) contemplates that the authorization of ''trusted suppliers'' will comply with ''established industry standards.'' While there are many standards in the works, fewer are established. As concerns the qualification of distributors, the SAE ''G-19'' Committee, chartered in 2007, has not completed and released any standard applicable to the ''distributor'' function in the electronic parts supply chain. In the works are ARP6178 (Counterfeit Electronic Parts; Tool for Risk Assessment of Distributors) and AS6081 (Counterfeit Electronic Parts; Avoidance Protocol, Distributors).

[33] *See* GAO Report, GAO-12-74, ''Electronic Waste: Actions Needed to Provide Assurance that Used Federal Electronics Are Disposed of in an Environmentally Responsible Manner,'' Feb. 2012.

[34] Section 818 (c)(3)(A). Within 180 days of enactment, or June 28, 2012, DOD is to complete a self-assessment of its acquisition policies and systems for the detection and avoidance of counterfeit parts, and is to issue new guidance to DOD components engaged in the purchase of electronic parts. Section 818(a-b). As to DOD purchasing practices, a ''risk-based'' approach is to be used to minimize the *impact* of counterfeit electronic parts or suspect counterfeit electronic parts. This choice of words suggests that Congress recognizes the magnitude of the problem and the need to apportion scarce resources to efforts most likely to lead to the avoidance of counterfeit electronic parts in its supply system. In contrast, section 818(e) requires DOD to issue regulations governing contractors that will *eliminate* counterfeit electronic parts from the defense supply chain.

[35] Section 818(b)(2).

[36] Section 818(c)(3)(B).

[37] Section 818(e)(2). SAE's G-19 Committee is working on, but has not released, AS6171 (Test Methods Standard: Counterfeit Electronic Parts).

suspect or confirmed counterfeit electronic parts. New obligations are required on reporting and on treatment of the suspect or false parts. Various sources, including the GAO and the SASC,[38] have been critical of how industry, as well as DOD itself, historically have handled reporting once counterfeit parts have been discovered or are suspected. (The SASC report contains numerous examples of reporting that appears to have been untimely, inconsistent, and incomplete.)[39] DOD personnel who know or suspect the existence of counterfeit or suspect parts must make a report in writing within 60 days on GIDEP or a similar system, according to section 818.[40] The new regulations governing contractors also contain reporting obligations. A contractor (or subcontractor) who becomes aware or ''has reasons to suspect'' that any end item, component, part, or material purchased by DOD contains counterfeit (or suspect) electronic parts, must report on GIDEP (or other system as DOD may designate) within 60 days.[41] *In addition*, the contractor must report to *appropriate government authorities*, meaning that notification might be required by the context or as the new regulations may specify, by a prime contractor to its procurement contracting officer (PCO) or administrative contracting officer (ACO), and perhaps to the military department or command that is the end-item customer. As to discoveries by subcontractors, as these also must be reported to *appropriate government authorities*, a mechanism might be needed to communicate through higher tiers to the prime and from the prime to the government. A compliant contractor program, to detect and avoid counterfeit electronic parts, must include several elements pertinent to the reporting requirement – mechanisms to ensure *traceability* of parts, reporting itself, and *quarantining* of counterfeit and suspect counterfeit electronic parts. (Quarantining, in addition to facilitating later examination of a part, for causes that may include enforcement, also will help to avoid reentry of bad parts into the supply system.)

■ **Corrective Measures.** The new regulations, which DOD is to publish by September 26, 2012, shall provide that covered contractors who supply electronic parts or products that include electronic parts are ''responsible . . . for any rework or corrective action'' that may be required to remedy the ''use or inclusion'' of such parts.[42] At the very least, this obligation means that when a contractor identifies a counterfeit or suspect part, and after reporting the same, it must expunge the part(s) from its own inventory and remove and remedy their inclusion in work-in-process or undelivered work. Not resolved, but a source of potential concern for industry, is the question of whether a company that discovers and reports a counterfeit electronic part, where for example such a part was included in a system or assembly delivered to a higher-tier contractor or to the government customer, is responsible only for its own rework or corrective action or could face claims or demands for the costs experienced by the receiving contractor or using activity. Companies in the lower tiers of the supply chain can be expected to resist, if not refuse such exposure.

■ **Improvement of Contractor Systems.** Especially for systems integrators and defense contractors at higher tiers of the supply chain, another of the most important requirements of the new law is contained at section 818(e). This section directs the secretary of defense, by the regulations due no later than September 26, 2012, to implement a program to enhance contractor detection and avoidance of counterfeit electronic parts.[43] Such a program shall *require* covered contractors to establish *policies and procedures* to *eliminate* counterfeit parts from the defense supply chain. As a threshold matter, therefore, contractors are ''on notice'' that they must be prepared to document and demonstrate the existence of policies and procedures sufficient to achieve these ends. It may not be sufficient for such policies and procedures to mitigate risk of counterfeit parts, because the use of the word ''eliminate'' suggests little or no tolerance of any counterfeit parts.[44]

Contractor policies and procedures are to address:

- training of personnel;
- inspection and testing of electronic parts;
- processes to ''abolish'' counterfeit parts proliferation;
- mechanisms to enable traceability of parts;
- use of trusted suppliers;
- reporting and quarantining of counterfeit electronic parts and suspect counterfeit electronic parts;
- methodologies to identify suspect counterfeit parts and to rapidly determine if such a part, in fact, is counterfeit;

[38] *See e.g.* SASC report, at 17 (criticizing industry) and 64 (criticizing DLA); *see also* ''Defense Industrial Base Assessment: Counterfeit Electronics,'' U.S. Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation, http://www.bis.doc.gov/, January 2010.

[39] Reporting is a crucial function with both ''internal'' and ''external'' consequences. The ''internal'' function is that when counterfeit parts are discovered, they need to be located within the inventory, or in-process work, of the company making the discovery. The ''external'' function is to get the news out to other companies, as well as end-users, so that they can take necessary and prudent measures, such as further inspection and test, quarantine, removal, rework or repair.

[40] Section 818 allows for reporting to a different program designated by the secretary of defense, but DOD's subsequent instructions suggest GIDEP will be the required reporting mechanism.

[41] Section 818(c)(4). In answer to concerns expressed by industry, that reporting had been deterred previously, out of worry that a reporting company could be sued, section 818 provides that a reporting contractor shall not be subject to civil liability for satisfying its reporting obligations where a ''reasonable effort'' was made to determine whether a counterfeit or suspect counterfeit part was present. Section 818(c)(5).

[42] Section 818(c)(2).

[43] Relevant to this obligation is SAE Standard AS5553 (Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition), released by SAE International in April 2009. A ''Revision A'' now is in progress.

[44] This is in contrast to how the law requires DOD to act as concerns DOD's purchasing practices. As concerns guidance for DOD components that purchase electronic parts, section 818(b)(2) requires a ''risk-based approach to *minimize* the impact of counterfeit electronic parts . . .'' (Emphasis added.) It is hoped that DOD, in the rules and/or in their enforcement, will recognize the practical impossibility of insisting upon absolute, immediate ''elimination'' of counterfeit parts by all private concerns in the supply chain. Even if such were possible, theoretically, it would require a lengthy period of time and could cause great expense.

  FCR ISSN 0014-9063

■ the design, operation, and maintenance of systems to detect and avoid counterfeit (and suspect) electronic parts; and

■ flowdown of avoidance and detection requirements to subcontractors.

Further, the DOD regulations must provide for ''review and approval'' of contractor systems for the detection and avoidance of counterfeit (and suspect) electronic parts, which processes shall be comparable to those established for ''contractor business systems.''[45]

■ **Costs of Counterfeit Electronic Parts, Rework or Corrective Action.** The new law makes the cost of counterfeit electronic parts and suspect counterfeit electronic parts, and the cost of rework or corrective action ''that may be required to remedy'' the use or inclusion of such parts, unallowable costs under DOD contracts.[46] The SASC described this as an ''incentive'' to industry to make sure that it avoids the use or inclusion of counterfeit parts – and, undoubtedly, there will be such an effect as companies will seek to limit their exposure. There may be many other cost-related affects, however, which will be incurred by companies at all levels in the defense supply chain, and which these companies will expect the government to pay as ordinary, reasonable, and allowable expense. In the context of DOD's strained budget, questions will arise as to how DOD will absorb such expense, and DOD's zeal in enforcement of the new statute may require moderation as DOD's financial exposure becomes evident. Cost-related issues are discussed further below, under ''Critical Implementation Concerns.''

■ **Sanctions.** The new law, while it requires covered contractors to implement approved plans to detect and avoid counterfeit parts, and requires DOD to establish processes to review and approve such contractor systems, does not state squarely what happens to a contractor that fails to propose or implement such a system, or where the system it employs is found deficient. Instead, the law makes reference to those provisions of the FY 2011 NDAA, at Section 893, which led to the new rules on ''contractor business systems.[47] This suggests that DOD may issue rules that will decrement payments to contractors if they fall short of meeting the requirements for an acceptable system to detect and avoid counterfeit parts.[48] Further, section 818 requires DOD, in its new guidance, to address ''remedial actions'' that will be taken in the case of a supplier that repeatedly fails to detect or avoid counterfeit parts or fails to exercise due diligence.[49] Suspension or debarment is an action that DOD is to have available in such cases.

Critical Implementation Concerns. Apart from issues of policy or fairness, section 818(c)(2) presents very difficult implementation issues. Covered contractors are precluded from recovery of remedial costs on cost-type contracts irrespective of the contribution of other actors, including the U.S. government itself, to the presence and problem of counterfeit parts. There may be considerable contention, including claims and disputes, over the ultimate allocation of cost responsibility. Also unresolved, and potentially a source of future litigation, is the question of whether the duties of the new statute, including ''remedy'' for use of inclusion of a counterfeit electronic part, or the associated costs of ''rework or corrective action,'' apply only prospectively to new hardware delivered after the law's effective date, or retroactively as might encompass equipment long-ago delivered but remaining in inventory.

The new law makes the cost of rework and corrective action unallowable where necessary to ''remedy'' use or inclusion of a counterfeit electronic part. However, this does not appear to render unallowable the potentially large costs that will be required by other elements of section 818, such as higher materiel costs, costs of increased detection, inspection and test, and costs to develop, implement and sustain new systems and processes to assess and manage risk and assure compliant reporting and proper disposition of bad parts.

Many new measures are required that inevitably will increase the detection, reporting, and exclusion of counterfeit parts already in the inventory. Most of these costs will affect the higher tiers of the defense supply chain, especially in that the highest remedial costs likely will be incurred by the last contractor in the chain to have employed a part, before product delivery to the government. This might occur even though the prime-level contractor might have no knowledge of the fault and might legitimately have relied upon lower tier sources, or even the government (if GFP), as the source of the part or for validation and acceptance of the assembly in which a part is included.

Further, the law disallows costs of counterfeit (or suspect) parts and rework or corrective action, but does not answer a question that inevitably will appear: namely, what a contractor is to do, and at whose ultimate expense, where no ''genuine'' part is available from an original component manufacturer, authorized distributor, or other ''trusted source.'' In such event, if redesign is required, or the commissioning of limited production of a surrogate part, are these costs unallowable? Contractors facing such exposure certainly will look to the government to assume the financial responsibility.

Making remedial costs unallowable has a direct effect only upon CAS-covered contractors who bill on an incurred cost basis. Many supplies that may be ''infected'' by counterfeit parts, however, will have been provided under fixed-price contracts. There is considerable uncertainty as to how to treat remedial costs that would be allocable as direct costs to such contracts, and there also will be uncertainties as to whether or when particular costs are properly characterized as allowable warranty costs rather than unallowable costs of remediating counterfeit parts.

With considerable cause, industry has expressed concern that DOD might not have sufficient time to prepare regulations that can at once cover the complexities of the problem, the breadth and diversity of industries af-

[45] Section 818(e)(2)(B); *see also* Section 893 of the 2011 NDAA, 10 U.S.C. § 2302. The final ''Business Systems Rule,'' 77 Fed. Reg. 37, at 11335, was promulgated on February 24, 2012.

[46] Section 818(c)(2).

[47] Section 818(e)(2)(B).

[48] The implementing regulations for the business system rule were the subject of substantial public comment and there were several significant revisions before the Final Rule was published. There can be expected to be significant commentary concerning the reasonableness of any proposed withholding as well as many other complex implementation issues raised by section 818.

[49] Section 818(b)(3).

fected and their many layers, and the whole of Congressional imperatives, without excess risk of unknown and dysfunctional consequence. As of this writing, DOD has been opaque to receipt of input from the vendor community. While informal submissions have been made, and there are reports of communications between DOD and industry associations and individual companies, there has been no organized, open process for input from those who must create, validate and implement the new policies and procedures. As was done very recently, with the rule enhancing the authority of CBP to investigate and interdict the import of potential counterfeits, industry is concerned that DOD will issue the section 818 rules on an ''interim'' basis, effective on the date of publication, presumably allowing for receipt of comments afterwards.[50] Even if DOD has a technical legal basis to issue these rules first and seek comment afterwards, this is unsound in this application because of the complexity of the subject matter and the very real potential that interim rules, given immediate effect, will have severe, unknown and adverse consequences upon both the industrial base and upon DOD's ability to secure necessary supplies and support. If interim rules ''must'' be issued without public comment prior to their effective date, DOD would serve its own interests and align its conduct more closely with the OFPP Act by limiting the scope of initial rules and proceed to elaboration informed by public comment and experience.

Responsible Measures –"Acting Ahead." From the foregoing, it is apparent that the new regulations will require many actions and impose many risks and costs upon the defense contracting community, and, to an extent, upon the commercial firms that supply commodity electronic parts and electronic equipment. Some companies, particularly large, higher-tier primes and leading system subcontractors, already have implemented procedures and process that will be required. However, close examination of the new law, and actions taken by DOD already that signal what to expect in the September regulations, reveal that many companies will find it necessary to conduct comprehensive self-examination, to assess vulnerability to counterfeit electronic parts, and that a complex combination of actions will be needed to respond and successfully avoid, if not eliminate such parts.

[50] *See* 77 Fed. Reg. 24375, ''Disclosure of Information for Certain Intellectual Property Rights Enforced at the Border,'' Apr. 24, 2012 (to be codified at 19 CFR Parts 133, 151). Industry has expressed its frustration and disagreement with what is perceived to have been increasing reliance by DOD on the use of interim rules. A few, recent examples include the Business Systems interim rule, DFARS Case 2009-D038, 76 Fed. Reg. 28856 (May 18, 2011) and the Sustainable Acquisitions Rule, FAR Case 2010-001, 76 Fed. Reg. 31395, May 31, 2011. Industry has asserted that DOD, in many instances where an interim rule has been used, has deviated from the ostensible requirements of Section 418b(a) of the OFPP Act, 41 U.S.C. § 418b(a) and FAR 1.501, which require publication for public comment of procurement regulations that create a significant cost or administrative impact on contractors or offerors. DOD has sought to justify its actions on the basis of ''compelling circumstances'' and cited the availability of authority to waive publication requirements.

  FCR ISSN 0014-9063