THE Procurement LAWYER

SECTION OF PUBLIC CONTRACT LAW • AMERICAN BAR ASSOCIATION • VOLUME 47, NUMBER 4 • SUMMER 2012

Legislating Supply Chain Assurance: An Examination of Section 818 of the FY 2012 NDAA

By Jeffery M. Chiow and Robert S. Metzger

Jeffrey M. Chiow

Robert S. Metzger

Section 818 of the 2012 National Defense Authorization Act (NDAA), Detection and Avoidance of Counterfeit Electronic Parts, introduced as a Senate amendment,[1] attempts to address the threat posed to America's national security by counterfeit electronic parts. Section 818 grew out of a Senate Armed Services (SASC) Committee investigation[2] utilizing reports by the Department of Commerce,[3] the Government Accountability Office (GAO),[4] industry groups,[5] and others.[6] The investigation highlighted serious risks to the nation's economic and security interests posed by counterfeit electronic parts. The risks are real, and Congress is to be commended for acting, but the problem is enormous and complex. Much will depend upon care and judgment in drafting implementing regulations and establishing new standards and procedures.

The Department of Defense (DoD) must find a balance that recognizes industry costs and contractor risk, potentially higher prices for many weapons and systems, and possible harm to the defense industrial base.[7] A March 16, 2012, DoD memorandum directs the secretaries of the military departments and directors of defense agencies to apply existing policies "to prevent, detect, remediate, and investigate counterfeiting in the DoD supply chain."[8] The memo, which parallels many of the provisions of section 818 and may foreshadow DoD's implementing regulations, calls for immediate action to decrease the probability of counterfeit parts throughout DoD's supply chain, with special emphasis on mission critical components, critical safety items, electronic parts, and load-bearing mechanical parts.

The new law sets two important deadlines. First, within 180 days of enactment (June 28, 2012), the DoD is to have completed an internal assessment of its policies and systems for the detection and avoidance of counterfeit electronic parts. It also must issue "guidance" on actions that DoD components can take to "implement a risk-based approach to minimize the impact of counterfeit electronic parts or suspect counterfeit electronic parts" on DoD.[9] Ninety days later, on September 26, 2012, section 818 requires DOD to revise the Department of Defense FAR Supplement (DFARS) to address the detection and elimi-

(continued on page 23)

Jeffery M. Chiow (jchiow@rjo.com) is an associate and Robert S. Metzger (rmetzger@rjo.com) is a partner in the Washington, D.C., office of Rogers Joseph O'Donnell, P.C.

Issue Highlights

contract with the government underlies its claim."

On October 21, 2005, P.J. Marx applied for a patent on a lead-free bullet. Shortly after the application, Marx entered into three separate NDAs concerning his ballistics research. He signed the NDAs as a sole proprietorship; subsequently he transformed his business into a succession of corporations, the last of which was Liberty Ammunition, Inc. The parties agreed that pursuant to the NDAs; Marx supplied DoD with information related to bullet design. Picatinny Arsenal found Marx's samples and schematics insufficient and decided to proceed with an in-house design. On July 6, 2010, the government issued Marx his patent. The CoFC cited three Federal Circuit decisions as holding that "no more than a non-frivolous *allegation* of a contract with the government" will suffice to establish jurisdiction. The actual existence of a contract is a matter of the merits of the case, rather than one of jurisdiction.

Meeting information: The Intellectual Property Committee generally meets bimonthly (lunch served). Contacts: cochairs Fernand A. Lavallee, (202) 799-4401, fernand.lavallee@dlapiper.com; Mary Shallman, (562) 797-2233, mary.e.shallman@boeing.com; and Holly E. Svetz, (703) 560-6992, hsvetz@wcsr.com. For more information on this and other committees, visit the Section's website www.americanbar.org/groups/public_contract_law.html and click on "committees on the left-hand navigation bar. PL

SUPPLY CHAIN ASSURANCE

(continued from page 1)

nation of counterfeit parts by contractors.[10] Those regulations must make contractors that supply electronic parts or products containing them responsible for preventing the use or inclusion of counterfeit (or suspect) electronic parts, and any necessary corrective action or rework. The DoD will not pay contractors for counterfeit (or suspect) electronic parts or for any costs of rework necessary to remedy the inclusion of such parts.

The statute demands that contractors manage their supply chain to eliminate the risk of counterfeit parts and take remedial actions consistent with the legislation's dictates under threat of civil or criminal sanctions. The establishment and maintenance of contractor systems to detect and eliminate counterfeit electronic parts will generate nonrecurring costs for the new systems, and recurring maintenance costs. These compliance costs presumably are recoverable on DoD contracts, unlike costs of counterfeit (and suspect) electronic parts and associated rework.

The law applies to all tiers in the supply chain and to every electronic part, whether simple or complex, where the end item is to be sold to the DoD under a contract covered by the Cost Accounting Standards (CAS).[11] Section 818 will reach deeply into the supply chain, including to commercial sources of electronic parts, because a compliant DoD contractor system to detect and eliminate counterfeit parts must be flowed down to subcontractors with no limitation as to "tier," complexity, function, or value of a subcontract.

There are many reasons to support the objectives of the new law, and certain key aspects of the law conform to industry expectations and objectives. For example, avoiding purchases from other than original equipment manufacturers (OEMs), authorized dealers, or other trusted suppliers is widely accepted as the most important requirement to ensure supply chain integrity. However, there are potentially enormous unanticipated consequences from the well-intended legislation and the details of regulatory implementation may prove decisive.

The Law's Mandates and DoD Responsibilities

Contractors are responsible for managing supply chain risk. Section 818 mandates that contractors take responsibility for detecting and eliminating counterfeit electronic parts in supplies and systems delivered to DoD and that they bear all of the costs of any associated rework or corrective action.[12] The premise of the law is that everything the DoD buys must be genuine, notwithstanding the proliferation of counterfeit parts throughout the global electronic parts market.[13]

Consistent with industry best practices, section 818 requires that "whenever possible" the DoD and all DoD contractors and subcontractors shall obtain electronic parts from OEMs or their authorized dealers or from "trusted suppliers" who obtain parts exclusively from OEMs or their authorized dealers.[14] When electronic parts are no longer in production and not in stock, purchases must be made from trusted suppliers.[15] Where there are no such reliable sources, contractors must notify DoD and the electronic parts they buy must be inspected, tested, and authenticated.[16]

DoD is required to establish qualification requirements—consistent with 10 U.S.C. § 2319—to identify trusted suppliers,[17] and contractors and subcontractors may identify additional trusted suppliers.[18] Contractors' trusted supplier programs must comply with industry standards, are subject to audit by DoD officials, and the contractor must "assume the responsibility" for authenticity of parts.[19] The law provides no safe harbor from the obligation to pay for repair or replacement of counterfeit (or suspect) electronic parts—even when contractors rely on DoD's trusted suppliers (or OEMs and their authorized dealers, for that matter).

Section 818 also requires DoD to establish a mandatory reporting program.[20] Whenever contractors and subcontractors know or "have reason to suspect" that they have received counterfeit electronic parts, they are required to make a written report to the appropriate government officials and the Government Industry Data Exchange Pro-

gram (GIDEP) or a similar incident reporting database within 60 days.[21] This requirement broadcasts the news of suspect counterfeit parts with the goal of avoiding their sale to other unwary purchasers or users, and ideally would enable DoD to provide direction to industry about next steps to take.[22]

Today, in the absence of such guidance, there is no consistency in how companies respond when counterfeit parts are detected. Some return counterfeit parts as defective product and demand a refund; others preserve the parts for a potential government investigation; while still others destroy the parts.[23] Some contractors are reluctant to report suspect counterfeit parts due to the perceived risk of triggering third-party litigation.[24] Under section 818, a contractor that carries out its reporting obligation under the law is immune from civil liability so long as the contractor made a reasonable effort to determine the item contained counterfeit electronic parts.[25] This safe harbor provision, however, does not limit a contractor's potential liability while it is performing due diligence. Nor does it provide any redress against a supplier that provides suspect counterfeit parts. These are issues contractors must address contractually.

The new law limits the sources from which DoD contractors and subcontractors may purchase electronic parts. It requires contractors to have an auditable process to identify other than government-approved suppliers. It contains a mandatory reporting requirement. A further potentially onerous requirement is the obligation for covered contractors to adopt and implement systems to detect and eliminate counterfeit electronic parts.[26]

By September 26, 2012, DoD must implement a program to improve contractor systems to detect and eliminate counterfeit electronic parts.[27] The contractor systems will need to address several areas, including:

- 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 a suspect counterfeit part is, in fact, counterfeit;
- design, operation, and maintenance of systems to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts; and
- flow down of counterfeit avoidance and detection requirements to subcontractors.[28]

DoD must also establish a process to approve or disapprove these new contractor systems similar to the process for the business systems rule created pursuant to section 893 of the 2011 NDAA.[29]

DoD must first establish internal processes. The statute assigns several initial responsibilities to DoD before it issues regulations over contractors. First, DoD must establish department-wide definitions of the terms "counterfeit electronic part" and "suspect counterfeit electronic part."[30] Second, DoD must implement a risk-based approach for its own procurement to minimize the impact of counterfeit electronic parts.[31] Third, DoD must issue or revise guidance to consider, among other things, suspension and debarment of suppliers who fail to demonstrate supply chain integrity.[32] Fourth, DoD must establish a reporting system for government employees and contractors to make written reports to appropriate government officials and GIDEP (or similar) within 60 days of discovering suspected counterfeit electronic parts.[33] Fifth, DoD must also develop a process to analyze, assess, and act on those required reports.[34]

History and Background

There have been previous legislative efforts to combat the issue of counterfeit parts. The Prioritizing Resources and Organization for Intellectual Property Act (PRO-IP Act), introduced in 2007 and passed in 2008, focuses broadly on the issues of counterfeiting and intellectual property piracy.[35] The PRO-IP Act created a new office for the enforcement of intellectual property, the US intellectual property enforcement coordinator, commonly referred to as the White House's "IP Czar."[36] In its 2010 report, that office announced the development of a government-wide working group to prevent the government purchase of counterfeit products.[37] The working group would identify "gaps in legal authority, regulation, policy and guidance that preclude an optimal U.S. Government procurement approach."[38]

The current push to confront counterfeit parts follows well-publicized examples of the harm counterfeit parts can cause, especially as concerns national security.[39] An *Inside the Air Force* article reported in March 2008 that the potential of fake parts in the military aviation inventory was so high that some aircraft could contain numerous counterfeit parts potentially reducing the reliability of weapons from 5–15 percent annually.[40] The article also touched on parts obsolescence and the increased counterfeit risks posed by reliance on commercial components, the profit motive for criminal counterfeiters, and the potential for state-sponsored hackers to infect commercial microchips with malicious code.[41] A *Business Week* article six months later expanded on and brought increased awareness to the issue.[42] A handful of government and industry reports within the last few years have helped illuminate the counterfeit parts problem.[43]

The extent of the problem and costs/ability to fix it are unknown. The true extent of the problem is unknown and is likely unknowable.[44] Even though it cannot be quantified, the threat posed by counterfeit parts is undeniable as demonstrated by the number and variety of reported incidents.

In response to SASC's 2011 inquiry, selected contractors reported 1,800 counterfeit part incidents involving over 1 million suspect counterfeit parts. Much of the SASC hearing was devoted to describing specific inci-

dents. When the source of fake parts was traced through the supply chain, in every case, the trail led to Shenzen, China. Witnesses from Raytheon Company, L-3 Communications Corporation, and The Boeing Company testified that counterfeit parts had been discovered, for example, in FLIR systems on Navy SH-60B helicopters, flight displays on Air Force C-27J combat tactical support aircraft, and Navy P-8A Poseidon antisubmarine and anti-surface aircraft.

Lieutenant General Patrick J. O'Reilly of the Missile Defense Agency testified at the SASC hearing that his organization had discovered seven instances of counterfeit parts since 2006, including one incident that resulted in the removal and replacement of almost 800 parts from an assembled missile.[45] In another incident, 38 missile assemblies were reworked and 250 parts were discarded.[46] Emphasizing the seriousness of the problem, Lt. Gen. O'Reilly's prepared testimony warned, "We do not want to be in a position where the reliability of a $12 million THAAD[47] interceptor is destroyed by a $2 [counterfeit] part."[48]

Where, why, and by whom are counterfeit electronic parts generated? GAO testified at the SASC hearing about an ongoing forensic investigation in which GAO created false part numbers and sought online vendors that would offer to fill the bogus orders.[49] Several online vendors responded by creating and sending counterfeit parts to the GAO.[50] An independent distributor testified concerning his trip to China, where he observed the overt counterfeit industry in Shenzen and nearby Shantou.[51] He saw scrap circuit board components stripped from e-waste, washed in a river, and left to dry on the riverbank.[52] The components were then sorted by women and children, sanded down and made to look new.[53] The parts later would be sold as new and often marked as "military grade" parts.[54] There was no effort to hide the counterfeiting work, and no concern among counterfeiters about the reliability of the components.[55]

A complicating factor in fashioning a remedy is that there are several sources of counterfeit parts acting with different motivations. State-sponsored entities may intentionally introduce counterfeit electronic parts into the defense supply chain to degrade the reliability or functionality of military systems and to introduce malware.[56] A criminal enterprise could provide counterfeit parts with similar "sinister" motives, to fund terrorist activity or simply to realize a profit. An unsophisticated parts broker might unknowingly introduce counterfeit electronic parts or a sophisticated parts broker might be deceived about the pedigree of electronic parts and unknowingly introduce counterfeits.

The material that becomes counterfeit parts also comes from a variety of sources. Discarded electronics may be recycled and salvaged parts reintroduced into the supply chain as if they were new. Other sources of counterfeit parts include production overruns or discarded materials from the OEM that are not properly discarded and are resold as genuine parts.[57] Whatever the source, the danger posed by counterfeit parts is that there is no guarantee of their reliability and, therefore, no way of predicting when they may fail or what the consequences of such failure might be.[58]

The nature of government procurement increases the risk of counterfeit parts. Counterfeit electronic parts impact the entire global economy.[59] As a result, supply chain scholars are engaged in efforts to develop systems to identify counterfeit parts and remove them from the supply chain to keep these untrustworthy components out of end products.[60] Legitimate manufacturers in all sectors need such systems to ensure the integrity of their supply chains.[61] While virtually all industries may be affected by the problem, section 818 reflects both urgency and criticality as to how counterfeit parts affect the defense industry. The defense supply chain is particularly vulnerable because of greater susceptibility to parts obsolescence in conjunction with equipment service lives longer than may be supported by the original manufacturer's parts supply chain. Due to DoD's national security mission, military equipment failure caused by counterfeit parts may have more detrimental consequences than in other sectors.[62]

> ***"We do not want to be in a position where the reliability of a $12 million THAAD interceptor is destroyed by a $2 [counterfeit] part."***

Many factors contribute to parts obsolescence in the defense supply chain. The defense and aerospace systems have much longer planned service lives than their electronic components.[63] The long government acquisition life cycle and short electronic component production runs can lead to situations where a system, when fielded, uses "commercial" electronic components that already are obsolete. Government-unique requirements also contribute to the obsolescence of electronic components. While government procurement policies for nearly two decades have encouraged commercial acquisitions, including the purchase of commercial-off-the-shelf (COTS) products,[64] government users continue to demand some level of customization, creating specialized market niches with small production runs and few suppliers.

Moreover, as Pentagon purchasing practices in recent years moved from military specific (MIL-SPEC) to commercial requirements, the obsolescence problem has been exacerbated, as the pace of technological innovation is faster in the commercial market for electronic parts than in a specialized government market. Where a government acquisition is made on a COTS basis, there may be no component level "bill of materials" and thus no parts traceability. Thus, in COTS-based acquisitions, component ob-

solescence may translate into system obsolescence. A 2003 European law, the Restriction of Hazardous Substance Amendment (RoHS), also contributes to component obsolescence as the global electronics supply chain endeavors to reduce hazardous materials in electronics.[65] Where defense systems rely on RoHS noncompliant electronic components, the DoD either must spend funds to engineer a compliant alternative or find a source for the obsolete RoHS noncompliant parts.

Reduced defense spending, global economic retraction, and a DoD preference for commercial parts over specialized military parts are key industrial base considerations. They have undercut the business case to support a supplier base focused on US defense requirements. While it is widely recognized that DoD systems are vulnerable to parts obsolescence, efforts to maintain the supply base have lacked coherence. Section 818 mandates greater vigilance on the part of DoD contractors and increases their exposure for counterfeit parts. The costs of increased supply chain security will not be borne by industry alone. The statute's "trusted supplier" regime may revive a discrete base of suppliers who answer to DoD needs.

The practice of using Internet searches to purchase electronic components increases the likelihood that purchasers will encounter unscreened counterfeit sources.

Contractors will likely charge a premium as compared to their purely commercial counterparts for parts already in inventory or new parts; DoD will bear the added expense resulting from this new law and policy.

Defense suppliers should operate with efficiencies and cost structures as would render them competitive in the commercial world. Practically, however, the new law may pose a barrier to participation in defense requirements if the costs of compliance render a supplier noncompetitive in the commercial marketplace. There is a risk that some companies will elect not to supply to DoD rather than lose commercial markets. However, if government and industry ultimately can agree on a reasonable apportionment of costs and risks, the new standards initiated for DoD may migrate outside military procurement. Companies may be able to leverage their DoD supply chain assurance investment across business lines.

The earlier-described problem of electronic part obsolescence makes it more likely that counterfeits will be introduced into the defense supply chain.[66] When a product is obsolete, the costs of acquiring it increase as suppliers have increased storage costs and there may be relatively little competition among remaining providers. As the price of genuine obsolete parts rises, so do the incentives to counterfeiters.[67] They are able to offer a price advantage over suppliers of the genuine part.[68] Additionally, the process of authentication is more burdensome for obsolete parts as there may not be an OEM or any trustworthy information readily available to verify a product's authenticity.

Government acquisition practices also have contributed to the purchase of counterfeit electronic parts. A singular focus on price, for parts deemed electronic commodities, ignores the potential risk that parts may be counterfeit. Specifically, the practice of using Internet searches to purchase electronic components increases the likelihood that purchasers will encounter unscreened counterfeit sources.[69] Auction procedures and lowest-priced technically acceptable procurements similarly favor low-cost suppliers, including counterfeit suppliers.[70]

In 2008, as news articles were first identifying the counterfeit parts problem, officials at a major DoD electronic parts supply center said they did not inspect electronic parts brokers or conduct background checks.[71] The law did not prohibit buying from Internet sites or even from in-home brokers, and the Air Force's brigadier general in charge of the supply center reportedly estimated, "less than one-quarter of 1% of what we buy is compromised."[72] Without training in supply chain risk mitigation and tools to ensure the legitimacy of sources, government purchasers cannot make informed decisions to trade off costs for the assurance that electronic parts are genuine.

Additionally, a low-cost purchasing approach penalizes those companies that invest the most in securing their supply chains. Simply put, contractors that invest the most will be unable to compete on price with companies that shirk their responsibilities. To achieve the intended benefits of section 818, DoD must therefore examine and credit supply chain integrity in its award decisions.

The 2011 NDAA section 806 concerns supply chain integrity in DoD procurements.[73] Section 806 gives DoD the authority to consider supply chain risk and take adverse procurement action where the secretary of defense or of a military department determines a company poses a supply chain risk to a national security system.[74] Section 806(e), provides for the reduction of supply chain risk in covered DoD procurements by (1) establishing qualification requirements designed to reduce supply chain risk,[75] and (2) allowing the exclusion of certain sources from competitions based upon a determination that they pose a risk to the supply chain.[76]

Section 806 also allows DoD to direct that companies be excluded from consideration for subcontracts.[77] Where DoD takes such action, it must notify other DoD components and other agencies that may be subject to similar supply chain risk.[78] DoD may also decide to limit the disclosure of information relating to the basis for a contractor's exclusion without being subject to review by GAO or in any federal court.[79] The Intelligence Authorization Act

for Fiscal Year 2012 contained a provision extending similar authority to intelligence agencies.[80]

Implementation Issues

Section 818 passed Congress without opposition. In important respects, the law follows industry "best practices" for avoiding and responding to counterfeit electronic parts. However, the particulars that emerge in the implementing regulations are important. There are three main opportunities to shape the regulations to achieve a balance between the commendable goal of the statute and the costs and consequences industry will experience in its implementation: (1) incentivizing compliance; (2) embracing a risk-based approach with realistic and targeted goals; and (3) shaping the process to align with commercial efforts.

Incentivizing compliance/allocating risk. In light of the significant cost repercussions of the new compliance requirements and contractor liabilities, the regulations to implement section 818 must provide an incentive for industry members that take a good-faith, risk-based approach to eliminating counterfeit electronic parts from the DoD supply chain. Implementing regulations should not unfairly penalize companies for past practices that were in compliance with law, regulation, and policy at the time.

Under section 818, the costs of counterfeit (or suspect) electronic parts and all associated rework are to be borne solely by the contractor, no matter what precautions a company takes or how well it has developed counterfeit detection policies and procedures. This is troubling for several reasons. Contributing causes to counterfeit parts, such as parts obsolescence, the globalization and commercialization of the supply chain, and the contraction of a specialized defense electronics supply base, are outside the authority or responsibility of defense system contractors.

Moreover, testimony at the SASC hearing indicated compliance efforts will need constant management as the most sophisticated counterfeiters closely monitor and adapt to counterfeit detection methods.[81] The problem is much bigger than any company can address through rigor in its supply chain management. The government has many important responsibilities, including its role in regulating imports, negotiating with China and other significant sources of counterfeit parts, and management of the relevant industrial base. Should the government fall short in its responsibilities, contractors should not carry all the financial consequence.

To avoid inequitable and undeserved financial injury to contractors, the regulations should include a safe harbor provision, some level of cost-sharing or other limitation of liability for contractors that have used government-approved trusted suppliers or authorized distributors and have compliant counterfeit detection and elimination systems. Setting limits on risk and cost will incentivize contractors to invest in compliance and use only trusted sources. These measures may produce positive results in the cost-benefit analysis that some companies will undertake to decide whether to remain in the defense supply base. Saddling responsible companies with unrecoverable costs and excess risk without credit for investments in compliance can convince some, if not many, to forgo defense supply.

If only because contractors will face an immediate consequence of unallowable costs for counterfeit parts remediation, the new rules will generate costs on contracts awarded before the statute or regulations. The government needs to be discriminating in what solutions it requires. Not all compliance solutions will be worth their potential cost or disruptive consequences. In some circumstances, it may be appropriate, or even required, for a contractor to receive an equitable adjustment to its existing contract. DoD will have some latitude, in rulemaking, to distinguish between costs of counterfeit parts and associated rework and corrective action, which are unallowable, and costs of compliance systems to detect and eliminate counterfeit electronic parts, which are allowable. Equity, and fair allocation of ultimate responsibility, suggests DoD should write regulations to distribute costs and consequences, rather than shift all to contractors.

In the budgeting and planning of new acquisitions, DoD must account for the costs of higher supply chain assurance. One cannot reconcile the additional burdens and risks of section 818 compliance with price-based purchasing decisions that insist on the lowest possible materiel cost. In best value acquisitions, the government can and should elevate supply chain assurance as a significant evaluation factor. In contrast, when the government uses auctions, or makes award on the basis of the lowest price, technically acceptable offer, its procurement practices work against the objectives of supply chain assurance.

Saddling responsible companies with unrecoverable costs and excess risk without credit for investments in compliance can convince some, if not many, to forgo defense supply.

Fair allocation of risk should go hand-in-hand with incentivizing compliance. The counterfeit parts problem targeted by the legislation arises in a variety of scenarios, some very complicated. For illustration, a fault in a system may prompt an expensive investigation of a "suspected" counterfeit electronic part. If the investigation shows that the failure was not due to a counterfeit electronic part, responsibility for the costs should be governed by the contract and any warranty provisions—and not assigned to the contractor by operation of section 818. In some cases, it may not be possible to determine what party is responsible for introducing a counterfeit part.

The new regulations should not transfer cost and liability to contractors irrespective of their responsibility or opportunity to avoid the problem.

Risk-based approach with realistic and targeted goals. While restricting the sources from which contractors can source electronic parts is key, the causes and sources of counterfeit parts are diverse and complex, and there is great potential for variation in how counterfeit parts can affect system operation or reliability. Thus, DoD should strive for a pragmatic, financially responsible approach that is "context sensitive" to the particular application, costs, and performance risks. The statute specifically instructs DoD to take a "risk-based" approach to its *own* purchasing policies.[82] Similarly, the law obligates the secretary of homeland security to implement a "risk-based methodology" to screen the imports of electronic parts.[83] But there is no recognition in section 818, that to succeed, contractors must also employ risk-based solutions. This gap can be addressed by DoD in rulemaking.

When the government uses auctions, or makes award on the basis of the lowest price, technically acceptable offer, its practices work against supply chain assurance objectives.

If the regulations require "100% assurance" or shift "100% responsibility" to contractors, for every part of every system, regardless of history, pedigree, or purpose, the result will be unaffordable and unachievable.[84] Inspecting every component of every electronic system would quickly inflate the costs of support and maintenance of existing equipment as well as new costs incurred on future DoD procurements. Where counterfeit electronic parts are found (or suspected), replacement parts will not be available overnight and not all obsolete parts can be readily reengineered or replaced with new designs. Should the regulations adopt a "strict liability" premise, and impose unreasonable costs or impossible deadlines upon suppliers, claims and controversies will arise (as to current contracts).

Overreaching in the regulations may drive out some suppliers, which would exacerbate the problem of parts obsolescence and availability, contributing to diminished competition and higher prices. Even if it were possible instantly to stop the influx of counterfeit parts, there are already counterfeit electronic parts in contractor and DoD warehouses and in fielded systems. Addressing these problems, in myriad real world examples, requires measured, responsible action, not drastic or punitive measures.

Risk assessment and cost-benefit analysis must be part of any viable approach to reducing the threat posed by counterfeit electronic parts. The government and industry must establish realistic goals and priorities. Identifying mission critical and sensitive components should be an early priority. Once DoD and contractors know which parts of the supply chain are critical and sensitive, they can better target their policies, procedures, and finite resources.

Shape the process to align with commercial efforts. All legitimate electronics parts suppliers have an interest to develop policies and procedures that reduce the likelihood of counterfeit parts. Therefore, a critical objective in drafting the regulations is to seek alignment between the DoD-specific regime and commercial industry standards and best practices. It is inevitable that DoD (and other US government purchasers) will continue to depend upon a global, commercial source base for electronic parts. Accordingly, it is crucial to encourage better supply chain practices for all sources and sectors for electronic parts, and not isolate the DoD supply base or hold it to impossible standards. Requiring defense contractors to perform to supply chain standards that vary greatly from commercial best practices will not work. As the deviation increases between DoD's standards and commercial norms, DoD's prices will increase.

A true industry standard for detection and elimination of counterfeit electronic parts has not been achieved, though there has been significant progress.[85] Aerospace Standard AS5553-Counterfeit Electronic Parts; Avoidance, Detection, Mitigation and Disposition was developed through cooperation between government and industry. Advancing the AS5553 standard or some other industry standard is essential to accelerate government and industry cooperation to meet the statutory deadlines and to harmonize DoD requirements with commercial best practices.

Conclusion

Confirming the integrity of the global supply chain for electronic parts is an enormously complex undertaking. The new legislation is an appropriate and powerful start that will reduce vulnerability to the poisonous consequences of counterfeit parts in the military supply chain. However, the implementation of section 818 will be critical. Correcting the practices and managing the forces that produced the problem of counterfeit parts will take many years and will require the disciplined cooperation of government and industry. DoD and industry should cooperate to establish prudent, workable rules that achieve Congress's important goal while minimizing avoidable costs and other unintended consequences on the defense industrial base. PL

Endnotes

1. Pub. L. No. 112-81 § 818 (introduced as Amendment No. 1092 to S. 1867, 112th Cong., 1st Session) (hereinafter "Section 818").

2. Prior to the SASC inquiry, Senators Tom Carper (D-Delaware) and Sherrod Brown (D-Ohio) sent a letter to the Dep't of Defense (DoD) in August 2010 urging DoD to address the issue.

3. *See* U.S. Dep't of Com., Bureau of Indus. & Sec., Off. of Tech. Evaluation, Defense Industrial Base Assessment: Counterfeit Electronics (Jan. 2010) (hereinafter "BIS Report"), *available at* http://tinyurl.com/yejcgmh.

4. GAO-10-389, Defense Supplier Base: DOD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Counterfeit Parts (Mar. 2010) (hereinafter "GAO Report"), *available at* http://www.gao.gov/assets/310/302313.pdf.

5. Aerospace Indus. Ass'n, Special Report, Counterfeit Parts: Increasing Awareness and Developing Countermeasures (Mar. 2011), *available at* http://tinyurl.com/7w9yynt.

6. Brian Grow et al., *Dangerous Fakes: How counterfeit, defective computer components from China are getting into U.S. warplanes and ships*, Bus. Wk., Oct. 2, 2008 *available at* http://tinyurl.com/45q6zu.

7. Concern over the potential costs of the regime embodied in Section 818 can be mitigated if the regulations properly eliminate the source of the greatest risk, independent suppliers, and follow other recommendations set out herein.

8. Memorandum from the Acting Deputy Under Secretary of Defense, Acquisition, Technology & Logistics on Overarching DoD Counterfeit Prevention Guidance to Secretaries of the Military Dep't & Directors of the Def. Agencies (March 16, 2012) (on file with authors) *available at* http://counterfeitparts.files.wordpress.com/2012/03/pdf.pdf.

9. *See* Section 818(b)(2).

10. In a February 21, 2012, letter, the Council of Defense and Space Industry Associations (CODSIA) expressed concern with the scale and implications of the tasks required by Sept. 26, 2012, which "implicates the global commercial supply chain for all of American industry." *See* Letter from CODSIA to Messrs. Ginman & Estevez, (Feb. 21, 2012) (on file with authors), *available at* http://www.pscouncil.org/c/b/Letters_Comments_Tes.aspx. CODSIA consists of six industry trade associations, TechAmerica, Professional Services Council (PSC), American Council of Engineering Companies (ACEC), Aerospace Industries Association (AIA), U.S. Chamber of Commerce, and National Defense Industrial Association (NDIA).

11. *See* Section 818(f)(1), *citing* Section 893(f)(2) of the 2011 NDAA, defining covered contracts for purposes of the business systems rule.

12. *See* Section 818(c)(2); *see also* Transcript of SASC Panel 1, Sen. Brown at 16.

13. *See* SASC Hearing Opening Statement of Senator Levin at 6 ("There is no reason on earth that the replacement of a counterfeit part should be paid for by taxpayers, instead of by the contractor who put it in a military system.")

14. *See* Section 818(c)(3)(A)(i); *see also* BIS Report at 200 (recommending procurement only from trusted sources).

15. *See* Section 818(c)(3)(A)(ii).

16. *See* Section 818(c)(3)(B).

17. *See* Section 818(c)(3)(C).

18. *See* Section 818 (c)(3)(D).

19. *See* Section 818 (c)(3)(D).

20. *See* Section 818 (c)(4).

21. *See* Section 818 (c)(4).

22. *See* Henry Livingston, BAE Systems Electronic Solutions, Securing the DOD Supply Chain from the Risks of Counterfeit Electronic Components: Recommendations on Policies & Implementation Strategy, (Oct. 18, 2010) (hereinafter "BAE Recommendations") at 3 of 6.

23. *Id.* at note *vii* and accompanying text.

24. *Id.*

25. *See* Section 818(c)(5).

26. *See* Section 818 (e).

27. *See* Section 818 (e)(1).

28. *See* Section 818 (e)(2)(A).

29. *See* Section 818 (e)(2)(B) *referencing* 10 U.S.C. § 2302 note.

30. *See* Section 818 (b)(1)

31. *See* Section 818 (b)(2).

32. *See* Section 818 (b)(3).

33. *See* Section 818(b)(4).

34. *See* Section 818(b)(4).

35. *See* Press Release, U.S. Copyright Office, Prioritizing Resources and Organization for Intellectual Property Act Becomes Public Law 110-403 (Oct. 20, 2008), (on file with the authors), *available at* www.copyright.gov/newsnet/2008/354.html.

36. *Id.*

37. 2010 U.S. Intellectual Prop. Enforcement Coordinator Annual Report on Intellectual Prop. Enforcement (Feb 2011) at 9, *available at* http://tinyurl.com/3dseora.

38. *Id.*

39. GAO Report at 9.

40. John Reed, *Fake Parts Are Seeping into Military Aircraft Maintenance Depots*, News from Inside the Air Force (Mar. 28, 2008) (on file with the authors), *available at* http://tinyurl.com/82q2t3a. The article quoted and cited anonymous safety officials and Robert Ernst, who was then the head of aging aircraft studies for the Navy. The 5-15% degraded reliability estimate was provided by Ernst based on studies by the AIA.

41. *Id.* The article cited a 2007 Defense Science Board study concerning the potential that military microcircuits could be used to host malicious code. The board's study concluded, "current systems designs, assurance methodologies, acquisition procedures and knowledge of adversarial capabilities and intentions are inadequate given the magnitude of the threat."

42. Grow, *Dangerous Fakes*, *supra*. Senator McCain read extensively from the *Dangerous Fakes* article in his opening statement at the SASC hearing.

43. BIS Report, *supra*; GAO Report, *supra*, AIA Special Report, *supra*.

44. *See* GAO Report at 4 (noting DoD has no common definition of counterfeiting and DoD databases do not capture data on counterfeit parts); *see also* News from Inside the Air Force, *supra* ("the true percentage of counterfeit parts entering U.S. inventories is still unknown" and "no one has studied the true size of the problem.")

45. SASC Hearing Opening Statement of Lt. Gen. O'Reilly, USA, Director Missile Defense Agency at 7.

46. *Id.*

47. Terminal High Altitude Area Defense.

48. Opening Statement of Lt. Gen. O'Reilly, *supra*. The general's testimony highlights the inherent complexities of the threat posed by counterfeit electronic parts. It is difficult if not impossible to know which $2 part of a $12 million system is truly critical to its reliability; and as a result, it is hard to decide where to devote resources to identify counterfeit parts. Any realistic plan for combating the problem of counterfeit electronic parts must acknowledge that 100% assurance is unachievable, particularly in the short term. There are counterfeit electronic parts already in the DoD's supply chain, so successfully stopping the influx of new counterfeit parts would not even solve the problem. Practically speaking, the MDA's mission requires detailed component testing that would be inappropriate and cost-prohibitive in less-expensive systems that are nonetheless critical to national security.

49. SASC Panel I Tr. at 8–9, 24 (Richard S. Hillman, GAO Managing Director Forensic Audits and Investigations testifying).

50. *Id.* The GAO's final report of that investigation published on February 21, 2012, found that 16 either rare or outright bogus parts GAO ordered and received from online vendors were fakes. *See* GAO-12-375,DoD Supply Chain: Suspect Counterfeit Electronic Parts Can Be Found on Internet Purchasing Platforms (Feb. 2012), *available at* http://gao.gov/assets/590/588736.pdf.

51. SASC Panel I Tr. at 7, 11 (Thomas Sharpe, Vice President, SMT Corporation testifying)

52. *Id.* at 7.

53. *Id.*; *see also id.* at 2–4 (Sen. Levin's opening remarks); *id.* at 9 (Brian Toohey, President Semiconductor Industry Association testifying).

54. *Id.* at 9 (Toohey testifying).

55. *Id.* In the *Business Week* article *Dangerous Fakes*, *supra*, a Chinese counterfeiter told the authors "The dates [on the chips] are 100% fake, because the products pulled of the computer boards are from the '80s and '90s, [while] customers demand products from after 2000."

56. From 2004 to 2008, hundreds of routers (devices that direct data through networks) were sold to the Army, Navy, Air Force, and Marines as Cisco® routers, but were, in fact, counterfeits made in China. *See* Business Week, *Dangerous Fakes*, *supra*. The head of cyber security under the director of national intelligence indicated that such counterfeit routers had been linked to the crash of mission-critical networks and may contain hidden "back doors" enabling hackers, thieves, and spies to steal sensitive data. *Id.* In April 2011, the Commerce Department sent a survey to telecommunication companies, including AT&T, Inc., and Verizon Communications, Inc., asking detailed questions about the origin of equipment in telecommunications networks apparently to determine what vulnerabilities may exist from the incorporation of Chinese-made network components.

57. Rob Spiegel, *Counterfeit components remain a huge electronic supply chain problem*, EDN, *available at* http://tinyurl.com/btgzzse.

58. *See* SASC Hearing Tr. at 5 (Sen. Levin's opening remarks).

59. SASC Panel II Tr. at 2.

60. *See e.g*, Bhanu Sood et al., 22 (no. 10) *Screening for counterfeit electronic parts*, J. Materials Sci.: Materials in Electronics 1511-1522, *available at* http://tinyurl.com/c24xmty.

61. KPMG Study: Managing the Risks of Counterfeits in the IT Industry (on file with the authors) (hereinafter "KPMG Study") *available at* http://tinyurl.com/cscs82c.

62. Counterfeit electronic parts have been found in defibrillators, auto brake systems, and in the electronics systems that control public utilities. SASC Hearing Opening Statement by Toohey. The presence of counterfeit parts in these and other places pose similar and significant risks.

63. Janice Wood, *Counterfeit parts threaten aviation*, Gen. Aviation News (Mar. 16, 2011) *available at* http://tinyurl.com/bs24tee.

64. Policies favoring commercial acquisitions were primarily introduced through 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 or the Clinger-Cohen Act), Pub. L. No. 104-106, 110 Stat. 186 (1996).

65. The European Directive 2002/95/EC on the restriction of the use of certain hazardous substances in electrical and electronic equipment (commonly "Restriction of Hazardous Substances Directive" or "ROHS") established an international standard to which electronics manufacturers adhere. The EU's REACH requirements effective June 1, 2007, also impose registration requirements and prohibitions on some substances in products including electronic chips.

66. *See* Reed, *Fake Parts*, *supra* (counterfeits primarily in supplies for older aircraft; and commercial approach opens door to enterprising brokers of out-of-production parts).

67. KPMG Study at 3.

68. *Id.*

69. *See generally* SASC Panel 1, Testimony of Richard J. Hillman.

70. *See* KPMG Study at 3 (explaining the price advantage counterfeiters hold).

71. *Dangerous Fakes*, *supra* at 4.

72. *Id.* There was no basis provided for the general's .025% estimate, but contemporaneous sources suggested counterfeit rates of 5-15%. *See* KPMG study, *supra* and Reed, *Fake Parts*, *supra*.

73. Section 806 of the 2011 NDAA took effect on July 6, 2011, and applies to any solicitation for a national security system or IT components thereof, in which DoD considers supply chain risk per 10 U.S.C. § 2305(a). A related DFARS case 2011-D019, is "on hold," but implementation does not depend on a rulemaking.

74. Pub. L. No. 111-383 § 806, H.R. 6523, 11th Cong. § 806 (2010).

75. *Id.* at 806(e)(2)(A).

76. *Id.* at 806(e)(2)(B).

77. *Id.* at 806(e)(2)(C).

78. *Id.* at 806(d)(2)(B).

79. *Id.* at 806(d)(1). It is not clear from the language whether the determination to limit disclosure is unreviewable or if the exclusion action itself is beyond GAO or court review.

80. *See* Pub. L. No. 112-87 § 309, Senate 1458, 112th Cong., 1st Sess., enhanced procurement authority to manage supply chain risk. A DFARS case implementing Section 806 is currently on hold "awaiting NII input."

81. *See* SASC Panel 1 Tr. at 7 (Sharpe testifying). Some reports of counterfeit electronic components reveal that false papers have been generated to accompany counterfeit electronic parts. BAE Recommendations, *supra* at 2.

82. *See* Section 818(b)(2).

83. *See* Section 818(d).

84. *See* KPMG Study, *supra* at 14 ("No anti-counterfeiting effort is entirely foolproof, but the better ones can make a significant difference.")

85. BAE Recommendations, *supra* at 5.