Bloomberg BNA

Federal Contracts Report™

DOD

Counterfeit Parts: What to Do Before the Regulations (and Regulators) Come? Practical Steps Industry Can Take Now

BY ROBERT S. METZGER

Section 818 of the National Defense Authorization Act of 2012 (2012 NDAA) imposes a new regime on defense contractors – and on the Defense Department itself – to detect and avoid counterfeit electronic parts in the defense supply chain. The law requires DOD, on or before September 26, 2012, to revise the DFARS to address the detection and avoidance of counterfeit electronic parts.

The statute set an initial deadline, of June 28, 2012, for DOD to complete an internal assessment of its acquisition policies and systems for the detection and avoidance of electronic parts. This date came and went without a DOD announcement of results from such an assessment. However, a March 16, 2012 Memorandum signed by Frank Kendall, now Undersecretary of Defense for Acquisition Technology & Logistics (AT&L), entitled ''Overarching DOD Counterfeit Prevention Guidance'', addresses several requirements of Section 818. DOD may believe this memorandum – the ''Overarching Guidance'' – answers the initial requirements of Section 818.

DOD has initiated no formal or public process to solicit comments from industry on the rules that it is developing for detection and avoidance of counterfeit electronic parts. Instead, it appears that DOD intends to issue the rules and to make them effective upon release, requesting comments after-the-fact. As suggested by Part I of this article (97 FCR 647, 6/26/12) it is regrettable that rules will be put in force on such an important and complex subject without first receiving comment from the affected industry. This increases the possibility, if not probability, of unintended adverse consequences from the initial rules.

In any event, prudent companies are urged to act now to understand the new law, DOD's Overarching Guidance, to examine their exposure to infiltration of counterfeit electronic parts, and to act to reduce vulnerability. Companies at many tiers of the supply chain will be affected by the new law. While the details of the forthcoming regulations are unknown, a great deal can be understood, from the DOD Guidance, and from the investigative report of the Senate Armed Services Committee, about ''best practices'' that can be employed to reduce the risk and mitigate exposure to counterfeit electronic parts.

Robert S. Metzger is a Partner in the Washington, D.C. office of Rogers Joseph O'Donnell, P.C., a San Francisco-based law firm with 30 years commitment to public contracting matters. The author acknowledges the continuing assistance and insight of Jeffery M. Chiow, his colleague in the Washington, D.C. office of Rogers Joseph O'Donnell, with whom he has co-authored previous articles on this subject, including Part I of this article, ''Counterfeit Electronic Parts: What to Do Before the Regulations (and Regulators) Come?'' (97 FCR 647, 6/26/12)

DOD's March 2012 Memorandum: 'Overarching DOD Counterfeit Prevention Guidance.' The Overarching Guidance is closely aligned to many requirements of Section 818 and thus should be understood to presage what DOD will expect of its contractors this Fall, when it issues the new DFARS regulations required by the statute. Accordingly, companies should consider how they can apply the propositions of the Overarching Guidance to their own business practices, in advance of the DFARS due this Fall:

 ISSN 0014-9063

Importance: The Overarching Guidance cites counterfeit items as a ''serious threat'' to the safety and operational effectiveness of DOD systems. Contractors should respond appropriately, and not wait until told to act by DOD.[2]

Contractors should appreciate that the threat comes both from *unscrupulous* actors, who supply bogus electronic parts to meet demand and make a profit, and potentially from *state-sponsored actors*, who introduce counterfeit parts that may harbor malware or otherwise pose a latent threat to operations or information security. With regard to electronic systems used to perform critical military functions, industry should particularly expect increasing emphasis on avoiding risk of the second type.

Risk Assessment: The Overarching Guidance requires DOD to develop ''policies and strategies'' that focus on items ''that affect system performance or operation, the preservation of life, or safety of operating personnel.''[3]

By comparison, Section 818 calls upon contractors to ''*eliminate*'' all counterfeit parts from the supply chain and ''*abolish*'' their proliferation.[4] However, it is a practical impossibility for any contractor instantly to identify and eliminate all counterfeits that might be in its supply chain. Contractors should employ a risk-based approach as does DOD itself. An appropriate place to start is to evaluate systems, either ordered or in the build cycle, where a failure of a component electronic part could have a grave affect as suggested by the quoted language. Not all systems or supplies will have this level of exposure. Not all counterfeits will cause a system to fail, for example where there are redundancies or where an electronic device or lower level assembly is incidental but not critical to system functionality.

Existing Policies: The Overarching Guidance emphasizes the importance of ''taking action now'' to apply *existing* policy and procedures.

Companies are well-advised to act immediately to control sources of supply for microelectronic parts and to reinforce efforts aimed at detection and prompt reporting of counterfeit parts and suspect counterfeit parts, and to segregate such parts for further investigation and proper disposition.

Definition: The Overarching Guidance provides a definition of ''counterfeit materiel'' as: ''an item that is an unauthorized copy or substitute that has been identified, marked, and/or altered by a source other than the item's legally authorized source and has been misrepresented to be an authorized item of legally authorized source.''

In and of itself, this is significant as there has been considerable debate, over time, as to how to define a ''counterfeit'' part. DOD's definition treats as ''counterfeit'' an item that may be functionally identical to or perform equally as an original part if it is an ''unauthorized copy or substitute.'' Though this definition likely will draw continuing study, if not controversy, for the time being companies should discipline their purchasing and receiving organizations to employ this ''tight'' definition or, if not, to document the basis for a different definition.[5]

Beyond electronics: Section 818 addresses only counterfeit *electronic* parts. The Overarching Guidance, however, expresses a broader concern, encompassing ''mission critical components, critical safety items . . . and load-bearing mechanical parts,'' in addition to electronic parts.

As companies respond and assess their systems and procedures, they should examine their vulnerability to non-electronic counterfeit parts and how adequately they are equipped to detect, avoid and eliminate other types of counterfeits.

''Probability'': DOD requires its components to take immediate action to ''decrease the probability'' of counterfeit items.[6]

Here, the Overarching Guidance evidences a practical recognition that it will be impossible, immediately, to find and eliminate all counterfeit items already in the supply chain. It is hoped the same reasoning will be extended to industry when the new DFARS are released. For now, companies following this principle can undertake an evaluation of materiel for ''susceptibility'' to counterfeit sources of supply.[7] A purchasing organization might be asked to review historical records to identify purchase orders for electronic parts from independent distributors or brokers, or to find purchases of items (electronic or not) from sources other than the original component manufacturer (OCM) or original equipment manufacturer (OEM). Other risk indicators can be identified, such as high failure or return rate, system life, age of original design, criticality of function, and so forth.

Notification: The Overarching Guidance *requires* DOD program managers to ensure that they are notified by their suppliers when critical items are not obtained from the OEM, OCM, or an authorized distributor – and this requirement flows down from the prime contract.

It is potentially significant that this notification is *not* triggered when there is evidence of a ''counterfeit'' or ''suspect counterfeit'' electronic part, such as might trigger a report on Government Independent Data Exchange Program (GIDEP). Rather, notification is expected from contractors based only on the source of supply where a ''critical item'' is concerned. In response, companies should act promptly to examine their records of supply to systematically identify potentially unreliable sources of mission-critical parts. Coordination with various internal functions may be required, e.g., QA, Purchasing, Engineering, Manufacturing, Product Support, Business Management, and Contracts. In-house inventory should be reviewed for

[2] The potential threat posed by counterfeit parts was well documented by the Report of the Senate Armed Services Committee, ''Inquiry Into Counterfeit Electronic Parts in the Department of Defense Supply Chain: Report of the Committee on Armed Services United States Senate'' (the ''SASC Report''), available at http://www.armed-services.senate.gov/Publications/Counterfeit%20Electronic%20Parts.pdf.

[3] This corresponds to Section 818(b)(2) (DOD to implement a ''risk-based approach to minimize the impact of counterfeit electronic parts . . . .'')

[4] *See* Section 818(e)(2)(A) (emphasis added).

[5] Where parts are not available from the original source, a company may consider a third-party alternative that satisfies form, fit and function. Such parts may be reverse-engineered to reflect a new or non-infringing design. To avoid any risk that they would be considered a ''counterfeit,'' a company would be well-advised to notify its higher-tier customer and/or the government of its plans and their justification.

[6] This is consistent with Section 818(b)(2), which instructs DOD to take a ''risk-based'' approach to minimize the impact of counterfeit or suspect counterfeit electronic parts.

[7] Specific suggestions in this regard are provided below.

  FCR ISSN 0014-9063

pedigree and to determine source of parts. Records can be reviewed to identify parts obtained from potentially unreliable sources of supply, such as uncertified brokers or independent distributors (except where approved). Protocols can be developed to instruct personnel on internal investigation, appropriate test and inspection, assessment, and escalation. Procedures should describe how to document and inform DOD customers, or higher tier contractors, when exceptions are discovered – even if there is no known failure in the potentially suspect part.

Program Protection: The Overarching Guidance requires DOD program managers to follow the ''Program Protection Plan Outline and Guidance,'' referencing a Memorandum from the USD/AT&L dated July 18, 2011. Included is a requirement to ''evaluate counterfeit risk and implement countermeasures for mission critical components.''

The Program Protection Plan Outline emphasizes early program protection planning and reflects a more comprehensive approach to delivering trusted systems. It is also specifically focused on analysis essential for system security design. This guidance should be taken into account by design and engineering organizations for systems in design and development. As to existing systems, the import may be to elevate the significance of assessing system vulnerability to the risks accompanying counterfeit electronic parts and to define countermeasures.

Non-critical items: Where a program manager finds there is a counterfeit risk that warrants action, for other than mission-critical components, the Overarching Guidance requires the manager to document risk mitigation.

The ''action'' that a program manager may take, following the Overarching Guidance, may involve direction to contractors. Companies receiving instructions for risk mitigation actions should record the direction and maintain accounting for associated costs (which should be allowable). As to non-critical items, companies can immediately apply similar practices to those of DOD. A risk-based assessment may begin with identification of ''mission critical'' systems and by isolating ''high risk'' situations for further study. As that process is extended further into the supply chain, and across the build cycle, there will be instances where concerns arise as to source reliability, or availability of parts with requisite pedigree, even in non-critical applications. Such risk mitigation efforts should proceed according to a documented plan and the results should be recorded and reviewed.

Safety Notice: The Overarching Guidance also reaffirms the requirement to include DFARS 252.246-7003, which requires a contractor to notify the government within 72 hours after discovery of ''credible information'' concerning ''nonconformances and deficiencies'' for ''critical safety items'' and otherwise that ''may result in a safety impact for systems, or subsystems, assemblies, subassemblies, or parts integral to a system.''

This is an important requirement that is *not* confined to ''counterfeit'' parts or limited to *electronic parts* but generally requires contractors to report to their customer such nonconformances as could affect safety. Even if absent from a present contract, higher-tier companies are advised to adopt such reporting practices.[8] The Overarching Guidance does not specify how a contractor is to accomplish the notification. A prime contractor should have practices that rapidly escalate potential safety issues for critical items and that dictate how and to whom notification is made. Notification on GIDEP is an appropriate step, but it may not be sufficient if the safety threat is imminent and/or the risk is great. More direct notification may be the responsible act. To conform to the literal terms of the Overarching Guidance, lower tier contractors must notify the ultimate government customer, when known. If unknown, a lower tier contractor should notify higher tiers in the supply chain and request confirmation of notice to the government customer.

Industry Standards: The Overarching Guidance directs DOD components to review industry standards for anti-counterfeiting and to ''address those standards in contracting requirements as appropriate.''

Plainly, companies should evaluate and adopt, or plan for adoption of, practices that conform to existing or emerging standards.[9] The SASC Report on its investigation of counterfeit parts cites favorably SAE AS5553-2009, ''Counterfeit Electronic Parts; Avoidance, Detection, Mitigation and Disposition'' developed by the ''G-19 committee'' of SAE International. Other potential Standards to evaluate include the published SAE ARP 6178-2011, ''Fraudulent/Counterfeit Parts; Tool for Risk Assessment of Distributors'' and a number of Standards now under development, including, in particular, SAE AS 6081 ''Counterfeit Electronic Parts; Avoidance Protocol, Distributors'', SAE AS 6174 ''Counterfeit Materiel; Detection, Mitigation, and Disposition'', SAE AS 6171 ''Test Methods Standards; Counterfeit Electronic Parts'' and SAE ARD 6884 ''Terms and Definition – Fraudulent/Counterfeit Electronic Parts''.

Testing: A further requirement of the Overarching Guidance is that DOD components establish testing and verification requirements for items not received from an OEM, OCM, or authorized distributor that have a ''high risk for counterfeit potential.'' Program managers are directed to apply these requirements to prime contracts and to flow these down to subcontractors and lower tier suppliers.

This instruction strongly suggests that a prudent company should adopt a testing regime rather than waiting for this to emerge in the DFARS regulations this Fall.[10] The costs of such an effort, unlike the costs of remediation, potentially are allowable. Testing may be accomplished as a function of Receiving Inspection for

---

[8] Section 818(b)(4) requires DOD to act to establish processes to ensure that DOD personnel report suspect counterfeit electronic parts. Section 818(h) increases the criminal penalties for trafficking in counterfeit military goods (not limited to electronic parts) where failure is likely to cause serious bodily harm or other significant harm to a combat operation.

[9] Section 818(c)(3)(D)(i) requires DOD to issue regulations that will establish qualification requirements for ''trusted suppliers'' who must ''comply with established industry standards.''

[10] Section 818 (c)(3)(B) requires the new DFARS regulations, implementing the statute, to include a requirement for ''inspection, testing and authentication'' of electronic parts that DOD, or a DOD contractor or subcontractor, obtain from any source other than the OCM, authorized dealers or ''trusted suppliers.''

newly acquired parts, although test resources also should be available to QA and Manufacturing if there is cause for suspicion that a counterfeit part has been encountered. Companies will need to examine their inventory status and test resources in light of risks. Test and inspection procedures range from the ordinary, inexpensive, and non-intrusive, such as visual inspection under a microscope, or validation of parts marking against known standard, to other and more rigorous forms of evaluation that are potentially destructive as well as expensive. Companies may wish to establish a continuing relationship with specialized test resources who own expensive equipment and who can be certified against industry standards. Internal protocols should determine the circumstances that justify or require more rigorous inspection and test.

GIDEP Reporting: DOD program managers are to ensure that contractor and subcontractor reports of suspected or confirmed counterfeit items are entered into the GIDEP program, which is to serve as the DOD central reporting repository.[11] The Overarching Guidance also requires DOD activities to report suspected or confirmed counterfeit items that they discover, using GIDEP.

Clearly, a prudent contractor will act immediately to examine and reinforce its mechanisms to learn of counterfeit or suspected counterfeit parts and to report on GIDEP. Inconsistency in use of GIDEP and other reporting practices by DOD and contractors was pointed out in GAO's 2010 Report.[12] More recently, criticism was leveled in the SASC report.[13] Beyond GIDEP, companies will wish to examine industry reporting resources, such as the ''High-Risk Parts Database'' that is maintained by ERAI.[14]

Investigate: DOD personnel are required by the Overarching Guidance to investigate suspected counterfeit incidents and report confirmed cases to criminal authorities.[15] Parts suspected of being counterfeit are to be held until resolution of non-conformance.

Contractors should be vigilant to inform their purchasers and, if appropriate, federal law enforcement personnel where they confirm a counterfeit part. It no longer appears advisable to treat suspected counterfeit electronic parts, whenever discovered, as ''returns to source'' or as ordinary warranty items. Where there is a basis to believe a part is ''counterfeit'' (as DOD defines it), the correct response by a contractor is to evaluate and resolve the question and to report promptly, taking care to ''quarantine'' the suspect part in order to preserve relevant evidence.[16]

Training: Finally, the Overarching Guidance directs DOD to develop and provide training to DOD personnel on proper measures to address counterfeiting.[17]

Companies are well advised to examine their existing training programs and to develop new and reinforced counterfeit parts training. Training may be advisable on several different levels. A basic awareness of Section 818 and the key rules concerning counterfeit and suspect counterfeit electronic parts may be appropriate for general distribution within a government contractor organization. Higher-level training is recommended for those activities, such as Supply Chain (Purchasing), QA and Manufacturing who have more direct responsibility in the acquisition of electronic parts, incoming inspection and test, use, storage, and disposition. Because there are important new requirements to flow down to vendors, and new demands can be expected from higher tier contractors, special training may be appropriate for Business Management and Contracts.

A 'Functional' Approach to Contractor Detection & Avoidance of Counterfeit Electronic Parts. Part I of this article examined the requirements of Section 818 at what were termed ''junctions'' of the supply chain: Detection, Exclusion, Enforcement, Purchasing Practices, Inspection and Testing, Reporting, Contractor Systems, Costs and Sanctions.[18]

DOD's Overarching Guidance, examined above, is instructive on many of these junctions – but not all. Key areas required for contractors to comply with Section 818, but not well covered by the Overarching Guidance, concern *Purchasing Practices*,[19] *Detection and Avoidance*,[20] *Contractor Systems*[21] and *Cost Accounting*.[22] Undoubtedly, the DFARS due this September will ad-

[11] Section 818(b)(4) requires DOD to act to ensure that its own personnel report to GIDEP or a similar program and Section 818(c)(4) similarly requires reporting by DOD contractors. Even before enactment of Section 818, DOD had required that all occurrences of suspect and confirmed counterfeit items be documented in GIDEP. Dept. of Defense Instruction 4140.01,''*DOD Supply Chain Management Policy*'' (Dec. 14, 2011) at 13.

[12] GAO-10-389, ''Defense Supplier Base: DOD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Counterfeit Parts'' (Mar. 2010), at 6 (''the GIDEP Deputy Program Manager told us that GIDEP is not widely used to report suspect counterfeits'');

[13] SASC Report, at 64(DLA . . . rarely filed GIDEP reports for suspect parts it identified in 2009 and 2010).

[14] ERAI was formerly known as the Electronic Resellers Association, Inc. ERAI is now comprises resellers (distributors), OEMs, contract manufacturers, government agencies and other trade organizations. Information about ERAI's database can be obtained at http://www.erai.com/Index.aspx.

[15] Section 818(c)(4) requires contractors to report in writing within 60 days to ''appropriate government authorities'' and to the GIDEP program. Presumably, upon confirmation that a part is counterfeit and discovery of evidence of willful and deceitful supply of such a part, the ''appropriate'' government authority will be the Department of Justice or a U.S. Attorney's Office.

[16] Under Section 818(e), DOD is to issue regulations that require defense contractors to implement a program to enhance detection and avoidance of counterfeit electronic parts. An element of a compliant program is the ''reporting and quarantining of counterfeit electronic parts and suspected counterfeit electronic parts.'' *Id*. at § 818(e)((2)(A)(vi).

[17] Section 818(b)(2) requires DOD to act to improve training of its personnel and Section 818(e)((2)(A)(i) includes as an element of a compliant contractor system the training of personnel.

[18] Several of these (Detection, Exclusion, Enforcement, Sanctions) concern acts that are the responsibility of the federal government. Examples are increased enforcement by the Customs and Border Protection (CPB) unit of the Department of Homeland Security, tougher measures intended to keep offshore-sourced counterfeits from entering the U.S. and to punish would-be importers.

[19] Section 818(c)(3) requires implementation of controls on electronic parts purchasing practices and qualification of ''trusted suppliers.''

[20] Section 818(c)(2)(A) requires contractors are to detect and avoid the use or inclusion of counterfeit electronic parts or suspected counterfeit electronic parts.

[21] Section 818(e) speaks to required contactor systems for detection and avoidance of counterfeit electronic parts.

  FCR ISSN 0014-9063

dress these subjects. However, companies can act now to improve their systems and reduce their vulnerability to counterfeit electronic parts, easing the burden of eventual compliance with the new rules.

Conversations should occur among the many affected internal disciplines and functions, e.g., Supply Chain Management (Purchasing), QA, Materiel Management, Business Management and Contracts, Legal and Compliance, as well as Manufacturing, Design and Engineering organizations. Results should be documented and, where appropriate, reviewed with subject area experts and process consultants.[23]

Section 818 was the product of a two-year investigation of the Senate Armed Services Committee. The report examines and relates several ''Case Studies.'' From these, one can discern both practices to avoid and actions to take. These are presented for the four functional junctions cited above.

Purchasing: The SASC report emphasizes the substantially greater risk of purchasing electronic parts from a source other than the OCM, OEM or authorized distributor.[24]

Four military systems were addressed as ''Case Studies.'' In the first of these, suspect counterfeit parts intended for use in the Navy's SH-60B Seahawk helicopter were traced to an independent distributor, an electronic parts ''recycler'' and a web-based seller. The second involved purchase of parts for the C-27J avionics system from an ''independent electronic parts distributor'' that in turn had purchased the parts from a China-based supplier (not the OCM). In the third Case Study, suspect counterfeit parts used in both the C-27J and C-130J originated in China and were sold through an offshore independent distributor. In a fourth example, suspect parts used on the Navy's P-8A again were traced to China and purchased through an independent distributor unauthorized by the OCM. The SASC opined that ''the risk of acquiring a counterfeit part [is] far higher when purchasing from an independent distributor than from a manufacturer or manufacturer's authorized distributor.''[25] From this finding flows the requirement of Section 818 (c)(3) that contractors shall obtain parts from ''trusted suppliers'' i.e., original manufacturers or their authorized dealers.

The Senate is correct, of course, that the best way for contractors to eliminate risk of purchasing a counterfeit electronic part is to limit sources of supply for electronic parts exclusively to OCMs, OEMS, and their authorized distributors. There are times, however, when parts are needed that no longer can be obtained from these sources. Independent distributors, even brokers, remain appropriate sources provided that due diligence is taken to assure their reliability and necessary documentation is obtained to demonstrate the pedigree of required parts.[26] There are reliable independent distributors, as distinguished from unscrupulous component brokers, Internet sources, and other suspect providers.[27] Some brokers have extremely high standards of quality assurance and can be used with confidence.

Today, it is not known how DOD will manage the ''trusted supplier'' program or what standards it will impose in the new DFARS regulating use of independent distributors or brokers. New standards are in development that should assist.[28] Where potentially unreliable sources of supply are required, companies should alert their customer and should take necessary steps to elevate supplier diligence, incoming inspection and test, and recurring quality measures to reduce vulnerability.

Detection and Avoidance: From the SASC report, it is clear that the best way to avoid counterfeit parts is to purchase only from sources of the highest reliability. However, when called upon to support systems with a long life cycle, when parts are out of production, or supplies from OCMs and their authorized distributors are exhausted, there may be no choice other than to purchase from outside the most secure channels, i.e., from independent distributors or brokers.[29] The challenge then becomes finding an affordable, realistic way to screen or conduct acceptance testing of parts.[30]

---

[22] Section 818(c)(2)(B) states that the costs of counterfeit electronic parts, and of rework or corrective action, are unallowable under DOD contracts.

[23] Observations developed during the internal review process can be employed as inputs to industry groups or in comments made to proposed or interim regulations. We urge companies to identify key areas of uncertainty in the meaning or implementation of the statute, key risk areas such as loss of necessary sources of supply, and areas of financial exposure or potential legal liability. The accumulation of such observations and experience may prove very helpful in persuading DOD and its supporting activities how it should enforce the law, and may prove helpful if legislative fixes are required.

[24] ''Buying parts in the independent distribution market can present significant risks.'' SASC Report, at 10.

[25] *Id.* at 16.

[26] The SASC did not prohibit use of independent distributors. The Report stated that ''[o]ne way to mitigate the risk of obtaining counterfeit parts from independent distributors is to audit potential distributors and develop a list of trusted suppliers.'' Id., at 10.

[27] Independent brokers can be a reliable source for needed parts. Confidence in this supply channel can be obtained through such steps as (i) requiring distributors to certify compliance with international Standards; (ii) confirming that distributors have screening and test systems and processes in place; (iii) assuring that a distributor is a member of respected industry organizations; (iv) checking on-line references; and (v) conducting personal meetings to verify controls and business responsibility. Many of these are suggested in ''10 Tips for Avoiding Counterfeit Components,'' an article by Dawn Gluskin, CEO of SolTec Electronics, appearing on-line at EBN on July 20, 2011, available at http://www.ebnonline.com/author.asp?section_id=1270&doc_id=231518 .

[28] In development is SAE AS 6081 ''Counterfeit Electronic Parts: Avoidance Protocol, Distributors'', about which information can be obtained via the SAE International website at http://www.sae.org/works/documentHome.do?docID=AS6081&inputPage=wIpSdOcDeTaIlS&comtID=TEAG19D, and SAE ARP 6178 ''Fraudulent/Counterfeit Electronic Parts: Tool for Risk Assessment of Distributors'', available at http://standards.sae.org/arp6178/.

[29] There will be situations where parts are needed that cannot be procured without using a higher risk source. Difficult choices are presented. Conceivably, an alternative may be to re-engineer a card or assembly to use new-build, high integrity parts. Or, a small production run could be ordered from a Contract Manufacturer or after-market parts fabricator. These can be very expensive alternatives, however, and slow to bring to fruition.

[30] SAE AS 5553-2009 ''Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition'', released in April 2009, and now undergoing a revision, is an important resource. The SASC Report states that several of the requirements of Section 818 are ''in line'' with SAE AS 5553. SASC Report, at 66. AS 5553 may be accessed through the SAE website at http://standards.sae.org/as5553/.

The SASC report, at 36, shows that some counterfeit parts may pass all ''production testing'' but nonetheless suffer from diminished reliability or harbor risk of failure when utilized in harsh, military operating conditions. For this reason, companies should take care not to assume lot sampling, or limited incoming inspection and test, will be sufficient to find all counterfeits. Companies also would be well counseled to identify and validate all in-house inventories, whether in materiel stores or engineering labs.

As the risk increases that counterfeit parts *might* be in the supply chain, the cost and complexity of determining whether a part is ''suspect,'' ''confirmed'' counterfeit, or acceptable increases. Counterfeiters are reported to employ increasingly sophisticated techniques to disguise the falsity of a part's marking or internal elements.[31] These are factors, again, which emphasize the comparative security of a narrowly controlled set of suppliers for a given part, and the importance of having access to sophisticated tools for counterfeit inspection, evaluation and test.

Issues involving avoidance of counterfeit parts can arise in many different situations. As indicated by the SASC report, a risk can arise where a higher-tier supplier is informed by an original component manufacturer (or its authorized distributor) that it is discontinuing production of a particular electronic part.[32] In such a situation, ''avoidance'' of future vulnerability to a counterfeit may require concerted action involving the OCM, OEM, authorized distributor, the higher-tier contractor or government customer, or even other third parties such as a contract manufacturer or other aftermarket fabricator. In addition, companies may opt to ''sunset'' products sooner if the assemblies are reliant on obsolete parts that are only available from untrusted sources.

Contractor Systems: The SASC report cites examples where, in the view of the SASC staff, companies were slow to recognize that product failures were traceable to counterfeits and instead treated potentially suspect failures as a ''due course'' warranty issue.[33] Also revealed was a lack of consistency in reporting and that, in some cases, reports were made but not to all interested or involved parties.

For example, in the case study about a suspected counterfeit memory chip in the Air Force C-27, the SASC report indicates that the contractor that learned of the counterfeit part reported it to the ERAI database and on GIDEP, both as required by that company's policy, but did not alert the prime contractor or the Air Force.[34] Nearly a year passed, according to the report, between confirmation of a counterfeit part and notification to the end use customer. From this example, and the SASC's criticism, a prudent contractor might conclude that when it has evidence confirming a counterfeit electronic part, it should identify at least the next higher tier contractor and take positive action to ensure that higher tier contractors and the end use customer receive prompt notice.

Companies will likely be expected to investigate thoroughly product failures or other indicators that suggest the presence of counterfeit electronic reports. The SASC was critical of less than immediate action, incomplete reporting, and failure to act aggressively when indications were present of a counterfeit part.[35]

Cost Accounting: Section 818's insistence that costs are unallowable, when incurred to replace counterfeit electronic parts and for remedial action, also follows directly from the SASC investigation. The SASC clearly was incensed that the government was charged costs to remove counterfeit devices from military systems. The report explained that Section 818 would ''[s]trengthen the incentive to avoid and detect counterfeit electronic parts by ensuring that the cost of replacing suspect parts is paid by contractors, not the government.''[36]

The Senate's ''hard line'' on cost recovery probably reflects a judgment that contractors should not be paid for costs that would not have been incurred in the first place, had responsible supply chain assurance been implemented. This position, while understandable, reflects an oversimplification of the problem.

Many causes contribute to counterfeit parts that enter into the supply chain. In a simple scenario, a contractor with lax supply chain controls may resort to an unvetted broker because of low price and convenience. There, it makes sense to make the contractor responsible for the costs because, in effect, they had a duty to avoid counterfeits and acts within their authority or control would have eliminated the risk and avoided the harm.

In real experience, however, contractors may have very little control over the situation and assignment of blame – and financial responsibility – seems misplaced. Many contractors support DOD systems long out of production for which numerous microelectronic parts are no longer available from an OCM, OEM or authorized distributor. The choice is either to purchase a part from a broker or refuse (or fail) to support the system. (Only in unusual cases will DOD customers pay for special manufacturing of out-of-production parts.) Sometimes, a government customer will *direct* a contractor to proceed with parts sourced from brokers, event after being informed of risk.[37]

It is wrong to make a contractor entirely responsible for costs where the contractor has informed the customer that it cannot acquire original or ''trusted source'' parts, alerted the customer of the risk of alternate sources, acted as directed by its customer, but where a counterfeit part nonetheless appears. (This can happen, as it is widely recognized that some counterfeiters employ very sophisticated means to defeat detection measures.) Applying the analogy above, the contractor would not be in breach of its duty, of due care to avoid use of counterfeit parts, as it had no ability to avoid risk of counterfeits, short of refusing to perform an order, and no reasonable alternative course of action to entirely eliminate the risk.[38]

[31] SASC Report, at 69.
[32] *Id.* at 46.
[33] *Id.* at 37.
[34] *Id.* at 39.
[35] *Id.* at 41.
[36] SASC Report, at 66.
[37] Also possible is that the government itself, for example through the Defense Logistics Agency, which has purchased millions of parts, may be an unknowing source of a counterfeit part. DLA's record of protection against counterfeit electronic parts is less than perfect.
[38] The House Armed Services Committee, in its action on the FY 2013 NDAA, included ''safe harbor'' language to protect contractors in these circumstances. Where a contractor (i) has a counterfeit parts system approved by DOD, (ii) acquires parts from an approved source or from DOD; and (iii) gives

  FCR ISSN 0014-9063

The rule of Section 818, that costs of counterfeits and remediation are unallowable, has caused higher-tier contractors, system and platform suppliers, to have concern about potentially very large cost exposure for risks they did not create and cannot entirely control. The statute does not, however, address accounting for costs of *compliance* – or for costs caused by the absence of necessary parts from trusted suppliers. Costs of compliance, inclusive of new systems, process and higher material costs, should be allowable. Claims activity may result from extra costs caused by absence of necessary original source parts, and (for example where new requirements produce additional, allowable costs not otherwise recoverable against fixed price contracts.

Industrial Base Implications. At lower levels of the supply chain, where many companies operate without CAS-covered contracts, there will be financial impact apart from any rule on the allowability of costs. Costs of detection, avoidance and elimination of counterfeits will impose both non-recurring and recurring expense. Customers rarely will volunteer to pay higher prices to cover those costs. More likely, higher tier customers will flow down new demands and controls, and insist that suppliers absorb costs and risks. This will cause considerable hardship on middle and lower tiers of the supply chain, and may cause some number of firms to exit the defense market rather than absorb unrecoverable new costs or assume enterprise risks.

When they sell to DOD contractors subject to Section 818, small companies that supply electronic parts, circuits, boards, harnesses, assemblies, or systems, are no less obligated to comply with Section 818 than their vastly larger customers. These smaller companies, however, may prove hard pressed to implement the required contractor systems and they almost surely will have limited financial tolerance for the costs of compliance, much less for the consequences of a counterfeit part that ''slips through.'' One can expect higher tier contractors to seek to shift liability downward by tougher purchase order terms and conditions. Small businesses rarely will have the leverage to resist these demands while remaining an approved supplier. Again, some will exit the DOD supply chain, complicating the ability of higher-tier companies to furnish necessary supplies and to comply with socioeconomic incentives that have encouraged, if not mandated, contracting with small business.

Of even greater concern is the possibility that commercial device suppliers, particularly those who conduct parts fabrication at various locations around the world for a global customer base, also will decide that the hazards and costs of compliance with Section 818 do not justify continuing to do business with companies in the U.S. defense supply chain. Since so many of the systems purchased and used by DOD depend on electronic parts, many of them of a commodity character and installed in commercial systems, the cost impact to DOD and its dedicated suppliers would be very great if commercial device sources opt out.[39]

Self-Examination is Context-Sensitive. Success in detection and avoidance of counterfeit parts requires a critical self-examination. The situations of companies in the DOD supply chain will vary widely as will the risk of their exposure to counterfeit parts and their responsibility for critical systems. While the new law states a goal (elimination of counterfeit parts from the defense supply chain) as well as a requirement (that contractors take responsibility to avoid, detect, and eliminate counterfeits), the application of the law will be very different across the dispersed landscape of suppliers and their vendors which constitutes the affected ''defense industrial base.'' Managing compliance, and working with DOD to assure responsible implementation, will be greatly facilitated by communication of insight and experience from many vendors. DOD should be careful not to attempt a ''one-size-fits-all'' approach to the regulations due this September.

Even before the new regulations are adopted, most companies can get a head start and ease their ultimate costs of compliance. There are key questions to consider: Where are our existing products at risk of counterfeits? What can we do to establish stronger vendor controls? Can we influence future designs and specifications to minimize exposure? What actions are necessary now to sample, inspect or test existing inventory? Do we have a disciplined approach to risk-based assessment to determine where counterfeits might be present and, if present, where the greatest harm could occur? Are present systems clearly defined to require reporting and remedial action, and do personnel understand these requirements? How can documentation of process and outcome be improved?

These issues should be addressed systematically. A risk-based assessment (as recommended here) ultimately is an expression of the analysis of many elements of objective data as are available within many organizations. (Such elements include, for illustration, date of parts design, age of part in inventory, whether part is purchased from OCM or broker, presence of supporting documentation, criticality of part or system, historical device reliability record, date of most recent supplier audit, design life of part, results of inspection and test, and so forth.) Larger companies, either indigenously or with the assistance of outside consultants, will be able to devise information processing systems that will collect and maintain this information and apply it to generate risk profiles and control actions and dispositions in light of evaluated risks. Indeed, Section 818 appears to anticipate just such an outcome, since the law, at Section 818(e)(B), requires DOD to ''establish processes for the review and approval of *contractor systems* for the detection and avoidance of counterfeit electronic parts and suspect counterfeit electronic parts,'' and treats such processes as comparable to other, already regulated ''business systems.'' (Oversight of new counterfeit parts systems may be combined with

timely notice if a counterfeit or suspect part is identified, then costs to replace the counterfeit or for rework would not be unallowable. The Senate, as of this writing, however, has not agreed to this relief.

[39] For now, small businesses are urged to assess current products, customers, and requirements; evaluate supply chain sources, record & risk; eliminate sources of uncertain pedigree; notify customers if parts are unavailable or foreseen as such; identify potential standards and best practices; engage with relevant industry and trade associations; examine expected cost impact (recurring, non-recurring) of compliance, advise government customers and primes of expected cost and performance impact, and coordinate with other businesses similarly situated for shared advocacy or common systems.

existing business system review mechanisms in order to reduce costs.)

At lower tiers, compliance raises different concerns. Where a company furnishes boards, assemblies or completed devices, it may have little control over the design and have limited access to OCMs and OEMs. Qualification of trusted suppliers, while laudable, may present cost and capability challenges that exceed the ability of some companies to absorb. One can anticipate situations where mid-tier companies find they cannot supply parts to maintain current products because they cannot locate, qualify or afford the necessary parts from ''trusted suppliers'' or implement a testing regime sufficient to remove all doubt. Similarly, one can expect the new law to suppress what once was a thriving market of dubious brokers and traders of doubtful pedigree. While this is desirable, it is all too easy to envision that the same controls will give reputable independent distributors cause to question whether they can fill orders for parts not otherwise available, especially if a ''flow down'' from higher tier suppliers would cause them to assume risks and costs of remediation should a counterfeit part be discovered at the higher assembly or system level. It should not be forgotten that independent distributors, and brokers, exist because there is a continuing demand for needed parts that are not available from the original or ''best'' sources.

Conclusion. There will be no shortage of variation and complication in questions that arise from Section 818 and its implementation. Even though industry recognizes the threat posed by counterfeit electronic parts and endorses the aims of the new law, costs, uncertainty, and disruption are an inevitable consequence of legislation attempting to impose a ''new order'' for what is and will remain a global problem. Should DOD proceed ''aggressively'' to implement new regulations without industry input, it likely will solve some of the problem, but it can expect many unintended and costly consequences, disruption to the industrial base, and potentially a volume of controversy, complaints, and claims. Imposing a ''strict liability'' regime will punish those who experience counterfeit electronic parts, but that may not be an outcome ultimately in DOD's interest, taking into account the complexity of the problem and the many actions that must be coordinated among many actors to address this serious problem. A better course, accepting entirely the importance and positive purpose of the new law, is to proceed carefully with implementation, to receive inputs from all stakeholders, and to impose new rules and requirements in a responsible, risk-driven sequence.

FCR ISSN 0014-9063