I offer this submission as an elaboration upon the statement that I provided during the public meeting held by DoD on June 28, 2013 on the proposed rule, entitled “Detection and Avoidance of Counterfeit Electronic Parts,” DFARS Case 2012-D055, published in the Federal Register on May 16, 2013 (the “Proposed Rule”).

I am an attorney in private practice with the law firm of Rogers Joseph O’Donnell, PC. I have written and spoken extensively on counterfeit parts prevention. I am a Vice-Chair of the Supply Chain Subcommittee of TechAmerica, and a member of the Counterfeit Parts Task Force of the ABA Section of Public Contracts Law. However, the views I express here are my personal views, only, and do not reflect those of TechAmerica, or the ABA, or any client that I or my firm represent or advise.

I. Context of the Proposed Rule

As was exposed in 2011 and 2012 by the work of the Senate Armed Services Committee, the threat of counterfeit electronic parts was not taken seriously enough by some in industry, or by DoD itself. The result was Section 818 of the National Defense Authorization Act of 2012 (NDAA), Pub.L. 112-81, Dec. 31, 2011. The law acts upon many “junctures” of the supply chain. For present purposes, the most important are purchasing practices, inspection and testing, reporting, corrective measures, contractor systems and sanctions.

In Section 818, Congress directed DoD to issue new regulations governing contractors before the end of September 2012. The proposed DFAR emerged on May 16, 2013, seventeen months after enactment and nearly eight months later than Congress intended.

While the objectives of Section 818 are fairly plain, and its purposes widely supported, implementation is very complex. As was evident from the remarks made at the public session of June 28, 2013, perspective often varies and is informed by where a particular actor resides in the supply chain. The perspectives of higher tier DoD contractors differ significantly from the concerns of middle tier companies. Even greater divergence is evident as one considers the viewpoint of supply chain participants who are very important though not subject to Cost Accounting Standards (CAS) – such as distributors and brokers, small business, and commercial sources. As DoD recognizes, to its credit, it is most important to consider the breadth and depth of the supply chain in fashioning rules to implement Section 818 and to avoid unintended and harmful consequences as well as costs that might overwhelm the value of Section 818 rules.
By definition, the supply chain is both very broad and very deep. The supply chain is global, in that necessary electronic parts come from international sources. Also, DoD has only limited influence over the supply chain and must be careful not to isolate defense needs from commercial sources of technologies and innovation. The “supply chain” extends to a vast array of hardware and systems, products and services. It encompasses not only microelectronic devices but the software and firmware that drive those devices. The threat ranges from crude fakes to very sophisticated “cloned” parts that might harbor malicious code.

Thus, the implementation of Section 818 must be context-sensitive. DoD is to be commended for its apparent recognition that it should neither go “to far” or insist upon “too much” in these regulations. “Prescriptive” regulations, that attempt to impose “one rule” to fit all circumstances, are to be avoided. In the Proposed Rule, however, DoD has not yet gone far enough to inform industry of how it is to comply with Section 818’s key requirements.

Section 818 makes large defense contractors responsible to detect and avoid and (if possible) eliminate counterfeit parts and it is accompanied by various sanctions to drive home these obligations. Sanctions include disallowance of the costs of replacing counterfeit electronic parts and suspect counterfeit electronic parts – as well the costs of rework or corrective actions. The law also requires DoD’s largest contractors to adopt systems to detect and avoid counterfeit electronic parts. Industry – naturally – wants guidance on how to conform to the law’s requirements, minimize or mitigate exposure to disallowed costs or other sanctions, and on compliant systems and processes. DoD should share in these objectives, yet the Proposed Rule does little to inform industry. The Final Rule can do more, without doing too much.

The statute recognizes that a risk-based approach is appropriate for DoD’s own efforts to avoid counterfeit electronic parts and DoD has implemented such a strategy in its Counterfeit Parts Prevention policy, DoDI 4140.67, released on April 26, 2013. Yet the Proposed Rule imposes “strict liability” upon covered contractors, irrespective of their compliance efforts and without regard to any “fault.” This imposes both costs and risks upon industry, and discourages responsible Government participation in management of supply chain practices where risks are identified or identifiable. In the Final Rule, DoD would be well-counseled to implement Section 818 through accommodation of reasonable and different business practices, relying upon established industry standards, and delegating decision-making to contractors. DoD should not attempt to impose a technical orthodoxy upon such a dynamic and diverse industrial base.

II. The Proposed Rule Should Focus On Where the Supply Chain is Vulnerable

The Proposed Rule, at a high level, imposes new obligations on large DoD contractors, i.e., those covered by the CAS. It does not distinguish between the comparatively low risk of counterfeit parts being acquired from “trusted sources,” as these are identified by the statute, at Section 818(c)(3), and the comparatively higher risk when parts are acquired from other sources, such as distributors and brokers, to whom resort may be necessary for supply when the desired part is out of production, obsolete or no longer available from the “trusted source.” Nor does the Proposed Rule recognize the comparatively low risk of a counterfeit electronic part that is a “Commercial Off The Shelf” (COTS) item when it is purchased from the original source or an authorized distributor – or off a GSA Schedule. Though these supply chain “vectors” carry low risk, they
are subject to the Proposed Rule, on a strict liability basis. In contrast, commentary preceding the Proposed Rule suggests that DoD did not intend the rule to apply directly to small businesses and the treatment of “flow down” obligations leaves uncertain whether primes can apply requirements of the Rule to the host of smaller sources, including brokers and distributors, who are active supply chain participants but not CAS-covered.

If the “primary market” for electronic parts is from OCMs, OEMs, authorized distributors and COTS suppliers, the “secondary market” includes specialized sources, such as brokers and dealers, and intermediate and small business suppliers. This “secondary market” is more vulnerable to counterfeit electronic parts. Yet, the Proposed Rule does not inform covered contractors on what standards they should apply when purchasing parts from sources in the secondary market. As explained below, the statute envisioned that DoD would define how to qualify “additional trusted suppliers” who could be used with confidence when parts are unavailable from “trusted suppliers,” but the Proposed Rule offers no help in this regard.

Where the supply chain is vulnerable, of course, in part is a function of where demand exists that cannot be satisfied by parts purchased from sources of highest assurance. Vulnerability can be created in several different ways.

- One is the situation where DoD seeks to sustain equipment built years ago where the needed parts are out-of-production or obsolete. The risk is frequently present that such parts only can be furnished by distributors and brokers – and so the Proposed Rule, to deal with this vulnerability, ought to give more information to guide both the companies who buy from these sources and to govern the expected conduct of these sources. (But it does not).

- Vulnerability also is created when Government acquisition priorities and practices discourage or even preclude buys of parts from high-assurance sources. This occurs – frequently if not systemically – as a consequence of Government insistence upon “least cost” practices for system sustainment and from the preference for “lowest cost, technically acceptable” (LPTA) acquisition. Both work against the very interests that the Government supposedly seeks to promote through the counterfeit parts prevention rules. The impact of these acquisition practices is to steer purchases away from high-assurance sources whose prices are higher in reflection of greater investment and expense to assure parts authenticity, traceability and specification compliance.

Where these converge is in the absence of standards and practices as DoD might require, for purchases from the “secondary” market, but does not. It is impossible to eliminate a continuing requirement to purchase from distributors and brokers and it is necessary to make the Rule inclusive of responsible small business participation. The correct answer is neither to impose impossible standards upon secondary sources, or absolute liability upon prime and high tier contractors who must purchase from these sources, any more than it is to give a “free pass” to parts that happen to come from a small business. Rather, the Final Rule should recognize the great progress made by standards-setting bodies, such as SAE, and encourage contractors to adopt and conform to these standards as they evolve. And, specifically, the Final Rule should encourage, if not require, covered contractors to impose known industry standards, such as SAE
AS5553a, AS6081 or AS61711, on their “secondary” market sources and small business suppliers. While this decision will impose additional responsibilities and costs on these sources, this may be a necessary burden if counterfeits are to be avoided at all levels of the supply chain. Moreover, there already is evidence that some small businesses and certain distributors and brokers are working hard to implement these standards, in order to earn the status of an “additional trusted supplier” as contemplated by the Statute. Those companies who make the investment and commit to highest level of product assurance practices should be encouraged by DoD’s purchasing practices, and the flow-down requirements of the Final Rule, and not “punished” because their products come at a somewhat higher price.

III. Where The Proposed Rule is a Disappointment

Congress, in enacting Section 818, required DoD to issue regulations to cover key areas of contractor responsibility to detect and avoid counterfeit electronic parts. In several key areas, the Proposed Rule falls short of answering the statute’s assignments.

1) A definition of “counterfeit” and “suspect counterfeit” part. Section 818 (b)(1) requires DoD to establish “Department-wide definitions of the terms ‘counterfeit electronic part’ and ‘suspect counterfeit electronic part.’”

There are several problems with the proposed definition. The principal problem is that the first part of the definition does not incorporate a “fault” element and thus does not distinguish between actors who intentionally misrepresent the authenticity of a part, on the one hand, from persons who may unknowingly, and despite all due diligence, nonetheless pass on a part that proves to be counterfeit.

The structure of Section 818 and the Proposed Rule is that adverse cost and liability consequences attach to contractors should they deliver parts that are defined as “counterfeit electronic parts” or “suspect counterfeit electronic parts.” Contractors are required to report the discovery or suspicion of counterfeit parts, and must implement systems to detect and avoid counterfeit electronic parts, which systems are subject to Government review and approval. Thus, the operation of the law and the Final Rule will depend greatly upon what is finally defined as a “counterfeit” or “suspect counterfeit part” and it is here that DoD can act to mitigate the potentially harsh but avoidable consequences of a strict liability regime as otherwise might apply. Should DoD revise the core definition of a “counterfeit” part to be one that is “knowingly or recklessly” misrepresented, as specified and genuine, the regulation as revised would provide some protection contracting parties who have taken all responsible or required acts to detect and avoid counterfeit parts.

Another issue with the first part of the definition is that it includes an unnecessary second part – an “item misrepresented to be an authorized item of the legally authorized source” – that raises many questions of interpretation and could exclude supply from bona fide distributors or brokers who acquire excess and out of production authentic parts. These sources, from the “secondary” market, remain vital to the supply chain. It is unclear whether the definitions accommodate any distributors other than those who have some license or contractual relationship with the original authorized source.
The third part of the proposed definition treats as a counterfeit part a “new, used, outdated, or expired item procured from a legally authorized source that is misrepresented by any source to the end user as meeting the performance requirements for the intended use.” This would characterize as “counterfeit” even items newly made by original manufacturers that happen to fail an acceptance test. Ordinary quality problems should not be treated as “counterfeit” parts. This part of the definition should be removed.

2) **Strengthening contractor purchasing practices.** This is addressed by Section 818(c)(3). The requirement is that contractors—“whenever possible”—“obtain electronic parts that are in production or currently available in stock from the original manufacturers of the parts or their authorized dealers, or from trusted suppliers who obtain such parts exclusively from the original manufacturers of the parts or their authorized dealers.”

The Final Rule should clarify how industry is to identify the “trusted suppliers” for parts that are in production or available from authorized dealers. However, industry knows that electronic parts should be purchased from OCMs and their authorized distributors. But this is not always possible as there are thousands of systems in the inventory for which parts remain in demand but are not available from such “trusted suppliers.”

Section 818(c)(3)(B) says that where electronic parts are not in production or currently available in stock from original sources, they are to be obtained “from trusted suppliers.” The law also directs DoD to “establish requirements for notification” and for “additional inspection, testing and authentication” of parts that are obtained from other than the “trusted suppliers.” The Proposed Rule does not offer guidance on these points—and it is needed. Nor does the Proposed Rule offer information to implement Section 818(c)(3)(C), which calls for qualification requirements for DoD to identify “trusted suppliers that have appropriate policies and procedures in place” to avoid counterfeit electronic parts.

The Proposed Rule also is silent on Section 818(c)(3)(D), which calls for DoD to authorize contractors and subcontractors to identify and use “additional trusted suppliers” provided that the standards and processes comply with established industry standards and the contractor or subcontractor “assumes responsibility for the authenticity” of parts provided by such suppliers. This last omission is especially important. For covered contractors to continue to support DoD systems where required parts are out of production or obsolete, those contractors must be able to qualify and purchase from “secondary” market sources, such as distributors and brokers. DoD should seize upon the authority of Section 818(c)(3)(D) to delegate to covered contractors the authority to define and impose requirements upon their “secondary” sources that reflect contemporary processes and evolving industry standards.

In its present form, the Proposed Rule does little more than repeat the words of the statute. This leaves unresolved crucial questions faced by DoD’s covered contractors thousands of times a year. If DoD intends to make the force of the rule felt upon its largest contractors, then at least it should authorize and delegate to them to apply industry standards to the identification and qualification of the necessary “additional trusted suppliers.”
3) **Improvement of contractor systems.** Section 818(c)(2)(A) makes contractors “responsible for detecting and avoiding the use or inclusion of counterfeit electronic parts.” For this purpose, Section 818(e) requires DoD to implement a program to “enhance contractor detection and avoidance of counterfeit electronic parts.” There are nine (9) specified elements to such a program, identified by Congress as -

- Training – inspection and testing – processes to abolish counterfeit electronic parts proliferation – improved traceability of parts – use of trusted suppliers – reporting and quarantining of counterfeit parts – methodologies to identify suspect parts and rapidly determine if a part is counterfeit – enhanced systems to detect and avoid counterfeit electronic parts – flow down to subcontractors – and review and approval of contractor systems.

Here again, the Proposed Rule does nothing more than recite – word for word – the relevant provisions of the statute. No additional dimension or detail is provided. Nowhere does the Proposed Rule indicate how to determine whether a system is “acceptable.” Nor does the Proposed Rule inform industry as to how to evaluate the adequacy of such a system, or what role industry standards may play.

The prudent course for DoD is to recognize that it must enable its largest contractors to take the lead in detection and avoidance of counterfeit electronic parts. Each contractor is in the best position to make risk-based decisions on how best to implement supply chain assurance measures. DoD should endorse contractor use of industry standards and allow for a flexible, but accountable response at implementation of contractor systems. This will allow for adaptive and responsive implementation of prevention measures, by contractors, and reduce the oversight burden that otherwise could fall upon DoD.

Many crucial decisions, regarding counterfeit risk mitigation, will require at least notification to the customer if not the active participation of the customer in choices among competing choices of varying costs and risks. Especially because the law and regulations expose contractors to great potential liability if a counterfeit is found in a system, DoD should take a more proactive approach to working with contractors to help define, assess, qualify and verify systems to prevent counterfeit electronic parts.

4) Congress was insistent on **improved reporting** by DoD and industry. At 818(c)(2), the law requires DoD to revise regulations to require DoD contractors to report in writing within 60 days to “appropriate Government authorities” and GIDEP whenever a contractor “becomes aware, or has reason to suspect” a counterfeit.

It is through reporting that industry and government inform each other of known risks and identified threats. Reporting helps to establish “threat vectors” and to mitigate or avoid potentially harmful effects. But reporting is essentially ignored by the Proposed Rule. A FAR Case, 2013-002, will address reporting – but it remains pending. In contrast to many other areas of counterfeit parts prevention, where industry has moved out to improve its practices while waiting for DoD, reporting is an area where little has been accomplished, since enactment of Section 818, because of the importance of the Government’s role.
As an urgent matter, DoD should conduct a review of reporting to the GIDEP system since enactment of the NDAA. Today, industry relies upon a “patchwork” of private and public reporting systems (such as ERAI). There is anecdotal information that reporting trends to GIDEP do not match those to ERAI, and that reporting to GIDEP after enactment of Section 818 has actually fallen. Considering the greater sensitivity to the threat of counterfeits that followed NDAA enactment, a reduced rate of GIDEP reporting afterwards is an indicia of failure of the reporting system.

5) Another crucial subject, contractor responsibilities for costs, is at Section 818(c)(2)(B):

“The costs of counterfeit and suspect counterfeit electronic parts and the cost of rework or corrective action that may be required to remedy the use or inclusion of such parts are not allowable costs under Department contracts.”

A new contract cost principle is proposed to address the cost of “remedy” for use or inclusion of counterfeit electronic parts. The reach of costs excluded is not defined – as the proposed regulation does no more than restate the terms of Section 818(c)(2). Also, as drafted, the cost principle could apply beyond those “covered contractors” who are subject to the Cost Accounting Standards. (This was the intent of Section 818.) This is because proposed 231.205-71(c), which disallows costs of counterfeit and rework, is not expressly limited to CAS-covered contractors, as is 231.205-71(b).

DoD should take a judicious approach to the treatment of costs arising from Section 818. As a threshold matter, both recurring and non-recurring costs of implementation of contractor systems to detect and avoid counterfeit parts surely must be allowable, as these are both “reasonable” and now “necessary” costs of doing business. Similarly, allowable costs must include any price increment that a covered contractor pays to have higher assurance of authenticity when it purchases from sources in the “secondary” market, and for the same reasons contractors should not face question when they employ additional inspection and testing to verify the authenticity of parts they purchase from such “additional trusted suppliers.” For the same reasons, contractors should have confidence that the costs they may incur, in the investigation of a “suspect” part, will be allowable if the contractor makes a reasonable final determination that the part is not “counterfeit” – even if a failure or test discrepancy was the original cause for investigation.

IV. Key Recommendations

a. Definitions

The definition should incorporate an “intent” element and be revised to recognize that a part is “counterfeit” where it has been “knowingly or recklessly misrepresented.” Recognition of “intent” would make the definition consistent with the relevant industry standards, SAE AS5553a, in its current form. DoD also should seek to conform the DFARS definitions to those of other federal agencies, such as DHS and NASA, and with its internal documentation, such as DoDI 4140.67, the Counterfeit Prevention Policy. Ideally, common definitions will apply internally and externally and these will align with those used by authorities charged with protection of intellectual property and criminal enforcement.
The Final Rule should eliminate that language of the proposed *definition* that could cause an ordinary quality problem to be treated as a “suspect” or “counterfeit part.” The definition also should accommodate the market participation of qualified brokers and distributors. Care should be taken not to employ definitions that have an anti-competitive impact by giving excess market power to original sources, and which will accommodate post-manufacture item-unique identification methodologies as the Government may choose to deploy.

b. Purchasing Practices

Apart from the text of the Final Rule itself, DoD is strongly encouraged to examine how its own purchasing practices frustrate the objectives of NDAA Section 818 – especially those that appear to “reward” lowest cost materiel acquisition and therefore “punish” higher prices that may come with higher assurance of authenticity. A realistic view of the greater vulnerability posed from the “secondary” market should lead DoD to encourage its covered contractors to spend a little more to reduce risks of counterfeits – and this expense is one that should be paid by DoD as its part of doing business in accordance with Section 818.

The Final Rule also should provide more guidance on purchasing decisions that contractors and their DoD customers should make where parts are required that now are obsolete, out of production or cannot be obtained from “trusted suppliers.” A mechanism should be considered for contractors to identify alternatives when stated requirements will require purchase of obsolete or out of production parts, or unavoidably from sources of potential risk. Contractors should be encouraged to recommend alternatives to their customer – and should have a right to expect direction from each customer as to how to proceed. DoD should accept its responsibility for situations where it has been informed of risk in a particular parts procurement but DoD declines to authorize redesign or contract manufacture and instead leaves its contractor with no choice other than to use a broker or distributor that has not been qualified as an “additional trusted supplier.”

DoD also should integrate recognition of its existing “trusted foundry” and “trusted supplier” programs, and the emerging qualification programs of DLA (for distributors and test providers), so that due consideration is given for use of these special alternatives where justified and where funds are available.

c. Industry Standards

The Final Rule should give more formal recognition to the accomplishments of government and industry experts in the development and continuing refinement of industry standards and best practices. Section 818(c)(3)(D)(ii) provides that the “standards and processes” for identifying additional trusted suppliers, i.e., those used where parts are not available from original sources, are to “comply with established industry standards”. *Covered contractors* should know they are on solid ground if they perform diligence of their suppliers, including distributors, by reference to such standards. Further, covered contractors should be assigned the responsibility to qualify “additional trusted suppliers” in reliance upon these standards.
Similarly, where DoD adopts a standard for its internal use, the Final Rule should extend a presumption of validity to use by the private sector. In this way, industry can organize its compliance around the standards. This will answer many presently open questions about test and inspection methods, qualification of distributors and notification to government and industry when counterfeits are discovered. Reliance upon industry standards also is a sound way for DoD to enable its covered contractors to take responsibility to fulfill the objectives of NDAA Section 818 without unnecessarily intrusive or burdensome rules.

d. A Separate Contractor System

The Final Rule should treat prevention of counterfeit parts as a separate contractor business system rather than attempt to regulate counterfeit parts prevention through the existing DFARS treatment of purchasing systems. DoD should take the time to develop DFARS coverage that is specific to counterfeit parts detection and avoidance. The approach of the Proposed Rule, while expedient, is not ideal. Purchasing is a component of supply chain risk management, but there are many other relevant functions – such as design, engineering, quality assurance, materiel management and accounting and compliance – that are outside purchasing. Should DoD withdraw purchasing system approval, after a counterfeit incident, it literally would stop a major contractor in its tracks – even if the counterfeit intrusion had nothing whatsoever to do with purchasing practices.

e. Commercial Items

In the Final Rule, DoD needs to reconsider how it will treat COTS and commercial items, and (for similar reasons) items purchased off a GSA Schedule. The risk of a commercial off-the-shelf (COTS) part being counterfeit, where purchased directly from an original source, is comparatively very small. In contrast, there is potentially severe industrial base and supply chain impact should DoD attempt to force this Rule upon commercial device makers. The final Rule should specifically exempt COTS items purchased directly from OCMs, OEMs and their authorized distributors, as well as purchases from these sources via GSA schedules, and should accept commercial warranties and other standard commercial assurances of authenticity or provenance.

f. Small Business

The Final Rule must confront the problem of how to apply counterfeit-prevention objectives to small business. Introductory comments to the Proposed Rule indicate that the rule does “not apply to small entities as prime contractors” and that there is only a “negligible” impact on small entities in the supply chain. This is misleading, because the CAS-covered contractors, to whom the Proposed Rule does apply, are required to flow down “counterfeit avoidance and detection requirements” to all subcontractors. E.g., Proposed Rule 246.870–2(b)(9). Some small businesses have responded to Section 818 by making the investments necessary to comply. These should be rewarded and their participation in the defense supply chain should be encouraged. That can be achieved to imposing standards that flow down to all tiers of the supply chain, including small business suppliers. Some may find they cannot or will not participate, but others will participate and they will do so with greater assurance that counterfeits are avoided.
At the same time, there are signs in the marketplace that some necessary small businesses (and other sources) will refuse to accept flow-down of 818 requirements. This may stem from business decisions not to accept extra costs and risks for that portion of the marketplace represented by DoD purchases. Another cause may be that the extent or risk of liability, especially if it includes costs of system rework or “restitution” where a counterfeit escape occurs, is just too great to make business sense to companies (defense-oriented or not). DoD will need to fashion some form of “safety valve” to deal with the situation where the only sources of required parts refuse to accept flow-down and will not agree to conform to risk-mitigation industry standards as suggested above. Analytically, DoD should be just as concerned about the impact of a counterfeit from a small business as from a large contractor. But important socio-economic policies are served by small business participation requirements. Time will be needed to find the balance between achievement of these policy objectives and affordable, necessary requirements to avoid receipt of counterfeit parts from small business sources.

g. **Risk-Based Approach**

NDAA 2012, at Section 818(b)(2), directs the DoD to implement a “risk-based approach” to deal with the risk of counterfeits in its own purchasing practices. DoD already has implemented this strategy in DoDI 4140.67, its Counterfeit Prevention Policy. The same strategy should be extended to industry in the Final Rule.

A “risk-based approach” recognizes that it is impossible to eliminate all risk of counterfeit in every system that the DoD buys or supports. A risk-based approach gives priority to prevention efforts where the presence of a counterfeit part would do the greatest harm, to personnel safety or to operations, so that those systems and uses can be given special attention. The Final Rule should address how DoD will work with its suppliers to design, implement and operate a responsible, risk-based approach to the detection and avoidance of counterfeit electronic parts.

Respectfully submitted:

Robert S. Metzger  |  Shareholder
ROGERS JOSEPH O’DONNELL | a Professional Law Corporation
750 Ninth Street, N.W., Suite 710 | Washington, D.C. 20001
202.777.8951 direct  |  202.777.8950 main  |  213.880.4224 mobile

311 California Street, 10th fl | San Francisco, CA 94104
415.365.5355 direct - SF | 415.956.2828 main | 415.956.6457 fax
rmetzger@rjo.com
www.rjo.com