Testimony of Robert S. Metzger June 28, 2013
DoD Public Meeting
DFARS Case 2012-D055 (Detection & Avoidance of Counterfeit Electronic Parts)

INTRODUCTION

I appreciate the opportunity to speak before this hearing. My name is Robert Metzger. I am an attorney in private practice with the law firm of Rogers Joseph O'Donnell. My firm specializes in public contracts law and has 32 years' history of involvement in this area. I manage our new Washington, D.C. office.

I have written and spoken extensively on counterfeit parts prevention. A list of publications is at the end of my prepared testimony. I am the Co-Chair of the Supply Chain Subcommittee of TechAmerica, and a member of the Counterfeit Parts Task Force of the ABA Section of Public Contract 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.

WHY WE ARE HERE

Had all in the defense industry been more alert to counterfeit parts, Congress would not have found it necessary to legislate supply chain risk management. But – as was exposed in 2011 and 2012 by the work of the Senate Armed Services Committee – the threat of counterfeit electronics was not taken seriously enough by some in industry. Nor did DoD itself have an effective plan.

The result was Section 818 of the National Defense Authorization Act of 2012 – a law that acts upon many "junctures" of the supply chain. These include *detection, exclusion*, *enforcement*, *purchasing practices*, *inspection and testing*, *reporting, corrective measures*, *contractor systems* and *sanctions*. Our concern today is with the use of the government's *acquisition* and *oversight* powers to enforce and apply Section 818.

In Section 818, Congress directed DoD to issue new regulations governing contractors before the end of September 2012. On May 16, 2013, nearly eight months late, the proposed DFAR, Detection and Avoidance of Counterfeit Electronic Parts, was issued for comment. Responses are due on July 15, 2013.

WHY THIS HAS TAKEN SO LONG

While the objectives of Section 818 are fairly plain, and its purposes widely supported, implementation is very complex. There are risks of unintended and harmful consequences, and 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 created by criminals to very sophisticated "cloned"

parts that might harbor malicious code. In this sense, the implementation of Section 818 is very context dependent. DoD has earned some credit in that it did not attempt to impose one rule to fit so many situations. Especially here, *slow* regulations are better than *bad* regulations. The very broad statute, if combined with pervasive implementation, and overzealous enforcement, would have very negative and costly effects upon industry and DoD alike.

While industry has complained about the slow pace of DoD's implementation of Section 818, it is undoubtedly true that industry leaders at all tiers have worked diligently and effectively to improve counterfeit parts detection and avoidance, rather than waiting for the "shoe to drop" when final 818 regulations apply. Many of the goals of 818 are being achieved, practically, by responsible contractors. In the implementation of the Section 818 Rules, the efforts of these leaders should be credited, as a way to incentivize the self-directed initiative of other companies.

DoD may be well-counseled to implement 818 through *accommodation* of reasonable and different business practices, rather than by attempting to impose a technical orthodoxy upon such a dynamic and diverse industrial base. But DoD must take a leadership role.

THE PROPOSED RULE IS A MAJOR DISAPPOINTMENT

Taking all this into account, the proposed rule is a major disappointment. Fundamentally, the Rule focuses mostly on the larger contractors, where the risks are comparatively less, while giving essentially no guidance on how to deal with the high risk areas – namely, purchases of obsolete and out-of-production parts and purchases from small businesses who may lack avoidance systems or discipline.

Congress, in enacting Section 818, required DoD to issue regulations to cover key areas of contractor responsibility to detect and avoid counterfeit electronic parts. Congress imposed a "strict liability" regime, making contractors liable for the costs of replacing counterfeit parts and for rework, even if "best efforts" and "best practices" were employed. The regulations to implement Section 818 – at the very least – should have done as Congress directed, *by informing* industry of what it must do to be compliant with the law.

In five (5) key areas, the Proposed Rule fails against this basic standard.

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', which definitions shall include previously used parts represented as new"

One part of the definition, in the Proposed Rule, 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." (Emphasis added.) This definition must be corrected, as it would treat as "counterfeit" even items newly made by original manufacturers that happen to fail an acceptance test.

The Proposed Rule also contains a problematic definition of a "suspect" counterfeit part – "a part for which visual inspection, testing, or other information provide *reason to believe* that a part

may be a counterfeit part." This leaves more to be resolved than it answers. Under the law, costs of "suspect" as well as confirmed counterfeit parts are unallowable. A "suspect" counterfeit part should be one where there is evidence of third party intent to misrepresent or mischaracterize a part, its provenance or its performance. Costs to remedy ordinary defects should not be disallowed because of an initial suspicion that the part might be "counterfeit."

2) ***Strengthening contractor purchasing practices***. This is addressed by Section 818(c)(3):

> "Whenever possible," the law says, contractors "at all tiers" are to "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."
>
> Where electronic parts are *not* in production or currently available in stock from trusted suppliers, the law requires they be obtained "from trusted suppliers" (though it does not define who these might be). When parts are not available from one of the original sources, the law directs DoD to "establish requirements for notification" and for "additional inspection, testing and authentication."
>
> The law also requires DoD to establish standards and processing for identifying those "trusted suppliers" from whom parts are purchased when not bought from original sources – and these trusted suppliers are to comply with "established industry standards."

The Proposed Rule does little more than repeat the words of the statute. Industry *knows* that electronic parts should be purchased from OCMs and their authorized distributors – where possible. The crucial *problem* is that there are thousands of systems in the inventory for which parts necessary for sustainment are ***not*** available from such "trusted suppliers." The Proposed Rule does not tell industry what to do when it requires an *obsolete part* to support a system and that part is not available from one of the ideal sources. Nothing is said as to the notification to be made to DoD, or DoD's responsibility when it receives such notification, or what additional test and inspection is required to qualify either a supplier or a part.

3) ***Improvement of contractor systems***. This requirement appears at Section 818(e):

> DoD is 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, the Proposed Rule does nothing more than recite – word for word – the relevant provisions of the statute. Nowhere does the Proposed Rule indicate how to determine whether a system is

"acceptable." Nor does the Proposed Rule inform industry as to "who" will evaluate the adequacy of such a system, and there is little explicit as to the process that will be used to review and qualify a system. What is especially disappointing is that the successful functioning of a counterfeit parts avoidance *system* requires communication and cooperation between industry and DoD customer

Many crucial decisions, regarding counterfeit risk mitigation, should be made in consultation with the customer. 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 revised regulations are 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.

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 reach beyond those "covered contractors" who are subject to the Cost Accounting Standards. (This contravenes 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).

KEY RECOMMENDATIONS

First, the Rule should eliminate that language of the **proposed definition**, at 202.101(3), that could cause an ordinary quality problem to be treated as a "counterfeit part." The definition of "suspect" counterfeit part should be revised to include evidence of third party intent to misrepresent or mischaracterize a part, its provenance or its performance.

Second, the Rule should provide more guidance on **purchasing decisions** that contractors and their DoD customers should make where required parts are obsolete or cannot be obtained from

"trusted suppliers." A mechanism should be considered for contractors to identify requirements that call for obsolete parts. Contractors should be encouraged to identify risks and recommend alternatives to their customer – and should have the benefit of customer direction as to how to proceed. DoD also should integrate recognition of its existing "trusted foundry" and "trusted supplier" programs, so that due consideration is given for use of these special alternatives where justified and where funds are available.

Third, the Rule should follow the lead of the statute by giving formal recognition to the accomplishments of government and industry experts in the development 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". *Purchasers* should know they are on solid ground if they perform diligence of their suppliers, including distributors, by reference to such standards. Similarly, where DoD adopts a standard for its internal use, the Rule should extend a presumption of validity to use by the private sector. In this way, industry can organize its compliance around the standards, and this will answer many of the presently open questions about, for example, test and inspection methods, qualification of distributors and notification to government and industry when counterfeits are discovered.

Fourth, the Rule should treat prevention of counterfeit parts as a **separate contractor system** rather than attempt to graft elements of counterfeit parts prevention onto 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. This is a disproportionate response that may have little to do with the source of a counterfeit "escape."

Fifth, DoD needs to reconsider how it will treat **commercial items**. The risk of a commercial off-the-shelf (COTS) part being counterfeit, where purchased directly from an original component manufacturer (OCM), original equipment manufacturer (OEM) or authorized distributor, 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 and should accept that DoD's interests are satisfied by receipt of their commercial warranties and any other standard commercial assurances of authenticity or provenance.

Sixth, the 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). While some small businesses have responded to Section 818 by making the investments necessary to comply, there are signs in the marketplace that other small businesses refuse to accept flow-down of 818

requirements. Analytically, DoD should be just as concerned about the impact of a counterfeit from a small business as from a large contractor. Hence, for certain procurements, DoD may need to adjust or even waive small business participation requirements. DoD should invite input from its higher tier suppliers to determine whether they anticipate problems in small business participation and what actions they recommend in response.

Seventh, the Rule should do more to implement the direction of the statute, at Section 818(b)(2), where it directs the DoD to implement a "**risk-based approach**" to deal with the risk of counterfeits in its own purchasing practices. DoD's new Counterfeit Prevention Policy, DoDI 4140.67, employs a risk-based approach in many assignments. The proposed Rule, however, does not guide industry in setting risk-based priorities and offers neither standards nor assurance that "best efforts" will limit contractor liability

Risk-based assessment would give priority to prevention efforts where the **threat** is greatest that an unscrupulous actor has the capability to fabricate a counterfeit part or the intent to do so. Also considered is **vulnerability**, whether inherent or as can be introduced, such as where unfulfilled demand for certain parts, no longer available from secure sources, exposes the supply chain to nonconforming surrogates. **Consequences** also figure heavily into the risk-based equation. Counterfeit parts prevention is costly. Not all desirable actions are feasible or affordable.

This proposition of a "risk-based approach" recognizes that it is impossible to eliminate all risk of counterfeit in every system that the DoD buys or supports. What is feasible are data-driven, analytically informed methods for identifying those systems where the presence of a counterfeit would do the greatest harm, either to operations or personnel safety, so that those systems can be given special attention. Systems can be created to govern materiel control and purchasing decisions, and (for example) to create alerts and special practices, such as additional inspection and test, where threats are greatest, vulnerability acute or consequences most severe. The final Rule should address how DoD will work with its suppliers to design, implement and operate a responsible, risk-based approach to counterfeit part prevention.

Respectfully submitted,

Robert S. Metzger
June 28, 2013

Rogers Joseph O'Donnell, P.C. | 750 Ninth Street, N.W., Suite 710 | Washington, D.C. 20001
(202) 777-8951 (o)
rmetzger@rjo.com | www.rjo.com

Selected Publications & Presentations

"DoD's New Supply Chain Measures: The Counterfeit Prevention Policy (DoDI 4140.67) and Proposed DFAR (Detection & Avoidance of Counterfeit Electronic Parts)," SMTA/CALCE Symposium, College Park, MD, June 25, 2013

"Supply Chain Security: Converging Threats & Coordinated Responses," D.C. Microelectronics Group, June 6, 2013

"DoD Counterfeit Parts Rule – So Little After So Long," *Law 360*: Expert Analysis, June 4, 2013

"New DOD Counterfeit Prevention Policy: Resolves Responsibilities Within DOD But Leaves Many Contractor Questions Unresolved," *Federal Contracts Report*, a publication of Bloomberg BNA, May 15, 2013

"Supply Chain Security: Reducing Threats to Critical Systems," ERAI Executive Conference, April 18-19, 2013 (co-authored)

"An Appraisal of Select Provisions of the FY 2013 National Defense Authorization Act," *Federal Contracts Report*, Jan. 8, 2013

"Supply Chain Security & Integrity," ACI Industrial & National Security Conference. Nov. 14, 2012

"DoD Counterfeit Parts Rule: What Result When That Butterfly Beats Its Wings?", *Service Contractor*, by Professional Services Council, September 2012 (co-authored)

"Counterfeit Electronic Parts: What to Do Before The Regulations (and Regulators) Come? (Part 2)," *Federal Contracts Report*, Aug, 21, 2012

"Legislating Supply Chain Assurance: Examination of Section 818 of the FY 2012 NDAA," *The Procurement Lawyer*, Section of Public Contract Law, ABA, Vol. 47, No. 4 - Summer 2012 (co-authored)

"Counterfeit Electronic Parts: What to Do Before The Regulations (and Regulators) Come? (Part 1)" *Federal Contracts Report*, June 21, 2012, (co-authored)

"Counterfeit Parts Report - A Guide for Contractors, DoD," *Law 360*: Expert Analysis, May 24, 2012 (co-authored)

"Counterfeit Parts in DoD's Supply Chain: TechAmerica Webinar on Section 818 of 2012 NDAA," April 16, 2012 (with Jeffrey M. Chiow)