June 11, 2014

Defense Acquisition Regulations System
Attn: Ms. Amy Williams (DARC Deputy Director)
OUSD (AT&L) DPAP/DARS

Re: DFARS Case 2012-D055
Final Rule 79 Fed. Reg. 26092 (Effective May 6, 2014)
Public Meeting: Detection & Avoidance of Counterfeit Electronic Parts – Further Implementation

My name is Robert S. Metzger. I am an attorney in private practice with the law firm of Rogers Joseph O'Donnell, PC. I manage the Washington, D.C., office of the firm. I can be reached by email at rmetzger@rjo.com and by telephone at (202) 777-8951. I have written and spoken extensively on counterfeit parts prevention. *See* http://www.rjo.com/pub_counterfeit.html.

I offer this written statement for the record of presentations to be made at the Public Meeting of June 16, 2014, announced at 79 Fed. Reg. 26725 (May 9, 2014), to solicit further views on implementation of the requirements for detection and avoidance of counterfeit electronic parts on Department of Defense ("DoD") contracts, now subject of the final rule, as published at 79 Fed. Reg. 26092 and effective on May 6, 2014.

My observations are divided into two parts. In the first, I focus on apparently positive aspects of the final rule and raise questions about whether the principles behind these decisions will be positively employed in the administration of the rule and supervision of companies subject to it. In the second part, I focus upon four acute problem areas with the rule and suggest how DoD can respond.

I. THE POSITIVE ACCOMPLISHMENTS IN THE FINAL RULE WILL HAVE VALUE ONLY WITH CONSISTENT AND PRUDENT ADMINISTRATION AND OVERSIGHT

The Department of Defense deserves credit for its thorough efforts to digest and respond to the many comments that followed the proposed rule, on detection and avoidance of counterfeit electronic parts, which was published for comment at 78 Fed. Reg. 28780 on May 16, 2013. DoD also is to be commended for its consideration of the many concerns that were expressed by industry, and for its recognition of the serious threat that is posed by the risk of counterfeit electronic parts.

There are several important features of the final rule that represent positive changes from the initial draft. As shown below, however, the value of these changes depends ultimately upon the "symmetry" between industry's understanding and that of the government oversight and administration community. The purposes of the rule are entirely commendable. It *can* be interpreted to promote sensible, cost-effective measures that will achieve the goals of Section 818 without disruption to ongoing supply obligations or injury to the broad defense industrial

base. It is equally true, however, that the rule could be interpreted differently by the oversight authorities and applied in a harsh and inflexible way. If so, the dysfunctional costs and consequences of this rule will far exceed its value. This fundamental tension – between the positive value that might be achieved, and the negative harms that may occur, is largely for the Government to resolve. A restrained approach to implementation, receptive to the many lessons that will be learned through experience, will pay great dividends to all concerned.

1) The definition of "counterfeit electronic part."

The revised definition is improved to recognize that an "intent element" for a part to be classified as "counterfeit." This refinement to the definition should help covered contractors to determine when a part is "suspect" or confirmed as a "counterfeit electronic part" because inspection and testing should in most cases provide an objective basis for trained personnel to conclude that there has been an "intentional" effort to mischaracterize or misrepresent a part. The definition also is important because it shifts the focus of wrongdoing to the actor who possessed the intent to produce a counterfeit, rather than the company who might discover it in the proper operation of its system to detect and avoid counterfeits.

2) The definition of "suspect" counterfeit electronic part.

Similarly, this definition now recognizes that "credible evidence" must be present to provide "reasonable doubt" as to whether a part is authentic. The promulgation comments, 79 Fed. Reg. 26095, indicate that this is a "fact-based approach" and acknowledge that it is "not practical or cost-effective to test in every case of a suspected counterfeit." This, too, should assure contractors because the implication of the comments, and the phrase itself, admits that situations could arise where a counterfeit "escape" occurs, notwithstanding best efforts, because no "credible evidence" or *facts* were present to justify the time and expense of additional testing.

If the DCMA shares a similarly nuanced, it would go some distance to solve the problem, discussed further, of how to deal with accumulated inventory that now is subject to this rule. Contractors should be able to assert that inventory is not "suspect" merely because they do not possess documentation as now may be required for parts to be acquired prospectively. A "fact-based approach," as to inventory, would enable covered contractors to assess and demonstrate, where warranted, positive indicators of conformity and authenticity. The risk of a counterfeit is not eliminated, but it is minimized.

3) "Minimizing risk to the Government."

Another important provision is DFARS 252.246-7007(c)(2) which specifies that "selection of tests and inspection shall be based on minimizing risk to the Government. 79 Fed. Reg. at 26108. A crucial question is the extent to which contractors can employ "risk-based assessment" methods tailored to the particular circumstances of their business, including relative vulnerability of their supply chain to counterfeits and the significance of adverse consequence should a counterfeit "escape" occur. Again, however, where flexibility is suggested by the rule, as here, its value in the marketplace depends largely on the extent to which DCMA and other

government contracting and oversight personnel recognize and allow companies to use that flexibility.

4) Authorization to take a "risk-based approach."

In the promulgation comments, DoD asserts that the final new DFARS rule "does take a risk-based approach," 79 Fed. Reg. at 26096, and the system criteria, at DFARS 246.870-2(b), obligates contractors to "include risk-based policies and procedures" for the twelve (12) enumerated areas of their systems to detect and avoid counterfeit electronic parts. The promulgation comments indicate that the contractor's system is to recognize "the amount of risk based on the potential for receipt of counterfeit parts from different sources." 79 Fed. Reg. at 26096. If these principles actually are applied in DCMA oversight of contractor purchasing systems, some of the fears of industry, about how this rule might be applied with costly and disruptive effect, will be avoided. For example, to support some legacy programs, some companies will have no choice other than to resort to accumulated inventory, and some of that may have been purchased from distributors, even from brokers.

Similarly, many companies will face the challenge of how to qualify "additional" sources for parts that are not available from those "trusted sources" favored by Section 818 and the DFARS. Resort to distributors, and perhaps to brokers, will be the only choice other than to stop work or refuse the job. Contractors will be able to apply disciplined, fact-driven methods to assess the relative risk of inventoried parts, and to screen the use of distributors to situations where the risks are highly controlled. But they cannot eliminate that risk entirely, except by refusal to perform. Practically, DCMA must be able to agree that a contractor has a compliant system, even where it employs risk-based methods that allow it to use inventory or to continue to make purchases, if necessary, from distributors or brokers.

5) Where "flexibility" is allowed.

There are twelve required areas that must be included in a contractor's counterfeit parts prevention system. DFARS 246.870-2(b)(1) - (12). For three of these, the promulgation comments expressly assert that the rule provides a contractor with "flexibility." The three areas are (i) training (DFARS 246.870-2(b)(1), 79 Fed. Reg. at 26106), traceability, (DFARS 246.870-2(b)(4), 79 Fed. Reg. at 26107) and methodologies to identify suspect counterfeit electronic parts, (at DFARS 246.870-2(b)(7), 79 Fed. Reg. at 26107). For training, the comments state that "DoD is providing contractors with the flexibility to determine the appropriate type of training required for individual firms." 79 Fed. Reg. at 26097. For traceability, the comments advise that the rule "provides a contractor flexibility to utilize industry standards and best practices to achieve the required outcome." 79 Fed. Reg. at 26097. Similarly, as concerns the methodologies to identify "suspect" parts, the comments indicate that "the rule provides the contractor flexibility to employ a risk-based approach to tests and inspections." 79 Fed. Reg. at 26098). It is commendable that DoD recognizes, by such flexibility, that the implementation of the rule must be context-driven because the universe of affected companies is so diverse.

Industry wonders, however, whether flexibility will govern oversight and administration of the nine other required system elements. Some of these, taking into account

prevailing practices, are relatively straightforward. But several system elements have raised great concern among leading industry participants, especially those where the operational and financial outcome will vary enormously with the Government's chosen approach to oversight and administration. DFARS 246.870-2(b)(5) commands the use of suppliers that are original manufacturers or other authorized sources. An *inflexible* approach to this required system element could prove calamitous – because, read literally, a covered contractor would "fail" the requirement if it proceeds to use or buy any part from any other source. That is an impossible obligation to meet, as DoD components surely recognize. In this critical area, industry needs to know that DCMA will take an informed, flexible approach to administration and oversight.

6) How far does "flexibility" go?

A related question is how far flexibility will go – and whether companies have any reason to expect DCMA (and other government oversight authorities) to implement and enforce the rules with *consistency* – across the wide span of affected contractors or even within separate business units of an individual contractor. This is by no means assured; indeed, the rule and promulgation comments have essentially nothing to say about how DoD will assure consistency among its oversight or contracting personnel. The issue will prove to be most important. Take, for example, the flexibility that the comments endorse for methodologies to identify "suspect" counterfeit parts. An individual contractor will need to know that the methodologies it employs for one business unit will be sufficient for its other business units. It will need assurance that what was approved by one oversight official will not fail in the judgment of a different official. Moreover, higher tier, covered companies can be responsible for the compliance of their subcontractors with the rules (and for the adequacy of their systems). As the comments recognize, circumstances vary. Flexible implementation of the rules is an appropriate response. But when it comes time to conduct Contractor Purchasing System Reviews (CPSRs), deference must be given to the responsible actions that contractors have chosen to implement, even if there is great variation among contractors. Notions of "flexibility" will mean little to DoD's industrial base if the concept is absent in CPSRs and companies find themselves sanctioned for practices they've developed, in the absence of any prescriptive guidance, applying their knowledge of products and their risks.

7) Industry Standards.

Commendably, the rule declines to specify industry standards, "because industry standards are continually evolving." 79 Fed. Reg. at 26098. To meet the requirement design, operations and maintenance of a system to detect and avoid counterfeit electronic parts, DFARS 246.870(2)(b)(8), the promulgation comments say that "a contractor may elect to use current Government- and industry-recognized standards." *Id*. However, nothing is said about "industry standards" in the "system criteria" that govern a contractor's purchasing system, or in the flow-down clause at DFARS 252.246-7007. This is another of several areas where the "adaptive" language of the promulgation comments does not match with the operative phrases in the rule itself. This is important to industry because there are many choices among industry standards, many sources of those standards, and the standards are evolving. (Some issues raised by the new rules, for example "embedded software or firmware," as are included in the definition of an

"electronic part," are not now the subject of *any* standard.) Industry participants will make informed choices as to those standards relevant to their business. They will not want to find out, at the time of CPSR, that DCMA presumes to "second guess" their choice, even if they experience a counterfeit "escape" (a possibility that cannot be eliminated), and disapproves their purchasing system. This is not a reasonable risk for industry to assume. The answer must be for the government oversight community to approach CPSR and related tasks with appropriate deference for contractor judgment and knowledge. That respects rather than exploits contractors – who, after all, share with the Government the motivation to avoid counterfeits.

II. FOUR ACUTE AREAS WHERE THE RULE FALLS SHORT

I will comment upon four acute areas where the rule falls short:

1) Qualification of "Additional" Trusted Suppliers and Other Sources

In my previous submission to DPAP, for the March 27, 2014 meeting to address the subject of "trusted suppliers," I observed:

> Demand remains and will continue for the supply of electronic parts that are no longer available from the original sources. Such parts may be obsolescent or no longer in production. They may be available only from independent distributors, if they happen to hold such parts in inventory, or from brokers, who may find such parts in the "open market."

I suggested that the March public meeting was an "important opportunity to clarify how DoD and its supply chain should deal with the conflict between statutory insistence upon parts with no counterfeit risk, on the one hand, and market requirements for parts available only from sources with imperfect assurance, on the other."[1] Unfortunately, this critical subject remains unresolved in the final DFARS, with the result that all sectors of the supply chain remain anxious that they cannot know whether, in what circumstances or with what controls they may acquire and use parts from sources, such as distributors, who are not the original sources.

Section 818(c)(3) requires DoD to issue DFARS regulations, on the subject, but 2 ½ years have passed since enactment of the FY 2012 NDAA and no rules have emerged. No DoD official, so far as is known to this author, has denied the proposition that continuing and substantial demand exists for parts that are "obsolete" or "out of production" or otherwise unavailable from the "trusted suppliers" who are preferred both by statute and regulation. It is no consolation to industry, which has to deal with these questions countless times, every day, that DoD "contemplates further implementation" with respect to this subject under a new DFARS Case, 2014-D005. 76 Fed. Reg. at 26095.

---

[1] *See* Statement of Robert S. Metzger, at 2; March 27, 2014, *available at* http://www.acq.osd.mil/dpap/dars/publicmeeting/presentations/Counterfeit_Electronic_Parts-Further_Implementation/Rogers_Joseph_Presentation.pdf.

Despite DoD's inability to issue any regulations on this key point, there should be no misunderstanding that the use of such "additional" trusted suppliers is permitted by law. This is evident from the plain words of Section 818 itself – words which control over anything contrary that DoD might do in eventual regulations. Section 818(c)(3) provides that DoD contractors should "*whenever possible*" obtain electronic parts from original manufacturers and their authorized distributors. (Emphasis added.) This phrasing necessarily admits that it may *not* be possible to acquire parts from such sources – and the law does *not*, in any word, phrase or reasonable interpretation *prohibit* the use of such sources. Section 818(c)(3)(B) continues to require DoD to "establish requirements for notification" and "inspection, testing and authentication" of electronic parts that are obtained from "any source other" than one that falls within the most preferred categories. Although DoD has not provided rules on these subjects, it should confirm that contractors may use their reasonable judgment, risk-informed as appropriate, to make their own decisions on notification, inspection, testing and authentication measures. Where such practices are reasonable and responsible, guided by industry standards, informed by risk-assessment, and otherwise suitably documented, contractors should be secure in the knowledge that they can qualify, purchase and use parts from "additional" trusted suppliers that are not OCMs or authorized distributors.

The phrasing of the system criteria on use of trusted suppliers, at DFARS 246.870-2(b)(5), recognizes only suppliers that are the OCM or authorized sources, saying nothing about "additional" trusted suppliers or other sources. To be consistent with the statutory analysis, above that language must be interpreted to accommodate the use of "additional" trusted suppliers and other sources. This can be done by recognizing that the twelve enumerated system criteria, according to DFARS 246.870-2(c), are to "*address*" the "*following areas*" – language that imposes an obligation to "direct efforts toward" or "attention to" each area, rather than imposing a prescriptive rule.

As industry and Government begin the era in which supply chain security and counterfeit parts avoidance are matters of law and regulation, and oversight and administration, all would benefit from DoD's public acceptance of a prudent, interim approach to qualification of suppliers, as outlined above, pending the outcome of the DFARS Case 2014-D005.

2) **Treatment of Inventory**

Section 818 says nothing about inventory. Its focus, as is evident from Section 818(c)(3), is prospective, i.e., on future purchases of electronic parts and what measures might be taken to reduce vulnerability to counterfeits. But millions of electronic parts have been purchased, and inventory of parts, bought before the new rules, is in the hands of "covered contractors" subject to the new DFARS. And the final DFARS also is silent, in the rule, about inventory. But what was said in the promulgation comments has created a major issue for industry.

In one response to a question regarding inventory, the response is to parrot § 81(c)(3)(A)(i) to remind contractors that they are to obtain parts, "whenever possible," that

are currently in production or available in stock from the original manufacturer. 79 Fed. Reg. 26095. Another question prompted this answer:

> If the parts are already on the contractor's shelf or in inventory, and they were not procured in connection with a previous DoD contract, they will be subject to the same requirements, such as traceability and authentication.

79 Red. Reg. at 26099 (emphasis added). Contractors have reacted with some alarm. One problem is that many contractors, including large companies who manufacture or support may forms of equipment, purchase electronic parts in large quantities and keep them in inventory until required for production or maintenance. It has not been the common practice of industry to purchase or account for electronic parts, excepting special items such as space-qualified parts, either on a contract or customer basis. Some industry sources advise that it would be very expensive to do so, and could take years to implement such a system. So the qualification of the comment, suggesting that parts bought for a previous DoD contract are not subject to new rules, is of little or no practical value.

Many millions of dollars of electronic parts have been purchased and are being maintained in the inventory of covered contractors (and others). Companies are concerned that this comment may mean that they must discard and replace the subject inventory. Why? One reason is that the traceability rules now imposed by the new DFARS were not in place when these parts were acquired. Thus it will be impossible to show the "provenance" of inventory with the same level of data or documentation as will accompany future purchases of electronic parts. Nor is it practicable or affordable to perform tests as necessary for "authentication" of all the parts in inventory. If the proposition expressed by the comment is literally applied, therefore, little of accumulated inventory will be useable in performing DoD contracts without risking a violation of the new DFARS and putting purchasing system approval in jeopardy.

The actual adverse consequences, however, are considerably worse than even that. Companies will be required to assume the cost of replacement of the discarded inventory. (Arguments can be made that those costs, because they were required to comply with a new regulation, are not only allowable but also may be recovered through claims.) Some of the parts now in inventory, however, will be obsolete and out of production, or otherwise unavailable. That implies massive costs in the disruption to existing manufacturing and support commitments, and the real possibility that companies will inform government customers that they cannot perform existing contracts because they are precluded from using inventory. What extends this scenario towards the absurd is that this waste – of millions of parts, worth millions of dollars, will occur without *any* evidence that any parts in inventory actually were flawed, faulty, "suspect" or "counterfeit."

This result – all too real a prospect based on industry reaction – would be both absurd and, as suggested previously, is both unnecessary and avoidable. It is *unnecessary*

because parts in the inventory of covered contractors should be presumed not to be counterfeit absent some "credible evidence" or, at least, fact-driven indicators or "red flags" to cause additional investigation. It is *avoidable* if, as suggested previously, DoD endorses or DCMA allows contractors to design and use a "risk-based approach" to assess where (if at all) existing inventory may be vulnerable to counterfeit insertion, and to evaluate when ultimate use of the part is known whether the intended application or other information warrant additional authentication or assurance measures.

DoD can and rapidly should clarify the promulgation "comment" that has given rise to these concerns among its principal contractors. This can be done, for example, by recognizing that a responsible contractor, with good inventory management practices, and no evidence or cause for concern as to the authenticity of its existing inventory, can employ that inventory without violating the DFARS "system criteria" for counterfeit parts detection and avoidance. Guidelines can be suggested that will inform covered companies as to how they should assess their existing inventory and what additional risk measurement or risk mitigation measures should be taken where cause exists for concern that counterfeits may be present. DoD also would instruct DCMA and other DoD components to allow covered contractors to use existing inventory absent specific determination that particular systems present critical safety or performance risk such that additional scrutiny of parts drawn from inventory is justified.

3) **Flow-Down**

The final rule, at DFARS 252.246-7007(9), requires:

> (9) Flowdown of counterfeit detection and avoidance requirements, including applicable system criteria provided herein, to subcontractors at all levels in the supply chain that are responsible for buying or selling electronic parts or assemblies containing electronic parts, or for performing authentication testing.

This is explained in the promulgation comments:

> However, all levels of the supply chain have the potential for introducing counterfeit or suspect-counterfeit electronic items into the end items contracted for under a CAS-covered prime contract. The prime contractor cannot bear all responsibility for preventing the introduction of counterfeit parts. By flowing down the prohibitions against counterfeit and suspect counterfeit electronic items and the requirements for systems to detect such parts to all subcontractors that provide electronic parts or assemblies containing electronic parts (without regard to CAS-coverage of the subcontractor), there will be checks instituted at multiple levels within the supply chain, reducing the opportunities for counterfeit parts to slip through into end items.

79 Fed. Reg. at 26009. The drafters of the regulation are right, of course, that counterfeits can be introduced at any level of the supply chain, just as they are right – conceptually – that a COTS or "commercial item" could be a counterfeit. *See* 79 Fed. Reg. at 26099. The rule goes too far in reliance upon an idealized notion of how all tiers of the supply chain will work together and, undoubtedly with the best of intentions, operates from an idealized conception of the defense supply chain that, unfortunately, cannot be reconciled to the reality experienced by those contractors covered by the rule.

Section 818, by its terms, binds only "covered" contractors, i.e., those that are subject to CAS. Similarly, the regulations have legal effect only upon such CAS-covered contractors. Indeed, the promulgation comments confirm that Section 818 "specifically limited to covered contractors" the obligation to improve contractor systems to detect and avoid counterfeit electronic parts, and allowed that the new rule "has limited application *at the prime contract level* (including implementation of paragraph (c)(3) of section 818 (Trusted Suppliers) *to CAS-covered contractors.*" 79 Fed. Reg. at 26098 (emphasis added). A fundamental contradiction is present. ***Notwithstanding this (necessary) admission that the rule only applies to CAS-covered contractors, the regulation requires flowdown across the entire breadth and depth of a covered contractor's supply chain:***

> (e) The Contractor shall include the substance of this clause, including paragraphs (a) through (e), in subcontracts, including subcontracts for commercial items, for electronic parts or assemblies containing electronic parts.

DFARS 252.246-7007(e). This is even more curious when considered in the context of the prefatory language that begins the clause at DFARS 252.246-7007:

> The following paragraphs (a) through (e) of this clause **do not apply unless the Contractor is subject to the Cost Accounting Standards** under 41 U.S.C. chapter 15, as implemented in regulations found at 48 CFR 9903.201–1.

79 Fed. Reg. at 26109 (emphasis added). In other words, the preface of the clause that imposes flow-down requirements says expressly (albeit "in the negative") that none of "(a) through (e)" (which comprise the *whole* of the flow-down requirements) apply, *except that* (e) specifically requires flowdown to contracts, including those for commercial items, that obviously will not be performed by CAS-covered contractors.

It is impossible to reconcile this discrepancy, just as it is impossible to execute the flow-down instruction in the marketplace. Companies that are not CAS-covered are not subject to Section 818 or the DFARS regulations – and many know it. The Government has no legal authority under the statute or this rule to compel them to adhere to its terms or purposes. *Only* if they accept the flow-down, from a covered contractor, does the rule apply. That means that companies not CAS-covered are subject to the DFARS *if* and *only* to the extent they agree to accept it *as a matter of contract.* Since the rule imposes many duties, some potentially costly,

and suggests many liabilities, some potentially material, many companies in the supply chain of CAS-covered contractors have refused or will refuse to accept the flow-down.

Here, the rule makes a serious error by putting covered contractors at risk of disapproval of their purchasing system, or some other form of non-compliance, should their vendor base decline to accept the flow-down or insist upon negotiation of terms that vary and may diminish the obligations and risks. Surely DoD does not intend that its covered contractors will apply for contracting officer permission, waivers, or deviations, or other specific relief each time that a member of their supply chain refuses to accept the flow down or negotiates a different deal. That result would be absurd and truly calamitous to the industrial base and to the system of defense supply and support. Accordingly, DoD must issue clarification that recognizes that a contractor's system will not fail CPSR where contractors find they must continue to do business with suppliers who will not accept or modify the flow-down. This is not to discourage reasonable efforts to secure the flow-down, but it is necessary to accept the reality that the companies who are subject to this rule have neither the market nor legal power to impose it upon those members of their supply chain who refuse or resist.

4) **Required Disclosure**

A final point concerns the question of whether a contractor must make a disclosure to the Inspector General in the event it discovers a "suspect" or confirms that an electronic part is "counterfeit." The DoD Office of the Inspector General ("OIG") manages the disclosure program as required by FAR 52.203-13 (Contractor Code of Business Ethics and Conduct) and reinforced by FAR 9.406-2(b)(vi), which makes knowing failure to disclose such information a cause for debarment. The OIG website, on the Contractor Disclosure Program, states the following:

> **Counterfeit Parts Reporting**
>
> National Defense Authorization Act (NDAA) for fiscal Year 2012, Section 818, requires Defense contractors report suspected electronic counterfeit parts or non-conforming parts to the government. **Contractors should report through the submission of a contractor disclosure.** All other reporting requirements remain in effect, to include entry into the Government-Industry Data Exchange Program (GIDEP) database, or similar programs.

See http://www.dodig.mil/programs/CD/index.html (emphasis added). The OIG is incorrect in this instruction, and DoD should act to see that the instruction is clarified.

Companies doing business with the United States Government are obligated to disclose "credible evidence" of certain criminal violations or of False Claims Act (FCA) violations or significant overpayments that arise in connection with their government contracts or subcontracts. FAR §§ 9.406-2(b)(1)(vi), 9.407-2(a)(8). The legal obligation to disclose does not arise until there is "credible evidence" of a violation.

Should a company have a system as this DFARS rule requires, such a system will fulfill its proper purpose if it identifies a "suspect" or confirms a "counterfeit" electronic part. If such a part is found, that triggers a GIDEP report and notification to the contracting officer. *See* DFARS 252.246-7007(c)(6). The making of such a report is consistent with the proper operation of the *system* and complies with the *regulation*; hence, there is no "violation" for the contractor to report. As to the counterfeit part, the definition of the final rule expressly includes an "intent element," 79 Fed. Reg. at 26094, and that is expressed in the words that a counterfeit is a part that has been "knowingly mismarked, misidentified, or otherwise misrepresented." *See* DFARS 252.246-7007(a). The party that is responsible for a "violation" present in a "suspect" or confirmed "counterfeit electronic part" is not the contractor making the discovery but that person or enterprise that engaged in the "knowing" activities, described above. (The analysis differs, of course, if a covered company discovers that its employees have violated the companies' counterfeit avoidance policies or engaged in wilful or reckless disregard of these policies.)

A contractor disclosure under the OIG program often, if not usually, is followed by an investigation. That would not be justified where the contractor's system, to detect and avoid counterfeit electronic parts, worked as intended. It would be wrong to burden reporting contractors, in such circumstances, with the burden and expense of this *additional* disclosure. In any event, both Section 818 and the DFARS call for disclosures using GIDEP and to the Contracting Officer. Through either or both of those vehicles, the Government will be informed and law enforcement can be involved, based on that disclosure, to go after the true culprit.

III. CONCLUSION

Important national objectives are served by the DFARS rule on detection and avoidance of counterfeit electronics parts. The final DFARS, if prudently interpreted and sensibly applied, can fulfill the objectives of Section 818 without causing disruption to defense supply and support and injury to the defense industrial base. DoD and its components charged with oversight, administration and enforcement should proceed cautiously with the new rule, be receptive to the lessons of experience, and act with discretion and flexibility.

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
rmetzger@rjo.com | www.rjo.com