Bloomberg BNA

Federal Contracts Report™

Counterfeit Parts

Even if everyone in the supply chain accepts this proposition as correct, the Defense Department's sustainment challenge requires the servicing of thousands of items of aging equipment where the electronic parts necessary for maintenance *are not* available from any ''trusted supplier.''

Changes to Counterfeit Parts Regulations Merit Review, Revision to Industry Practices

BY ROBERT S. METZGER

Late in 2011, Congress enacted Section 818 to the National Defense Authorization Act (NDAA) of fiscal 2012. Final Defense Federal Acquisition Regulation Supplement (DFARS) Rules, ''Detection and Avoidance of Counterfeit Electronic Parts,'' were issued May 6, 2014. The objective of Section 818 was to improve both Defense Department (DOD) and industry practices in the detection and avoidance of counterfeit electronic parts. Section 818 was a remarkable statute in several respects. It sought to influence the practices of the defense supply chain at multiple junctures, including detection, exclusion, enforcement, purchasing practices, inspection and testing, reporting, corrective measures, contractor systems and sanctions.

Ordinarily, when Congress tries by legislation to change the intricacies of how DOD does business with its suppliers, frustration is likely to overcome accomplishment. Here, however, the fundamental ''logic'' of Section 818 has held up well over the 2½ years of experience that government and industry have accumulated since enactment. The DFARS has resulted in efforts, especially by the larger defense contractors, to create, document and maintain systems to detect and avoid counterfeit electronic parts. Industry has recognized, broadly, that electronic parts should be procured from original sources, where available, and much has been accomplished in the development of new standards and best practices to assist both purchasers and suppliers.

Robert S. Metzger, rmetzger@rjo.com, heads the Washington, D.C., office of Rogers Joseph O'Donnell, PC, a boutique law firm specializing in public contracts. A frequent contributor to Federal Contracts Report, Bob was named a 2016 ''Federal 100'' awardee by Federal Computer Week for his contributions to cyber and supply chain security. This article reflects Mr. Metzger's personal views and should not be attributed to any client of his firm or organization with which he is involved or affiliated.

Over time, however, it became painfully evident that both the statute and the DFARS imposed certain constraints that produced adverse ''real world'' consequences and costs. Especially difficult was the concentration upon purchasing only from ''trusted suppliers'' in both Section 818 and the DFARS. Simply put, even if everyone in the supply chain accepts this proposition as correct, DOD's sustainment challenge requires the servicing of thousands of items of aging equipment where the electronic parts necessary for maintenance *are not* available from any ''trusted supplier.''

In August, DOD revised several key aspects of the counterfeit parts regulations. These make important changes affecting the strategy and practice of the defense supply chain. They introduce needed flexibility in the selection and qualification of parts suppliers. They offer relief from the potentially draconian disallowance of costs of part replacement or rework in the event a counterfeit part ''escapes'' into fielded systems. They increase the importance of conduct aligned with established standards, and add new emphasis to creation and collection of data for tracking the pedigree and provenance of electronic parts. At the same time, however, in certain crucial areas, the new regulations raise as many (or more) questions than they answer, such that new issues will cause industry doubt as to what is required for compliance.

This article seeks to review the most important of the August 2016 changes to counterfeit rules. Because the DFARS has changed in material respects, many companies will need to reassess and update the systems, policies, procedures and practices they built upon interpretations of the initial DFARS.

Changes to Statute and Regulation

The ''fundamentals'' of Section 818 have not been changed since its enactment. However, over time the statute has been revised in ways directly reflected in the August rules. Section 833 of the fiscal 2013 NDAA and Section 885 of the fiscal 2016 NDAA have expanded the ''safe harbor'' of circumstances where costs of a counterfeit part, and rework, are allowable. Section 817 of the fiscal 2015 NDAA and Section 806 of the fiscal 2017 NDAA have relaxed purchasing criteria to facilitate purchases from sources other than ''trusted suppliers.''

As concerns the DFARS, there were two principal rulemakings and another minor one in August 2016. On Aug. 2, DOD produced the Final Rule on DFARS Case 2014-D005, ''Detection and Avoidance of Counterfeit Electronic Parts.'' 81 Fed. Reg. 50635. Also on Aug. 2, DOD published a Proposed Rule on DFARS Case 2016-D013, ''Amendments Related to Sources of Electronic Parts.'' 81 Fed. Reg. 50680. On Aug. 30, another Final Rule was produced, this one on DFARS Case 2016-D010, ''Costs Related to Counterfeit Electronic Parts.'' 81 Fed. Reg. 59510. Collectively, these make significant changes to DFARS Subparts 202 (Definitions), 212 (Acquisition of Commercial Items), 231 (Contract Cost Principles), 242 (Contract Administration), 246 (Government Property) and 252 (Contract Clauses). The most notable changes are to:

- DFARS 202.101 adds definition of ''contractor-approved supplier'' and deletes ''embedded software or firmware'' from the definition of ''electronic part'';
- DFARS 212.301 adds a requirement to use the new ''-7008'' clause in solicitations for commercial items;
- DFARS 231.205-71 expands the allowable costs ''safe harbor'' to include parts obtained from any source in accordance with the ''-7008'' clause, among other conditions;
- DFARS 242.202 allows government review and audit of ''contractor-approved suppliers'';
- DFARS 246.870-2 establishes a three-tiered hierarchy for ''sources of electronic parts,'' including ''contractor-approved suppliers'' as the moderate-risk tier, and parts from ''other'' sources as the highest-risk tier;
- DFARS 252.246-7007 revises the existing clause to accommodate ''contractor-approved suppliers'' and adjusts the 12 system criteria to reflect now-allowed sources and new traceability requirements; and
- DFARS 252.246-7008 now establishes the basis for purchase from different categories of sources (beyond ''trusted suppliers'' as originally emphasized) and to express new traceability requirements and new uses of risk-based methods for inspection, test and authentication.

Of these, the new ''7008'' clause will have the greatest impact, in part, because it applies to all in the defense supply chain, and not just to the larger, Cost Accounting Standards (CAS)-covered contractors who were principally affected by the original DFARS.[1] The revised cost allowability policy is also a key change.

DFARS 231.205-71. Higher-tier contractors, and especially those who are CAS-covered, have been concerned about the potential that a counterfeit ''escape'' could expose them to potentially large costs that would be unallowable and often unrecoverable. The exposure was not limited to the cost of a replacement part but extended to the ''costs of rework,'' which, in the event of a catastrophic system failure, could be enormous. Since enactment of Section 818, industry groups have sought to establish and then expand a ''safe harbor'' for conduct that would cause such costs to be allowable in more circumstances. Initially, the ''safe harbor'' was limited to a combination of criteria that rarely would be met: an ''approved system'' to detect and avoid counterfeit parts; a requirement that the parts be government-furnished, together with timely notice if a counterfeit is discovered. Now, costs are allowable if: (a) the contractor has a system that DOD has reviewed and approved

[1] As revised DFARS 246.870-3 (''Contract clauses'') requires use of the ''-7008'' clause in all solicitations and contracts, including FAR Part 12 for acquisition of commercial items, when procuring ''(1) Electronic parts; (2) End items, components, parts, or assemblies containing electronic parts, or (3) Services if the contractor will supply electronic parts or component, parts, or assemblies containing electronic parts as part of the service.'' One may question whether DOD employed a ''risk-based process'' in making the ''-7008'' clause so broadly applicable, since acquisitions of parts in commercial items or commercial off-the-shelf acquisitions — where the parts are presently in production and the original equipment manufacturer is the product source — present lower risk and therefore less justification for application of the rule.

  FCR ISSN 0014-9063

(as before); (b) the parts were obtained as government-furnished property (unchanged) *or* in accordance with the methods allowed under the ''-7008'' clause (new); and (c) the contractor provides timely notice (within 60 days after it ''becomes aware'') both to the cognizant contracting officers and to GIDEP.[2] Thus, for companies that have satisfied *all* conditions, there is protection against large-scale liability that had concerned many in the industry. Other key changes are favorable — *e.g.*, allowing safe harbor for parts from any of the three tiers of sources, the various ways by which a contractor may become ''aware'' of a counterfeit, and the clarification to report both to the contracting officer and to GIDEP.

DFARS 246.870-2. The initial DFARS could be criticized for requirements that reflected a world more ''idealized'' than ''real,'' in that the emphasis on purchasing only from ''trusted suppliers'' suffered from a faulty assumption that actual needs could be met with parts available from only this class of sources. Experts agree that sourcing from original sources presents the least risk, and so, under the DFARS as revised, this is the preferred or highest ''tier'' of potential sources.[3] DFARS 246.870-2(a)(1)(i). However, the continuing needs for electronic parts are diverse and cannot be satisfied by resort only to the preferred, lowest-risk category of supplier. To maintain fielded DOD systems, many parts are needed that cannot be obtained from the lowest-risk sources. The DFARS has been revised to accommodate different methods to purchase parts, with three tiers reflecting levels of risk. The contractor's obligations — and the level and nature of government oversight — increase with the higher-risk methods.

The second ''tier'' or medium-risk supplier is described at DFARS 246.870-2(a)(1)(ii). New to this provision, and reflected also in the ''-7008'' clause, contractors may obtain electronic parts from ''contractor-approved suppliers'' provided that: (a) the contractor uses established counterfeit prevention industry standards and processes (including inspection, testing and authentication); (b) the contractor ''assumes responsibility for the authenticity'' of such parts, and; (c) the selection of contractor-approved suppliers is subject to review and audit by the contracting officer.[4]Recognition of medium-risk suppliers should prove of critical operational significance to many companies. Now, at least in theory, *any* **contractor** at *any* tier in the supply chain, is authorized to self-identify its own ''contractor-approved suppliers.''[5] This is the needed remedy to the practical conundrum that has frustrated industry since promulgation of the initial DFARS in 2014: It *is* necessary to use other than ''trusted suppliers'' *when* needed parts *cannot* be obtained from the preferred (lowest-risk) category.

Both to ''identify'' and ''approve'' such a supplier, the contractor is to use ''established counterfeit prevention industry standards and practices'' — though the regulation is silent on which of these, how they should be applied, and what risks justify higher scrutiny (and costs) than others. Especially as concerns ''inspection, testing and authentication'' (IT&A), there is an enormous range of possible outcomes as standards often describe process and methods that *can* be employed rather than

[2] GIDEP's long history began in 1959. It operates a database that is used to report issues of parts failure, as well as to collect and disseminate information on attributes of parts, components and materials. In recent years, GIDEP has assumed increased importance as the principal vehicle by which defense contractors are to report suspect and confirmed counterfeit electronic parts. Section 818(c)(4) requires that DOD contractors report to GIDEP. Unfortunately, GIDEP has not received the funding it needs to modernize its information systems, and so the present utility of the GIDEP exchange is less than what could be achieved with a modern, data-driven system. A February 2016 GAO report criticized DOD's management of GIDEP. *See* ''Counterfeit Parts: DoD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk,'' Report GAO-16-236. FAR Case 2013-2, ''Expanded Reporting of Nonconforming Items,'' has been open for several years. A proposed rule published June 10, 2016, that contemplated significant enlargement of product and parts deficiency reporting, for both civilian agencies and DOD, and an expanded role for GIDEP. 79 Fed. Reg. 33164. The proposed rule has not been finalized, however, and the current FAR Case Status Report indicates that this case is ''on hold . . . pending completion of a study regarding which changes to GIDEP are currently feasible.'' *See* ''Open FAR Cases as of 10/17/2016.''

[3] The DFARS gives preference to purchases of electronic parts that are in production by the original manufacturer or by an authorized after-market manufacturer based upon the attributes of the source (original manufacturer, authorized suppliers, or suppliers who obtain such parts exclusively from the original manufacturers or their authorized suppliers.) DFARS 252.246.870-2(a)(i); DFARS 252.246-7008(b)(1). Some sources fall within this category for certain parts but not for others. And sources in this category cannot be presumed always to exercise care in handling inventory, and in the disposition of returns, to avoid commingling of suspect or counterfeit parts with authentic items. DOD should consider adding language to assure that lowest-risk sources conform to industry standards and best practices. For example, SAE is developing AS6496 (''Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition - Authorized/Franchised Distribution'').

[4] Section 885(b) of the fiscal 2016 NDAA amended Section 818(c)(3)(D)(iii) to state that contractors and subcontractors are subject to approval (as well as review and audit) by appropriate DOD officials when identifying a ''contractor-approved supplier'' of electronic parts. By proposed rule published Aug. 2, 2016 — 81 Fed. Reg. 50680 — DOD intends to revise the new -7008 clause to implement the statutory change. Contractors ''may proceed with the acquisition of electronic parts from a contractor-approved supplier unless otherwise notified by DOD.'' Proposed DFARS 252.246-7008(b)(2)(iii). Left unstated are which circumstances will cause DOD to review or audit an identified ''contractor-approved supplier''; which criteria DOD will use in making a determination; how DOD will assure consistency in treatment on a common supplier that may come under the consideration of many contracting officers; and what consequence or action is to be taken as concern parts that companies may procure and use from such a supplier before a ''disapproval'' decision.

[5] Ostensibly, the medium-risk ''tier'' is well-defined. A source must be contractor-approved, using established industry standards, and the contractor must ''assume responsibility for the authenticity of the parts.'' These requirements apply by operation to the contractor who approves a ''Tier 2'' supplier and, we must assume, will flow down to the distributor or broker that is the ''approved supplier.'' Here, a problem arises. In any and every situation where a part must be obtained from a ''Tier 2'' (or ''Tier 3'') supplier, there is a risk of encountering a suspect or counterfeit part that cannot be reduced to zero. As such, a prudent ''contractor-approved supplier'' cannot vouch for ''authenticity;'' all it can do is capably perform and report on the inspection, testing and authentication measures that its customer requires. DOD and higher-tier contractors will have to apply the rules for ''contractor-approved suppliers'' carefully to avoid demands so rigorous and risky as would vitiate the ability of sources and customers to reach agreement.

prescriptive methods of what *must* be employed. DOD has offered no guidance on these important details so far. Industry welcomes flexibility, but some guidance would be helpful to inform contractor planning and actions.[6]

The clause states that the contractor ''assumes responsibility'' for authenticity, but the operative meaning or legal significance of this phrase is not self-evident. It could be that DOD expects contractors to be contractually liable for costs or rework if a part proves not to be ''authentic'' — but that could contradict the ''safe harbor'' of the revised Cost Principle (where all conditions are met). Or it could mean that contractors are ''responsible'' to correct if a part is not ''authentic,'' but what this adds, beyond ordinary quality assurance requirements and warranty of supplies, is not clear.[7]

A third ''tier'' of highest-risk supplier is made available through DFARS 246.870-2(a)(2), which applies whenever a contractor obtains an electronic part from a source other than the two preferred ''tiers'' (identified in (a)(1)) or from a subcontractor (other than the original equipment manufacturer (OEM)) that refuses to accept flowdown of the ''-7008'' clause. As to these sources, certain obligations derived from the ''-7008'' clause apply. The same obligations apply where a contractor cannot ''confirm'' that an electronic part is new or not previously used and that it has not been ''commingled'' with other stock in inventory that may be ''used, refurbished, reclaimed or returned parts.''[8] Analytically, it is troubling that the same mitigation measures apply to each of the three situations where ''(a)(2)'' applies. The actual risk of a counterfeit electronic part is likely to be higher if a part must be obtained from a broker or distributor, due to ''nonavailability,'' than is the corresponding risk where, for example, a part is purchased from a commercial or commercial off-the-shelf supplier that rejects flowdown. Similarly, the IT&A measures appropriate for purchase of an obsolescent part from a broker would vary greatly from prudent measures to parse accumulated inventory. This third ''tier'' offers a welcome ''relief'' mechanism, by enabling purchase in situations where lower-risk alternatives are not available. The drafting, which suggests the same IT&A obligations apply, irrespective of different risks (and mitigation methods), seems more expedient than informative.

DFARS 252.246-7007. Contractor Counterfeit Electronic Part Detection and Avoidance System (August 2016). The August 2016 DFARS changes affect only two of the 12 systems criteria for CAS-covered contractors that must have systems to detect and avoid counterfeit parts. Criterion 4 (traceability) is changed to eliminate prescriptive requirements, such as Item Unique Identification (IUID) marking, instead using high-level language encouraging ''[r]isk-based processes'' that ''enable *tracking*'' from the OEM to product acceptance by the government. DFARS 252.246-7007(c)(4) (as revised) (emphasis added). These changes seem promising — in concept, improved traceability will reduce supply chain risk — but the new language does not fare well on close analysis. Substitution of ''tracking'' for ''traceability'' seems contrary to industry custom and practice. ''Traceability'' is applied to address data and documentation of parts pedigree and provenance. ''Tracking'' often refers to ascertainment of the physical location of parts, assemblies or other equipment. Perhaps ''tracking'' was chosen because DOD seeks active, part-specific capabilities, such as that which might be provided by radio frequency identification tags or other technical instrumentalities. But there are no present, generally accepted industry or government standards for such tracking devices. Neither ''tracking'' nor ''traceability'' are self-defining, and they are not ''one-size-fits-all'' propositions. The absence of definition, or reference to standards, leaves great room for uncertainty and inconsistent application. Also, the notional proposition that contractors at any and every level of the supply chain can obtain or sustain end-to-end tracking (''from the original manufacturer to product acceptance by the Government'') is a worthy goal, but its achievement is outside the capability of most participants in the supply chain who have to accept such ''tracking'' or ''traceability'' documentation as the seller chooses to furnish.

The change to Criterion 5 (use of suppliers) conforms to other changes, especially to -7008 and the tiered approach of parts source selection. It provides no information whatsoever to inform a CAS-covered contractor on which measures, with respect to use of suppliers, will or might not satisfy the Defense Contract Management Agency when it examines a contractor's counterfeit parts system as part of purchasing system review. DOD should permit contractors to employ different methods to fit their circumstances but can improve upon operational guidance.

DFARS 252.246-7008. Sources of Electronic Parts (August 2016). The ''-7008'' clause is all new. It provides, at -7008(b):

> (b) *Selecting suppliers*. In accordance with Section 818(c)(3) of the fiscal 2012 NDAA (Pub. L. 112-81), as amended by Section 817 of the fiscal 2015 NDAA (Pub. L. 113-291), the Contractor shall —
>
> (1) **First** obtain electronic parts that are in production by the original manufacturer or an authorized aftermarket manufacturer or currently available in stock from —
>
> (i) The original manufacturers of the parts;

---

[6] The DFARS makes reference to ''standards and practice'' (including IT&A) ''*such as* the DoD-adopted standards.'' This phrasing implies that contractors may elect to select *other* standards. Which? And how will the adequacy be measured? This may be a significant question. DOD seeks the right to review and approve selection. *See* ''Amendments Related to Sources of Electronic Parts,'' DFARS Case 2016-D013, Proposed Rule, 81 Fed. Reg. 50680, Aug. 2, 2016. Contractors will seek confidence that their basis of ''identification'' and ''approval'' of a contractor-approved supplier is satisfactory to DOD. This issue becomes more acute should there be a counterfeit ''escape'' involving a part supplied by a ''contractor-approved supplier.'' Companies will want to know that the methods they use to approve a ''contractor-approved supplier'' will be sufficient to qualify for the ''safe harbor.''

[7] Inspection, testing and authentication here are applied to approval of the source (the ''contractor-approved supplier'') rather than approval of part(s) from the supplier. However, to mitigate risks as to authenticity, presumably contractors who approve such ''Tier 2'' suppliers will employ suitable inspection, testing and authentication measures as to the parts they receive.

[8] The clause, at DFARS 246.870-2(a)(2), refers to the ''notification, inspection, testing and authentication requirements of paragraph (b)(3)(ii) through (b)(3)(iv) of the clause at 252.246-7008.'' The referenced ''-7008'' clause, however, contains no content for any of (b)(3)(ii) through (b)(3)(iv).

  FCR ISSN 0014-9063

(ii) Their authorized suppliers; or

(iii) Suppliers that obtain such parts exclusively from the original manufacturers of the parts or their authorized suppliers;

(2) If electronic parts are not available as provided in paragraph (b)(1) of this clause, obtain electronic parts that are not in production by the original manufacturer or an authorized aftermarket manufacturer, and that are not currently available in stock from a source listed in paragraph (b)(1) of this clause, from suppliers identified by the Contractor as contractor-approved suppliers, provided that —

(i) For identifying and approving such contractor-approved suppliers, the Contractor uses established counterfeit prevention industry standards and processes (including inspection, testing and authentication), such as the DOD-adopted standards at https://assist.dla.mil;

(ii) The Contractor assumes responsibility for the authenticity of parts provided by such contractor-approved suppliers; and

(iii) The Contractor's selection of such contractor-approved suppliers is subject to review and audit by the contracting officer; **or**

(3)(i) Take the actions in paragraphs (b)(3)(ii) through (b)(3)(iv) of this clause if the Contractor —

(A) Obtains an electronic part from —

(1) A source other than any of the sources identified in paragraph (b)(1) or (b)(2) of this clause, due to nonavailability from such sources; or

(2) A subcontractor (other than the original manufacturer) that refuses to accept flowdown of this clause; or

(B) Cannot confirm that an electronic part is new or previously unused and that it has not been commingled in supplier new production or stock with used, refurbished, reclaimed or returned parts.

(ii) If the contractor obtains an electronic part or cannot confirm an electronic part pursuant to paragraph (b)(3)(i) of this clause —

(A) Promptly notify the Contracting Officer in writing. If such notification is required for an electronic part to be used in a designated lot of assemblies to be acquired under a single contract, the Contractor may submit one notification for the lot, providing identification of the assemblies containing the parts (e.g., serial numbers);

(B) Be responsible for inspection, testing, and authentication, in accordance with existing applicable industry standards; and

(C) Make documentation of inspection, testing, and authentication of such electronic parts available to the Government upon request.

Selecting suppliers (DFARS 252.246-7008(b)

Some content in the -7008 contract clause is not in the Subpart 246 Policy. This elaboration is significant. Under -7008(b)(1), the word ''First'' is used and, under (2), the text begins with the phrase ''If electronic parts are not available as provided in paragraph (b)(1) of this clause.'' This phrasing does more than emphasize the priority among ''tiers''; it can be read to *require* use of the lowest-risk (highest-tier) supplier and to *permit* use of a higher-risk (lower-tier) supplier *only* if the part cannot be obtained from the higher tier.

Selection of ''Tier 2'' and ''Tier 3'' sources involves the government. When a ''Tier 2'' source is used, the ''Contractor's selection of such contractor-approved suppliers is subject to review and audit by the contracting officer.'' DFARS 252.246-7008(b)(2)(iii). For a ''Tier 3'' source, a contractor must ''[p]romptly notify the Contracting Officer in writing.'' *Id.* at 7008(b)(3)(ii)(C). If the same supplier is used for multiple contracts, notice will be required by multiple contracting officers, inviting inconsistent results. The process for ''Tier 2'' focuses on the source (the contractor-approved supplier), while that for ''Tier 3'' focuses on the part. DOD may wish to consider whether it can adopt a systems approach to these functions, such that it reviews and may approve the systems used by contractors to qualify and use ''contractor-approved suppliers,'' and to use parts from the ''other'' sources in ''Tier 3,'' rather than asking contracting officers to perform functions for which they may not be trained and inserting DOD oversight at a piece part level.

The -7008 clause provides further details about use of suppliers in ''Tier 3.'' Some companies will be able to satisfy all their requirements without resort to highest-risk sources, but this tier will be important for other companies, especially those active in equipment sustainment. The third option [(3)(i)] seems reasonable, but again issues arise on close examination. Mitigation measures are required, but the regulation (''Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition - Distributors'') for actions to be taken, refers to content that is not present. The regulation does not inform contractors of the actions they must take. It is positive that the clause can be applied to permit defense supply chain participants to purchase from distributors, even brokers. Considering this is the category of highest risk purchase, however, it is surprising that the same nonspecific language (''[b]e responsible for inspection, testing, and authentication'') is used here as was employed for sources in the lowest- and middle-risk tiers. Similarly, reference is made to ''existing applicable industry standards'' without specifying which or discriminating among those potentially applicable.

Since this tier would be used, presumably, to permit ''one-off'' or ''small lot'' purchases from distributors for specific sustainment needs, one would have expected DOD to cite its own programs (*e.g.*, Defense Logistics Agency (DLA) Qualified Suppliers List for Distributors (QSLD)) and to identify the accepted SAE Standard AS6081. Instead, the reference to ''industry standards and processes'' is general and, as a consequence, vague. Moreover, the phrase lumps together three functions — inspection, testing and authentication — that are potentially distinct and may be performed by differ-

ent actors in the supply chain when a ''nonavailability'' situation triggers use of this ''third tier'' authority.[9]

All supply chain participants — customer, contractor, subcontractor, distributor, test lab, etc. — share an interest in *compliance* and a desire to avoid purchases from any supplier whose qualification DOD might disapprove. Considered in this light, the language of -7008 is deficient. While it earns credit for flexibility, the regulation lacks sufficient granularity to guide industry practice. This is an especially unfortunate outcome given the risks present and the potentially significant costs involved. Even as to the government role, the new -7008 is less than adequate. Regarding notification, for example, it is not clear whether a contractor must allow the contracting officer time to evaluate and respond. As to documentation, nothing is said to guide companies in what level of detail will be expected.

Traceability (DFARS 252.246-7008(c)

DOD strongly supports traceability as a means to reduce supply chain risk. As expressed in the new -7008(c) clause, however, the new requirement is poorly defined and may impose burdens on contractors of dubious value. The applicable part of the regulation states:

> (c) Traceability. If the Contractor is not the original manufacturer of, or authorized supplier for, an electronic part, the Contractor shall —
>
> (1) Have risk-based processes (taking into consideration the consequences of failure of an electronic part) that enable tracking of electronic parts from the original manufacturer to product acceptance by the Government, whether the electronic part is supplied as a discrete electronic part or is contained in an assembly;
>
> (2) If the Contractor cannot establish this traceability from the original manufacturer for a specific electronic part, be responsible for inspection, testing, and authentication, in accordance with existing applicable industry standards; and
>
> (3)(i) Maintain documentation of traceability (paragraph (c)(1) of this clause) or the inspection, testing, and authentication required when traceability cannot be established (paragraph (c)(2) of this clause) in accordance with FAR subpart 4.7; and
>
> (ii) Make such documentation available to the Government upon request.

Initially, the rule at (c)(1) seeks ''tracking . . . from the original manufacturer to product acceptance by the Government'' even though the DFARS may apply to *purchasers* and to other supply chain intermediaries who may lack authority to require the original supplier to provide desired traceability or who may purchase a part already in distribution that has less than full traceability back to the OEM. The regulation does not impose upon OEMs, authorized after-market manufacturers, authorized distributors, or anyone else, specific parts marking, documentation or other traceability requirements. End-to-end traceability can only be as good as the information provided by the OEMs and their distributors who first sell electronic parts. If there is no standard or minimum, for traceability expected at the point of manufacture and initial sale, all that follows is impaired. Hence, full compliance with the (c)(1) objective of the regulation is unlikely, if not impossible without resort to the additional tasks in (c)(2).

Even as to (c)(1), the relational linkage among ''risk-based processes,'' ''consequences of failure'' and ''tracking'' are not clear. If ''risk'' is considered at the platform, or system level, conceivably it makes sense to increase the investment in traceability. However, as one goes down the supply chain, the likelihood is reduced that a given supply chain actor will have any idea of the ultimate use of a part or the consequences of failure. Turning to (c)(2), the clause says that if desired traceability cannot be obtained — as will occur in many, if not the majority of cases — the contractor is to ''be responsible for inspection, testing, and authentication, in accordance with existing applicable industry standards.'' The practical meaning of this is unknown. Industry standards, such as SAE AS5553B, or AS6171[10], offer some guidance on IT&A, but that guidance is not now ratcheted to levels of traceability. DOD, therefore, has obligated its suppliers to apply IT&A to compensate for deficiencies in traceability, but did not inform suppliers of the standards or other criteria to apply.

Subcontracts (DFARS 252.246-7008(3)

The flowdown obligation that accompanies the -7008 clause follows:

> (e) *Subcontracts*. The Contractor shall include the substance of this clause, including this paragraph (e), in subcontracts, including subcontracts for commercial items that are for electronic parts or assemblies containing electronic parts, unless the subcontractor is the original manufacturer.

The phrase ''substance of the clause'' suggests that contractors may tailor the clause, but the complexities of -7008 and the mandatory nature of the flowdown (''shall include'') make it problematic how to tailor the clause to reduce downstream supplier objection without violating the obligation. A key question is whether the risk of counterfeits, when purchasing ''commercial items'' that have electronic parts, justify the cost, disruption and frustration that likely will accompany mandatory flowdown of the whole -7008 clause or its ''substance.'' A better choice would be for the DFARS to provide a short, simple clause for flowdown to commercial sources, e.g., obligating the source to deliver products that do not contain any counterfeit components (electronic or otherwise) and requiring prompt notification

[9] Inspection may be performed by both the supplier and the customer, but testing may be performed by an independent, qualified laboratory. Again, DOD has developed, through the DLA, the Qualified Testing Suppliers List (QTSL), but the DFARS regulation makes no reference to it. Nor did DOD cite any of the potentially relevant SAE Standards that concern testing of electronic parts — even though, in this high-risk domain, the specifics of standards and practices matter a great deal. *See* Robert S. Metzger, ''BNA Insights: JEDEC's New JESD243: A New Standard That Is Less Than Industry Needs to Avoid Counterfeit Electronic Parts,'' 105 FCR 335, Apr. 19, 2016.

[10] SAE AS6171, ''Test Methods Standard; General Requirements, Suspect/Counterfeit Electronic, Electronic and Electromechanical Parts,'' was approved Oct. 21, 2016, by the results of balloting held by the SAE Aerospace Council. AS6171 is an important resource to inform contractors (and the government) on how to apply risk-based methods to select appropriate measures of inspection and testing for electronic parts.

  FCR ISSN 0014-9063

to the purchaser in the event the supplier learns of a counterfeit.

Practical Impact

Larger defense suppliers have systems to detect and avoid counterfeit electronic parts and have developed policies, procedures and practices to implement those systems. Ultimately, different tiers of the supply chain are connected by contract and the process of solicitation, negotiation and award defines the nature of those connections and the attendant obligations.

Because there have been material changes in DFARS regulations, corresponding changes are needed in the contracting arrangements within industry. For example, before the August 2016 changes, higher-tier companies faced large potential liability for replacement of a counterfeit electronic part, or for rework, and they sought to defray that exposure by forcing suppliers to indemnify or even ''guarantee'' that parts they furnished were not counterfeits — even if the parts were obtained from other than OEMs or similar ''trusted sources.'' This practice leveraged the buying power of the higher-tier companies to the disadvantage of the supplier, sometimes producing unworkable and unfair results, especially where the supplier could obtain the necessary part only from sources with unavoidable risk.

The Cost Principle now has been changed to greatly reduce the financial vulnerability of higher-tier suppliers to unallowable counterfeit costs — provided that their system has been reviewed and approved and that other conditions are met. Contractors in this position now can purchase from ''contractor-approved suppliers,'' or even from the higher-risk (''other'') suppliers, and still receive allowable cost treatment. Companies should develop and document procedures and process to identify and qualify ''contractor-approved suppliers.'' This will entail review and selection among ''industry standards and processes'' and determination of suitable criteria and methods for ''inspection, testing, and authentication.'' For most companies, the process to establish ''contractor-approved suppliers'' will involve substantial new work, but it is likely to result in a leveraged benefit as a source (or sources), once qualified, can be used repeatedly. Companies may develop standing relationships with specialized distributors and test resources, working individually or in combination, which can be established as ''contractor-approved suppliers'' for regular use. Reference to existing DOD processes — such as the DLA programs to approve distributors and testing labs — as well as to industry standards — such as several from SAE — can inform the qualification and approval process for suppliers, as well as the application of inspection, testing and authentication methods to procured parts. It would be useful for DOD to inform contractors on acceptable approaches to select and document ''contractor-approved suppliers'' and to encourage contractors to ''aggregate'' qualification of this category of suppliers so that a ''moderate-risk'' supplier, once approved, can supply to others on the same basis.

Most companies will seek to limit their purchasing of electronic parts to the lowest- and moderate-risk categories of suppliers. Efficiency and risk management concerns will drive purchasers to use a small number of ''contractor-approved suppliers.'' The situation is less clear for the highest-risk sources. ''Tier 2'' invites establishment and use of a standing supplier relationship after qualification is accomplished. The drive to use ''Tier 3,'' in contrast, will be specific parts requirements where a necessary part cannot be obtained from either higher ''tier.'' Companies will not want to take the time or incur the expense (and risk) to identify, vet and select sources only after a need surfaces. The prudent approach again will be to pre-qualify the resources that will be necessary if, when and to the extent that ''Tier 3'' must be used. Considering the requirements of DFARS 252.246-7008(b)(3), contractors should assess brokers, distributors and test laboratories for their competence, equipment and capabilities for ''inspection, testing and authentication'' and they should assess the extent to which these resources have adopted or are accredited to ''applicable industry standards.''

As companies develop and use systems to procure from newly authorized sources, there will be questions about how to assure compliance and how to avoid exposure to legal liability. Companies will be well-counseled to disclose more rather than less to contracting officers. Disclosures should explain the basis for selection; the methods of IT&A chosen; which standards or practices were considered; the qualifications of sources and how they were reviewed, etc. While there is added burden to ''fulsome'' disclosure, there is a prophylactic benefit in reduced ''worst-case'' exposure. Greater disclosure reduces and may eliminate any risk that the government could pursue theories of erroneous ''implied certification'' of parts authenticity under the False Claims Act.

Conclusion

Recent changes to counterfeit parts rules are positive. Many questions still remain, however, and the DOD should fill gaps in existing regulations and offer guidance through such means as frequently asked questions and program guidance and instructions. Many companies built and now operate their systems to detect and avoid counterfeit electronic parts upon the 2014 DFARS. Because of changes that reduce the risk of unallowable costs, and allow different risk ''tiers'' of parts sources, these should be reviewed and revised. In the same vein, many higher-tier companies drafted and use flowdown requirements, and other contract terms, based upon risks and obligations arising from the 2014 DFARS and the limited-cost ''safe harbor'' then available. These also should be reviewed and revised. Where supplier purchasing practices and harsh terms and conditions work against access to newly endorsed categories of sources — especially ''contractor-approved suppliers'' — these should be re-evaluated. New processes and procedures may be needed for source assessment and approval, and new documentation will be required to inform government customers as required by the revised DFARS.

There is much to praise in the August 2016 changes to the counterfeit electronic parts rules. They show that DOD has been listening to the experience of its suppliers and that it is working to make the rules both more practicable in application and more successful in result. Still, as evident from the foregoing analysis, adherence by the defense industrial base to the intricacies of the rule will be challenging. The rule continues to rely upon manual processes imposed upon individual contractors

and on IT&A measures at the component level. Such a manual, contractor-specific, parts-intensive approach introduces many variables in performance, and produces many types of costs and burdens affecting many functions of contractors. Is this the best way to detect and avoid counterfeit electronic parts? DOD may wish to consider systematized approaches and encourage enterprise solutions that rely on information technology, improved data collection and analytics, and coordinated assessment and approval of sources and methods. Rather than push so many well-purposed demands upon so many suppliers in the defense supply chain, DOD should examine which functions it could assume that would ease the burdens on suppliers, reduce costs and improve the outcome.

  FCR ISSN 0014-9063