COVINGTON

COVINGTON & BURLING LLP

E-ALERT | Government Contracts

May 9, 2014

DOD RELEASES FINAL DFARS RULE FOR THE DETECTION AND AVOIDANCE OF COUNTERFEIT ELECTRONIC PARTS

As part of the Government's ongoing efforts to protect supply chain integrity as it relates to Government procurement, the Department of Defense ("DoD") issued on May 6, 2014 a long-anticipated final rule imposing requirements on contractors to establish a risk-based counterfeit electronic part detection and avoidance system.

BACKGROUND

The final rule results from special provisions in the National Defense Authorization Act ("NDAA") for Fiscal Year ("FY") 2012 (§ 818) and FY 2013 (§ 833) addressing counterfeit parts. Section 818 requires the Secretary of Defense to assess DoD's "acquisition policies and systems for the detection and avoidance of counterfeit electronic parts." Section 833 addresses special allowability requirements for the costs of counterfeit electronic parts and the corrective actions associated with such counterfeit electronic parts. To implement these requirements, on May 16, 2013 DoD issued a proposed rule on counterfeit electronic parts. Covington previously reported on the proposed rule here. Over fifty respondents submitted comments to the proposed rule, and the final rule issued (and effective) May 6, 2014 incorporates these comments, as well input that DoD received from a series of public meetings. A second Defense Federal Acquisition Regulation Supplement (DFARS") case, Detection and Avoidance of Counterfeit Electronic Parts—Further Implementation has been opened, and the report is currently due May 28, 2014.

THE FINAL RULE'S REQUIREMENTS

Applicability and Definitions

The final rule addresses how contractors must treat counterfeit electronic parts in their supply chain when contracting with the Government. Among the requirements imposed by the final rule is a new DFARS clause (DFARS 252.246-7007) that outlines the actions that contractors must take to establish a counterfeit part detection and avoidance system when the Government is acquiring electronic parts, end items, components, parts or assemblies containing electronic parts, and services where the contractor will supply the same. The new DFARS clause applies to contractors subject to full or modified coverage under the Cost Accounting Standards ("CAS"), as well as all subcontractors to CAS-covered prime contractors, regardless of the subcontractor's CAS or size status. Additionally, the final rule applies to commercial items and commercial-off-the-shelf ("COTS") items if those items are subcontracted by a CAS-covered contractor. Thus, small business concerns, including commercial item suppliers, may be impacted if they fall within the supply chain of prime contractors subject to the CAS and thus also subject to the final rule. Prime contracts awarded pursuant to a small business set aside are exempt from the rule.

The final rule applies to counterfeit *electronic* parts, suspect *electronic* parts, and obsolete *electronic* parts, including any embedded software or firmware, but does not extend to all counterfeit materials and items. A "counterfeit electronic part" is "an unlawful or unauthorized reproduction, substitution, or alteration that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified electronic part from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer." An important change from the proposed rule is the inclusion of an element of intent - "knowingly" - for situations involving misrepresentation and unlawful or unauthorized substitution. "Unlawful or unauthorized substitution" is defined to include used electronic parts represented as new, or otherwise false indications of "grade, serial number, lot number, date code, or performance characteristics."

A "*suspect* counterfeit electronic part" is one "for which credible evidence (including, but not limited to, visual inspection or testing) provides reasonable doubt that the electronic part is authentic." The "credible evidence" standard is not further defined in the rule and this same standard has generated significant questions as to proper interpretation under the FAR mandatory disclosure rule and is likely to present similar questions here.

Finally, the rule requires contractors to include the control of "obsolete electronic parts" in their counterfeit part detection and avoidance system, "to maximize the availability and use of authentic, originally designed, and qualified electronic parts throughout the product's life cycle." The final rule defines an obsolete electronic part as one "no longer in production by the original manufacturer or an aftermarket manufacturer that has been provided express design activity or original manufacturer." How long and to what extent contractors must continue to maintain such obsolete electronic parts is not clear in the final rule. The preamble states that "[g]uidance and mechanisms concerning supply chain processes to mitigate risks inherent with obsolete parts" are beyond the scope of the final rule."

Minimum System Criteria for a Counterfeit Electronic Part Detection and Avoidance System

Under the final rule, covered contractors must "establish and maintain an acceptable counterfeit electronic part detection and avoidance system" which includes "risk-based policies and procedures" that, at a minimum, address twelve enumerated areas. If a covered contractor fails to meet these system minima, its purchasing system may be disapproved and/or payments may be withheld for an inadequate business system. These twelve areas are summarized below.

Training of Personnel: The first requirement is to train personnel with regard to counterfeit electronic parts. The rule offers no guidance as to the scope of the training, instead intentionally providing flexibility for contractors to determine the type of training necessary.

Inspection and Testing of Electronic Parts: An acceptable system also requires the inspection and testing of electronic parts, to include criteria for acceptance and rejection of parts. The final rule allows contractors to make "risk-based decisions based on supply chain assurance measures when determining how much inspection and testing must be conducted. The rule provides limited guidance but notes that such inspection and testing procedures should be based on the assessed probability of receiving a counterfeit electronic part; the probability that an inspection or test will detect a counterfeit electronic part; and the known potential negative consequences of a counterfeit electronic part being installed, including human safety or mission success.

This risk-based approach is consistent with the Government's recent cybersecurity initiatives, including the NIST Cybersecurity Framework and the DFARS rule for the safeguarding of unclassified

controlled technical information. This approach, however, means that contractors should carefully consider their options and document their well-reasoned decisions when appropriate.

Processes to Abolish Counterfeit Parts Proliferation and Reporting and Quarantining Counterfeit Electronic Parts: To be compliant, covered contractors also must implement processes to abolish counterfeit parts proliferation. The final rule, however, offers no guidance as to what actions are considered sufficient to meet the requirement. The preamble to the rule indicates only that the additional requirements for quarantining counterfeit electronic parts is related to this requirement. That requirement obligates a covered contractor to report to the contracting officer and to the Government-Industry Data Exchange Program ("GIDEP") when it "becomes aware of, or has reason to suspect that, any electronic part or end item, component, part, or assembly containing electronic parts . . . contains counterfeit electronic parts or suspect counterfeit electronic parts." In addition to reporting, contractors also must retain (and quarantine) the counterfeit or suspect counterfeit parts until they are determined to be authentic. Additional guidance for reporting and quarantining will be addressed in the forthcoming FAR Case 2013-002, Expanded Reporting of Nonconforming Supplies.

Processes for Maintaining Electronic Part Traceability: Covered contractors must be able to trace the supply chain of electronic parts covered by the final rule back to the original manufacturer. The final rule intentionally does not mandate specific traceability technology or processes, such as Item Unique Identification ("IUID"). However, a contractor's process must include: "certification and traceability documentation developed by the original manufacturer in accordance with Government and industry standards; clear identification of the name and location of supply chain intermediaries from the manufacturer to the direct source of the product from the seller; and where, available, the manufacturer's batch identification for the electronic part(s), such as date codes, lot codes, or serial numbers." If contractors choose to utilized IUID, they must comply with the requirements of DFARS 252.211-7003, "Item Unique Identification and Valuation."

Although there is no mandated traceability technology, the preamble to the final rule specifically notes that "[w]ith regard to mission-critical electronic parts that could impact human safety, DoD does have a zero-tolerance policy." The rule does not define what qualifies as an "impact [on] human safety" or what consequences may be imposed for failure to meet that standard.

Use of Suppliers who are the Original Manufacturer or Sources with the Express Written Authority of the Original Manufacturer: The fifth requirement is for covered contractors to obtain electronic parts from the original manufacturers or authorized sources. If parts are not available from these sources, a contractor may use suppliers that "meet applicable counterfeit detection and avoidance system criteria," though this exception is not further explained.

Methodologies to Identify Suspect Counterfeit Parts: Under the final rule, covered contractors must also institute a risk-based methodology for identifying suspect counterfeit parts (as defined above) and determining whether those parts are actually counterfeit. Following comments that only an original manufacturer can make the determination that a part is counterfeit, DoD instructs contractors to use a risk-based approach, as with inspection and testing, to make such determinations.

Design, Operation, and Maintenance of Systems to Detect and Avoid Counterfeit and Suspect Counterfeit Electronic Parts: This requirement appears to mirror the overarching requirement that covered contractors "establish and maintain an acceptable counterfeit electronic part detection and avoidance system." The only guidance provided by the final rule is that contractors may opt to use existing Government or industry standards to meet this requirement.

Flowdown of Counterfeit Detection and Avoidance Requirements: Covered contractors that engage with subcontractors to buy electronic parts or to perform authentication testing must flow down the requirements of the final rule. This flowdown is required regardless of the CAS status or size of the subcontractor or whether the electronic item or authentication service qualifies as a commercial item.

As a result of this flowdown requirement, non-CAS contractors should be aware that these requirements may nonetheless be imposed on them should they subcontract with a CAS prime.

Processes for Keeping Continually Informed of Current Counterfeiting Information and Trends and Processes for Screening the GIDEP Reports and Other Credible Sources of Counterfeiting Information: The tenth and eleventh requirements essentially require covered contractors to keep abreast of counterfeiting information and trends to maintain supply chain integrity. Such processes should include reviewing appropriate industry standards and GIDEP reports.

Control of Obsolete Electronic Parts: Finally, covered contractors must control obsolete electronic parts, defined as electronic parts no longer in production by the original manufacturer or an expressly authorized aftermarket manufacturer.

Failure to Comply

As mentioned above, failure to comply with the final rule may result in withheld payments or the disapproval of the contractor's purchasing system. One method for establishing compliance is through a Contracting Purchasing System Review ("CPSR") conducted by the Defense Contract Management Agency ("DCMA"). The final rule amends two Contractor Purchasing System Administration clauses, a basic and an alternate, at DFARS 252.244-7001, which discuss CPSR. The preamble to the rule explains that CPSRs will involve examining the contractor's policies and procedures for the detection and avoidance of counterfeit electronic parts. If the CPSR uncovers a "significant deficiency," defined as "a shortcoming in the system that materially affects the ability of officials at [DoD] to rely upon information produced by the system," the DCMA will consider whether to disapprove the contractor's purchasing system or withhold payment. Factors taken into consideration for this determination include public law violations and repeat occurrences, and whether the contractor has taken corrective action.

Cost Allowability

The final rule adds a new section to the FAR cost principles addressing the allowability of the costs of remedying the use or inclusion of counterfeit electronic parts. Costs incurred in remedying the use of counterfeit or suspect counterfeit electronic parts are expressly unallowable under the rule, unless: (1) the contractor's operational system for detecting and avoiding counterfeit electronic parts has been reviewed and approved by DoD; (2) the counterfeit or suspect counterfeit electronic parts are Government-furnished equipment; and (3) the contractor provided notice to the Government within 60 days of becoming aware of a counterfeit or suspect counterfeit electronic part.

It is likely that most CAS contractors will be able to meet the three requirements for allowable costs. For commercial item contractors who may serve as subcontractors, recovery of the costs of compliance may be more difficult because they often do not operate on a cost reimbursement basis with the Government. Thus, commercial item contractors will need to include these costs in their pricing to prime contractors, likely increasing costs to the Government.

KEY CHANGES FROM PROPOSED RULE

There were several significant changes between the May 16, 2013 proposed rule and the final rule issued on May 6, 2014.

- Clarifying that the rule Applies only to Electronic Parts: The scope of the final rule encompasses only counterfeit *electronic* parts as opposed to counterfeit parts. The preamble to the rule explains that the definition was revised because the original term was too broad.
- Shift to Risk-Based Approach: The final rule, specifically in the discussion of inspections and testing, makes clear that the contractor's system for detecting and avoiding counterfeit electronic parts should be based on a risk assessment. The risk assessment should be based on the contractor's unique supply chain and security practices, and there is no one size fits all approach.
- Suspect Counterfeit Electronic Parts: The final rule also responded to comments regarding the proposed rule's vague standard for identifying suspect counterfeit electronic parts by imposing a "credible evidence" standard, requiring that there be "reasonable doubt that the electronic part is authentic." While at first glance this standard may appear more manageable than the proposed rule, as noted above the "credible evidence" standard has proven troublesome in the mandatory disclosure arena, in that it is not defined and has created uncertainty. There is a chance of similar issues with regard to suspect counterfeit electronic parts.
- Clarification of Applicability to Commercial and COTS Items: As discussed above, the final rule clarifies that it is applicable to subcontracts for commercial and COTS items, regardless of the size or CAS status of the subcontractor.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our government contracts practice group:

Susan Cassidy	+1.202.662.5348	scassidy@cov.com
David Fagan	+1.202.662.5291	dfagan@cov.com
Alan Pemberton	+1.202.662.5642	apemberton@cov.com
Roger Zakheim	+1.202.662.5959	rzakheim@cov.com
Kathy Brown	+1.202.662.5993	kbrown@cov.com
Catlin Meade	+1.202.662.5889	cmeade@cov.com