

## GOVERNMENT CONTRACTS UPDATE

---

June 2014

### **RISKY BUSINESS: HOW RULES GOVERNING COUNTERFEIT ELECTRONIC PARTS AND REPORTING ON NONCONFORMANCE HAVE PUT RISK AT A PREMIUM IN THE GOVERNMENT'S SUPPLY CHAIN**

#### AUTHORS

Paul A. Debolt  
Keir X. Bancroft

#### RELATED PRACTICES

Government Contracts

#### RELATED INDUSTRIES

Government Contractors

#### ARCHIVES

2014 2010 2006  
2013 2009 2005  
2012 2008 2004  
2011 2007

Any contractor or subcontractor supplying the government with electronic parts or other items should consider new rules aimed at controlling counterfeit electronic parts and monitoring for nonconformance. In an industry where cybersecurity regulations are on the rise, suppliers risk nonpayment, claims of breach, or worse if they ignore these new rules, which have already been incorporated into the Defense Federal Acquisition Regulation Supplement ("DFARS") and which may soon be incorporated into the Federal Acquisition Regulation ("FAR").

#### **CAS-Compliant Contractors Must Comply With DFARS Rules on Detection and Avoidance of Counterfeit Electronic Parts**

As Venable [reported earlier](#), under a new DFARS clause, contractors subject to the cost accounting standards ("CAS") who supply the Government with electronic parts will need to develop a counterfeit electronic parts avoidance and detection system featuring the 12 criteria (the top three of which were added in the final rule):

1. **Keeping continually informed of counterfeiting information and trends**
2. **Screening Government/Industry Data Exchange Program ("GIDEP") reports and other credible sources of information**
3. **Control of obsolete electronic parts**
4. Personnel training
5. Electronic parts inspection and testing
6. Abolish counterfeit parts proliferation
7. Electronic parts traceability
8. Using OEMs or other sources with written authorization
9. Reporting and quarantining of both suspect and actual counterfeits
10. Methods for rapidly confirming counterfeits
11. Design, operation and maintenance of detection and avoidance systems
12. Flowdowns to all levels of the supply chain

Other key changes in the new rules include:

- Limiting the rule's coverage by clarifying its application to counterfeit "electronic" parts;
- Adding an element of intent to the definition of a counterfeit by specifying it is "knowingly" mismarked, misidentified, or otherwise misrepresented to be authentic;
- Revising and expanding the definition of "suspect counterfeit part" as one "for which credible evidence . . . provides reasonable doubt" that it is authentic; and
- Including a new definition of "obsolete part" encompassing parts "no longer in production[.]"

While implementing a number of new requirements, the final rule does preserve elements of the proposed rule. For example, though it applies to contractors subject to CAS, it includes a mandatory flowdown clause that may apply to small business subcontractors, and under subcontracts for commercial items. The rule again states that costs for rework and corrective action are unallowable; it

offers a limited safe harbor allowing costs for contractors with approved avoidance and detection systems, detecting counterfeits in Government-furnished property, and supplying timely notice.

Though compliance with the new DFARS rule will likely be costly, failure to maintain an avoidance and detection system prescribed by the rule could result in disapproval of a contractor's purchasing systems or the withholding of payments the system fails.

### **Proposed FAR Rule on Expanded Reporting of Nonconforming Items**

A new FAR rule has been proposed that may expand reporting requirements to agencies beyond just the DOD, that will apply to prime contractors not subject to CAS compliance, and address supplies beyond the realm of electronic parts. The proposed FAR requirement would expand a contractor's responsibility to provide written reports to, and to screen reports in, the GIDEP.

### **New Contractor Reporting and Notification Requirements**

Under the proposed rule, a contractor must provide notice when:

1. The contractor becomes aware ***that any end item, component, subassembly, part, or material contained in supplies*** purchased by the contractor for delivery to or for the Government is counterfeit or suspect counterfeit. (In those cases, written notification is required within 30 days and the contractor must retain the nonconforming items if possible).
2. The contractor becomes aware that an item purchased by or for the contractor for delivery to or for the Government is counterfeit or suspect counterfeit, ***or contains a major or critical nonconformance that is a common item and constitutes a quality escape resulting in the release of like nonconforming items to more than one customer.*** (In those cases, the contractor must make a report to GIDEP within 60 days.)

The proposed rule clarifies that the term "common item" is defined as "an item that has multiple applications versus a single or peculiar application," and the term "quality escape" means "a situation in which a supplier's internal quality control system fails to identify and contain a nonconforming condition."

#### *New Contractor Screening Requirements*

Contractors must also screen GIDEP reports to avoid the use and delivery of counterfeit or suspect counterfeit items or items that contain a major or critical nonconformance.

The proposed rule will have a wide scope. There are no apparent exceptions for small businesses, and the rule will apply to commercial items and non-commercial items, as well as purchases above and below the simplified acquisition threshold. Contractors will be able to sign up to receive alerts from GIDEP via email about new reports submitted concerning any items included on a list they supply.

*Comments on the proposed FAR regulations are due by August 11, 2014.*

For more information on how the final and proposed regulations might impact your business, or to better understand the requirements regarding counterfeit electronic parts or reporting nonconforming items, please contact [Paul Debolt](#) at , [Keir Bancroft](#) at , or any of the other attorneys in Venable's **Government Contracts Practice Group**.