VENABLE® LLP

Government Contracts Update

February 2012

Are Those Real Parts? Government Contractors Must Comply With New Inspection and Reporting Requirements Created by NDAA 2012 for Counterfeit Electronic Parts

AUTHORS

Paul A. Debolt

George W. Wyatt

RELATED PRACTICES

Government Contracts

RELATED INDUSTRIES

Government Contractors

ARCHIVES

2012 2008 2004
2011 2007 2003
2010 2006 2002
2009 2005

The recently enacted National Defense Authorization Act ("NDAA") of 2012 establishes a host of new requirements for government contractors regarding detection and avoidance of counterfeit electronic parts. These new requirements will apply to any contractor who is subject to cost accounting standards and supplies products or weapons systems with electronic parts to the Department of Defense ("DoD"). Contractors who fail to follow these new requirements risk suspension, debarment and potential civil and criminal liability.

The NDAA 2012 requires the Secretary of Defense to first assess DoD acquisition policies and systems for how they detect and avoid counterfeit electronic parts. Then, no later than June 28, 2012, the Secretary is to implement a risk-based policy to minimize the impact of counterfeit electronic parts, which includes ensuring the traceability of parts, inspecting and testing of parts, and taking corrective action to recover costs for replacing counterfeit electronic parts from contractors. At that time, the Secretary is also to issue guidance on remedial actions for DoD to take – including consideration of suspension and debarment – against contractors who have failed to detect or avoid counterfeit electronic parts or who have "failed to exercise due diligence in the detection and avoidance" of counterfeit electronic parts.

The NDAA 2012 also requires the Secretary, no later than September 26, 2012, to revise the DFARS to address the detection and avoidance of counterfeit electronic parts. These regulations will shift the burden of detecting counterfeit electronic parts to the contractors. In particular, the new regulations will make contractors responsible for detecting and avoiding the use of counterfeit electronic parts, as well as for any rework or corrective action that may be required to remedy the use or inclusion of such parts. The cost for detecting and avoiding counterfeit electronic parts and the cost of any rework or corrective action required because of counterfeit electronic parts will not be an allowable cost.

The revised DFARS will also establish requirements for the inspection, testing and authentication of electronic parts that a contractor or subcontractor obtains from sources other than the original manufacturers of the parts or their authorized dealers. The DFARS will also be revised to establish a written reporting system, under which a contractor or subcontractor who becomes aware, or has reason to suspect, that a component, part or material supplied to the DoD contains counterfeit electronic parts has 60 days to report it to the Government. There is a safe harbor from civil liability if a contractor complies with this written reporting requirement, but that safe harbor is only available if the contractor made a "reasonable effort" to determine whether the items supplied contained counterfeit electronic parts.

The NDAA 2012 further requires the Secretary to implement a program of contractor detection and avoidance of counterfeit electronic parts. Contractors that supply electronic parts or systems that contain electronic parts will be required to establish policies and procedures to eliminate counterfeit electronic parts from the defense supply chain. Those policies and procedures will cover the inspection and testing of electronic parts, mechanisms for the traceability of parts, use of trusted suppliers, the reporting and quarantining of counterfeit electronic parts, methodologies for identifying counterfeit electronic parts, and the flow down of requirements to subcontractors.

Finally, the NDAA 2012 creates new criminal liability for trafficking in counterfeit goods or services with fines of $2,000,000 for individuals and $5,000,000 for companies and up to ten years in prison for first offenses. Those fines and prison terms significantly increase for repeat offenders or for counterfeit military goods or services or in cases where the counterfeit parts lead to bodily injury.

Given that a counterfeit electronic part may have entered the supply chain with a manufacturer of a single component four or five steps removed from the end product supplied to DoD, the difficulty for

government contractors to ensure these counterfeit electronic parts are detected cannot be overstated. Not only will contractors now have to engage in additional inspection and testing, they will also face unrecoverable costs of replacing counterfeit parts that go undetected, as well as risk possible suspension or debarment. In addition, contractors risk criminal liability and the ever-present threat that an employee will rush to file a *qui tam* action under the civil False Claims Act based on the presence of unreported counterfeit parts. In short, the NDAA creates an onerous inspection and reporting regime which government contractors will struggle to comply with in the future. Contractors must begin to plan now for how they will address this serious risk.

For more information on the new requirements in the NDAA 2012 regarding counterfeit electronic parts, please contact **Paul Debolt** at **padebolt@Venable.com**, **George Wyatt** at **gwwyatt@Venable.com** or any of the other attorneys in Venable's **Government Contracts Practice Group**.