

Reproduced with permission from Federal Contracts Report, 104 FCR , 8/4/15. Copyright © 2015 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

DOD

DCMA Instruction Said to Ease Burden in Detecting Counterfeits

By DAVE HANSEN

A recent Defense Contract Management Agency (DCMA) Instruction for overseeing contractors' efforts to exclude counterfeit electronic parts from their supply chains is in some ways industry-friendly, Rogers Joseph O'Donnell, PC Shareholder Robert Metzger told Bloomberg BNA in an e-mail July 24.

In particular, he said the Instruction calls for a "pragmatic" approach to looking for counterfeits that's based on risk, which is more realistic than trying to devote 100-percent effort to entire supply chains. But Metzger and other practitioners also noted changes they would like to see, including more specific information about acceptable systems for detecting electronic parts, how DCMA oversight will be conducted, and reporting responsibilities when counterfeit electronic parts are found.

"Overall, the Instruction is a positive step," he said. "The threat of counterfeits is very real, and every participant in the defense supply chain should be vigilant" in detecting and avoiding them.

The Instruction complies with the anti-counterfeiting provisions in section 818 of the fiscal 2012 National Defense Authorization Act (96 FCR 621, 12/20/11). Section 818 requires contractors to purchase electronic parts from manufacturers, authorized dealers or trusted suppliers. It also requires large defense contractors to create systems to detect and avoid counterfeit electronic parts.

The DOD issued a final rule in May 2014 to implement the act, tasking the DCMA with reviewing and approving contractors' systems to detect counterfeits (101 FCR 507, 5/6/14).

'Risk-Based' Approach. The Instruction directs both the DCMA and contractors to focus on materiel purchases that have the greatest risk when it comes to counterfeit electronic parts.

The Instruction also requires the DCMA to evaluate the risk of counterfeit electronic parts as "high," "moderate," or "low." Parts with a high risk will require more frequent monitoring, the Instruction says.

This scoring system recognizes that harder-to-obtain materiel presents a moderate risk, Metzger said. It also acknowledges that companies may use distributors that were not franchised or factory-authorized for such parts.

"This should help assure many companies that they can comply...even where they have no choice other than to buy out-of-production, obsolete or otherwise unavailable parts from distributors," he said.

At the same time, he said a risk-based approach "clearly favors distributors with a proven track record" that are already qualified by the Defense Logistics Agency.

Technical Specialists. The guidance assigns to trained "technical specialists" the task of reviewing a contractor's counterfeit detection systems. Metzger said this should improve contractor guidance and oversight.

The Instruction also directs DCMA personnel to report counterfeit parts to the "Contract Integrity Center" (CIC). The CIC coordinates investigations by DCMA personnel, criminal investigators, intelligence authorities and other stakeholders. It also provides guidance on actions taken in response to reports.

Assigning the CIC this responsibility will centralize decisions and improve consistency and accountability when follow-up actions are taken, Metzger said.

'Mixed Bag.' The Instruction is a "mixed bag," Foley & Lardner LLP Senior Counsel Frank Murray told Bloomberg BNA in an e-mail July 27.

Although it's helpful in some ways, it has only limited information on acceptable specific processes and procedures for detecting counterfeits, he said.

According to Murray, this could result in different technical specialists viewing the same detection system differently, which would make life more difficult for contractors. A related problem is that a contractor's counterfeit-detection system could be deemed inadequate based on the presence of just one counterfeit part.

The Instruction answers some questions but raises others, Crowell & Moring Partner Peter Eyre told Bloomberg BNA July 28.

For example, although it charges DCMA with verifying that contractors establish early detection procedures, it fails to say how that oversight will be conducted, he said.

The Instruction also states that if DCMA identifies deficiencies in a contractor's counterfeit detection system, certain stakeholders will be notified. But there's no mention of what information will be circulated or how it will be used, Eyre said.

Additional Changes. The Instruction categorizes the risk of a counterfeit electronic part according to the source of the part but not its use. Metzger said a better practice, which is standard in the industry, is to con-

sider the nature of the component and how it's used when calculating risk.

He also said it's important to consider the consequences of a part failure "at the system level" and whether safety or mission performance would be compromised.

In addition, he said although the Instruction informs the DCMA of what to do and whom to consult within the government when a suspect counterfeit is identified, it doesn't completely resolve who in the supply chain should notify the Government-Industry Data Exchange Program (GIDEP) or when they should do so.

The DCMA is supposed to encourage contractors to report counterfeits to GIDEP and can do so on their behalf if they don't, Metzger said. "This will generate some industry resistance, because some believe that there is an adverse stigma associated with any reporting to GIDEP," he said.

To contact the reporter on this story: David Hansen in Washington at dhansen1@bna.com

To contact the editor responsible for this story: Jeff Kinney at jeffkinney@bna.com

The DCMA Instruction is available at:<http://www.dcmamil/policy/1205/DCMA-INST-1205.pdf>.