NEWSLETTER

DOD and GSA Issue Cybersecurity Recommendations

February 2014

Authors

Kevin J. Maynard
Partner
202.719.3143
kmaynard@wiley.law

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

On January 23, 2014, the U.S. Department of Defense (DOD) and General Services Administration (GSA) Joint Working Group on Improving Cybersecurity and Resilience Through Acquisition issued a final report, "Improving Cybersecurity and Resilience through Acquisition," outlining several recommendations regarding the incorporation of security standards into acquisition planning and contract administration. The report is one of several cybersecurity-related initiatives undertaken by the Executive branch in response to the President's February 12, 2013 Executive Order (EO) for Improving Critical Infrastructure Cybersecurity (EO 13636).

The recommendations seek to strengthen the government's cyber resilience by increasing the use of cybersecurity standards in federal acquisitions, and by improving government management of the people, processes, and technologies involved in the procurement of information and communication technology. Although the Joint Working Group's recommendations are relatively broad and will require development of additional rules and contracting strategies, the report includes a number of recommendations that should be of particular interest to federal contractors, including the following:

- **Include Cybersecurity Requirements as a Condition of Contract Award.** First, the government should institute baseline cybersecurity requirements (*e.g.*, anti-virus protection, security software patches, etc.), as a condition of contract award in acquisitions that present cyber risks. In particular, DOD and GSA recommend that contracting agencies include cybersecurity requirements among technical specifications, and use performance measures to ensure that cyber risks are identified and mitigated throughout the lifespan of the product or service being procured.

This dovetails with a final rule DOD issued in November 2013 requiring contractors to implement security programs on systems that store or transmit "unclassified controlled technical information," a category of information that includes all technical data and computer software with military or space applications subject to DOD access controls. 78 Fed. Reg. 69273; *see* Wiley Rein Client Alert, *New DOD Final Rule Imposes Cyber-Reporting Obligations and Basic Safeguarding Protocols for "Unclassified Controlled Technical Information."* Additional rulemaking is anticipated in response to the Joint Working Group's recommendation, particularly in light of DOD's statement in the final rule that it intends to address "basic" security requirements for a broader range of unclassified nonpublic information in an upcoming final rule.

- **Conduct Cybersecurity Training.** Second, DOD and GSA recommend that the government address cybersecurity through training, particularly for potential offerors and other industry stakeholders. The report highlights GSA's "Pathway to Success" training for vendors seeking Multiple Award Schedule contracts as an example of a program that could incorporate specific training regarding cyber risk management.
- **Develop Common Set of FAR Definitions.** Third, to promote efficiency and effectiveness of cybersecurity initiatives in government contracting, the government should develop common cybersecurity definitions for inclusion in the Federal Acquisition Regulation (FAR). The Joint Working Group intends for this recommendation to be harmonized with the ongoing DFARS rulemaking, "Detection and Avoidance of Counterfeit Electronic Parts." *See* 78 Fed. Reg. 28780; *see also* Wiley Rein Client Alert, *DOD Releases Long-Awaited Proposed Rule on C ounterfeit Electronic Parts*.
- **Implement "Cyber Risk Management Strategy" for Federal Acquisitions.** Fourth, the government should implement an interagency "federal acquisition cyber risk management strategy." To facilitate this goal, the government should develop "overlays"—fully specified sets of security requirements that facilitate tailoring security requirements for specific products, risks, and circumstances.
- **Require Purchases from "Trusted Sources."** Fifth, DOD and GSA recommend that certain acquisitions require contractors to purchase from original equipment manufacturers, authorized resellers, or other trusted sources to ensure that end items and components have the latest security updates. Eligible suppliers would be identified through qualified products, bidders, or manufacturers lists (QBL) developed using a broad set of criteria, including long-term business viability, quality control systems, and customer support. However, because implementation of this recommendation would necessarily limit available sources, the report recommends that this approach only be used for acquisitions that present significant cyber risks.
- **Increased Accountability.** Sixth, the government should increase contracting agencies' accountability for cyber risk management. To do so, the Joint Working Group recommends that the government integrate security standards into each step of the acquisition process; definition of requirements, development of the solicitation, source selection, conformance testing, technology refresh reviews, and on through the rest of contract performance.

The report advises that implementation of these recommendations should be aligned with other efforts to improve cybersecurity infrastructure, including the Comprehensive National Cybersecurity Initiative, the Cybersecurity Framework developed under the EO, the National Infrastructure Protection Plan, and other risk assessment and management activities.