wiley

ALERT

GSA Seeks Input on How Procurement Policy Can Drive Cybersecurity Improvements

May 17, 2013

On Tuesday, May 14, the General Services Administration (GSA)-led Joint Working Group on Improving Cybersecurity and Resilience Through Acquisition released a request for information (RFI) seeking input on the feasibility, security benefits and relative merits of incorporating security standards into acquisition planning and contract administration, as well as steps that could be taken to harmonize existing procurement requirements related to cybersecurity. *See* 78 Fed. Reg. 27966 (May 13, 2013).

The RFI is one of several activities being undertaken throughout the Executive branch on cyber after President Obama's February 12 Executive Order for Improving Critical Infrastructure Cybersecurity (Executive Order 13636). Section 8(e) of Executive Order 13636 requires GSA and the Department of Defense, in consultation with the Department of Homeland Security and the FAR Council, to make recommendations on cybersecurity-related acquisition procedures that could be used to strengthen the Government's cybersecurity posture. The RFI is one of several public outreach initiatives that the Joint Working Group has undertaken, and includes 37 specific questions for industry on three core issues, including (i) the feasibility of adopting cybersecurity standards in federal acquisitions, (ii) commercial procurement practices related to cybersecurity and (iii) opportunities to harmonize potential conflicts in statutes, regulations, policies, practices and contractual terms related to cybersecurity. The RFI invites comments that highlight any applicable distinctions in responses related to classified and unclassified acquisitions.

Several of the RFI questions suggest a potential shift toward a set of uniform cybersecurity "baseline" standards for federal contractors that manage federal IT systems or maintain government information

Authors

Jon W. Burd
Partner
202.719.7172
jburd@wiley.law

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Nova J. Daly
Senior Public Policy Advisor
202.719.3282
ndaly@wiley.law

Practice Areas

Government Contracts

on their own IT systems. One of the anticipated challenges to developing and implementing effective uniform baselines will be to harmonize any such "baseline" with the Federal Information Security Management Act (FISMA), which generally delegates responsibility for implementing information security compliance to individual agency heads, based on each agency's unique cyber risk assessment. *See* generally 44 U.S.C. § § 3543, 3544. One approach that the Joint Working Group has considered includes establishing multiple tiers of cybersecurity standards to correspond to a range of cyber risk levels, from which agency heads could select the appropriate tier of standards given their unique IT requirements and cyber risk assessments.

The RFI comment deadline is June 12, 2013, but GSA has encouraged industry to provide comments as soon as possible because the Joint Working Group's deadline for reporting on the Executive Order initiatives coincides with the June 12 comment deadline. The ultimate report to be issued by GSA and the Department of Defense will likely have lasting impact on federal procurement policy and practice, especially given the heightened sensitivity in Congress and with the Administration on cybersecurity protection.

Given the speed with which recommendations and actions are being taken throughout the Executive branch, government contractors and other companies and industry groups that indirectly supply IT resources to the federal government should closely watch this proceeding and consider making their views known. This is an important opportunity for industry to shape federal cybersecurity policies that may emerge from the report, and ensure that they are well-informed and appropriately balance business practicality and efficiency with national security.