WILMERHALE

GSA-Joint Cybersecurity Working Group Issues Request for Information on Cybersecurity Standards in Government Contracts

2013-05-13

Today, in response to a directive in President Obama's February Executive Order on Critical Infrastructure Cybersecurity, the Joint Working Group on Improving Cybersecurity and Resilience through Acquisition ("Joint Working Group"), headed by the General Services Administration, published a Request for Information ("RFI") to be used in its report to the President making recommendations on the possibility of incorporating cybersecurity standards into federal acquisition planning and contract administration, and, to the extent applicable, the foundation for establishing or identifying government-wide cybersecurity contracts.[1] Comments are due by June 12, 2013.

Background

Under Section 8(e) of President Obama's Critical Infrastructure Cybersecurity Executive Order,[2] the GSA and the Department of Defense ("DoD"), in consultation with the Department of Homeland Security ("DHS") and the Federal Acquisition Regulation Council ("FAR Council") are to make recommendations to the President, within 120 days, "on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration . . . [including] what steps can be taken to harmonize and make consistent existing procurement requirements related to cybersecurity."[3] Presidential Policy Directive 21, which accompanied the Executive Order, directed GSA, in consultation with DoD, DHS, and other appropriate departments and agencies, to "provide or support government-wide contracts for critical infrastructure systems and ensure that such contracts include audit rights for the security and resilience of critical infrastructure."[4]

To accomplish these tasks, GSA and DoD have formed the Joint Working Group, which is led by GSA and includes representatives from DoD, GSA, DHS, the Office of Federal Procurement Policy ("OFPP"), and the National Institute of Standards and Technology ("NIST"). The Joint Working Group is reaching out to all stakeholders, including industry, and is engaged with the DHS Interagency Task Force ("ITF"), a group established by DHS for overall coordination of the implementation of the Executive Order and PPD-21.[5]

The Request for Information

The RFI requests comments on several categories of information, including: (1) the feasibility of incorporating cybersecurity standards into federal acquisitions; (2) commercial procurement cybersecurity; and (3) "any conflicts in statutes, regulations, policies, practices, contractual terms and conditions, or acquisition processes affecting federal acquisition requirements related to cybersecurity and how the federal government might address those conflicts."[6] For example, the Joint Working Group is interested in proposals for the most feasible methods for incorporating cybersecurity standards into government contracting; the implications of imposing baseline standards; the challenges in developing cross-sector standards; how contract types and source selection methods impact a contractor's cybersecurity risk assessment; whether there are widely accepted risk analysis frameworks used within particular sectors that could be adopted to federal acquisitions; and what cybersecurity requirements affecting procurement currently exist.[7] Commenters are also instructed to highlight any applicable distinctions between classified and unclassified acquisitions.[8]

Implications

This RFI presents an opportunity for government contractors to share their views on possible future cybersecurity mandates on government contractors. The government possesses considerable authority to regulate contractors' information security practices under the Federal Information Security Management Act.[9] As with other government contracting requirements, this could open new avenues for potential False Claims Act liability. Contractors should seize the opportunity to participate in this discussion to help shape any possible future procurement preferences or contract administration requirements.

---

[1] Joint Working Group on Improving Cybersecurity and Resilience Through Acquisition Request for Information, 78 Fed. Reg. 27,966 (May 13, 2013) (hereinafter "RFI"), available here.

[2]Exec. Order No. 13,636, Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11,637 (Feb. 12, 2013). For more information on this Executive Order, see http://www.wilmerhale.com/pages/publicationsandnewsdetail.aspx?NewsPubId=10737420369.

[3]*Id*. §8(e). Note that, under the Executive Order, this report is due the same day as the close of the comment period for the RFI. Thus, it appears unlikely that the report will be produced by the June 12 (120-day) deadline.

[4]Presidential Policy Directive-21 (Feb. 12, 2013), available at http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[5] The ITF has eight working groups, drawing on representatives from differing combinations of agencies: (i) stakeholder engagement, (ii) cyber-dependent infrastructure identification, (iii)

planning and evaluation, (iv) situational awareness and information exchange, (v) incentives, (vi) framework collaboration, (vii) assessments: privacy and civil liberties and civil rights, and (viii) research and development. A description of the working groups and their tasks can be found in Implementation of the Cybersecurity Executive Order and Presidential Policy Directive: Timetable and Processes.

[6] RFI.

[7] *Id*.

[8] *Id*.

[9] 44 U.S.C. § 3541 et. seq.