WILMERHALE

Defense Department and GSA Issue Recommendations for Improving Cybersecurity in Government Contracting

2014-01-27

On January 23, the Department of Defense and the General Services Administration published their joint recommendations to the President "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."[1] The report, issued pursuant to President Obama's February 2013 Executive Order on Improving Critical Infrastructure Cybersecurity, "focus[es] on driving consistency in interpretation and application of procurement rules and incorporation of cybersecurity into the technical requirements of acquisitions."[2] Although the recommendations are high-level and do not directly impose new acquisition rules, we anticipate that these recommendations will influence future acquisitions and the adoption of new acquisition rules.

The report makes the following recommendations:

1. **Institute Baseline Cybersecurity Requirements for Acquisitions Where Cyber Risk is Present**: The government should do business only with companies that meet baseline cybersecurity measures in their operations and in the products and services they provide. Agencies should include these baseline requirements, with performance metrics, in the technical specifications for particular acquisitions. Agencies should take an incremental, risk-based approach to increasing contractual cybersecurity requirements beyond the baseline.[3] This recommendation is meant to be harmonized with the recent FAR and DFARS rulemakings on "Basic Safeguarding of Contractor Information Systems" and "Safeguarding Unclassified Controlled Technical Information."[4]
2. **Address Cybersecurity in Training and Public Outreach**: Agencies should institute public and private sector workforce training to increase knowledge and understanding of the importance of cybersecurity in government acquisition. In outreach to the private sector, the government should make clear that it is "changing its buying behavior with respect to cybersecurity."[5]
3. **Define Common Cybersecurity Terms for Federal Acquisitions**: Key terms should be defined in the FAR and DFARS.[6] This recommendation is intended to be reflected in the current DFARS rulemaking on "Detection and Avoidance of Counterfeit Electronic Parts."[7]

4. **Institute a Federal Acquisition Cyber Risk Management Strategy**: The government should identify a government-wide hierarchy of cyber risks, aligned with the methodologies and procedures from the Cybersecurity Framework being developed by the National Institute of Standards and Technology (NIST). To promote consistency, the government should develop tailored sets of security requirements and supplemental guidance for specific technologies or operational environments. These "overlays" should be included in contracts where the particular cyber risks are present.[8]
5. **Purchase from Original Equipment Manufacturers (OEMs), Their Authorized Resellers, or Other "Trusted" Sources**: In some cases, the risk of receiving counterfeit or otherwise nonconforming items is best mitigated by purchasing products directly from OEMs, authorized resellers, or other trusted sources. This requirement should be implemented consistently across the federal government. If the government chooses to purchase from another source, the government should obtain assurances of the security and integrity of the item.[9]
6. **Increase Government Accountability for Cyber Risk Management**: Government acquisition practices should be modified to incorporate cyber risk considerations into all phases of acquisition planning and contract administration. Key decisionmakers should be accountable for managing cyber risks in federal acquisitions.[10]

Implications

The DoD-GSA report provides a plan for further actions by the government. It is based on two premises: (1) the government's reliance on information and communications technology will continue to grow and (2) "[p]urchasing products and services that have appropriate cybersecurity designed and built in may have a higher up-front cost in some cases, but doing so reduces total cost of ownership by providing risk mitigation and reducing the need to fix vulnerabilities in fielded solutions."[11]

The report concludes that the government must "chang[e] its buying behavior with respect to cybersecurity."[12] Though high-level and process-oriented, the recommended changes could significantly affect both acquisition planning and contract administration. The report calls for changes to the FAR and DFARS and standard cybersecurity specifications for Government procurement. Government contractors should be prepared to express their views when these recommendations are implemented in the future.

---

[1] Exec. Order No. 13,636, § 8(e), Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11,637 (Feb. 12, 2013). For more information on the Executive Order and the tasks it mandates, see http://www.wilmerhale.com/pages/publicationsandnewsdetail.aspx?NewsPubId=10737420369. The Report, "Improving Cybersecurity and Resilience Through Acquisition," prefaced by a Memorandum from Chuck Hagel, Secretary of Defense and Daniel M. Tangherlini, Administrator of General Services, to the Assistant to the President for Homeland Security and Assistant to the President for Economic Affairs (Jan. 23, 2014), can be found at: http://www.pubklaw.com/docs/finalcybersecurity01214.pdf (hereinafter, DoD-GSA Report).

[2] *Id*. at 4, 7.

[3] *Id*. at 7, 13-14.

[4] *Id*. at 14; 77 Fed. Reg. 51,496 (Aug. 24, 2012); 78 Fed. Reg. 69273 (Nov. 18, 2013).

[5] DoD-GSA Report at 7, 14-15.

[6] *Id*. at 7, 15.

[7] *Id*. at 15; 78 Fed. Reg. 28,780 (May 16, 2013).

[8] DoD-GSA Report at 7-8, 15-17. As models for overlays, the Report cites the Federal Risk Authorization and Management Program (FedRAMP), the government-wide program that provides a standardized approach to cybersecurity in cloud services; the Information Systems Security Line of Business, a set of controls and measures for security in federal information systems; and the Federal Strategic Sourcing Initiative.

[9] *Id*. at 8, 17-18.

[10] *Id*. at 8, 18-19.

[11] *Id*. at 6.

[12] *Id*. at 15.

Authors

Benjamin A. Powell

PARTNER

Co-Chair, Cybersecurity and Privacy Practice

Co-Chair, Artificial Intelligence Practice

benjamin.powell@wilmerhale.com

+1 202 663 6770

Barry J. Hurewitz

PARTNER

barry.hurewitz@wilmerhale.com

+1 202 663 6089