Advisory

JANUARY 2014

If you have any questions about this Advisory, please contact:

DAVID HALL
215.988.8325
dhall@wiggin.com

JOHN KENNEDY
203.363.7640
jkennedy@wiggin.com

ELISE GARBER
215.988.8314
egarber@wiggin.com

MICHAEL MCGINLEY
203.363.7638
mmcginley@wiggin.com

Federal Contractors: Meet the New Cybersecurity Standards or Lose Your Government Book

On January 23, 2014, Secretary of Defense Chuck Hagel and General Services Administration ("GSA") Administrator Daniel Tangherlini sent a strong message to Federal contractors and their suppliers: practice cybersecurity or the government will look elsewhere for the $500 billion in goods and services it procures annually.

Hagel and Tangherlini delivered this message in a report to the White House titled, "Improving Cybersecurity and Resilience through Acquisition" (the "Report"), which contains six recommendations designed to integrate cybersecurity into the Federal Acquisition System. The Report articulates the Department of Defense ("DoD") and GSA response to Section 8(e) of Executive Order 13636, which President Obama issued last February and which directed the DoD and GSA to advise the Administration on the feasibility, security benefits, and merits of incorporating security standards into the Federal acquisition and contracting system.

MAJOR CHANGES FOR CONTRACTORS

The Report calls for major changes to the Federal Acquisition System that will change the way most contractors conduct business with the DoD. Significantly, the Report recommends that for Federal acquisitions with cyber risk, "the government should only do business with organizations that meet such baseline requirements in both their own operations and in the products and services they deliver."

Citing the need to align cyber risk management with Federal acquisition processes, the Report highlights "the importance of cybersecurity relative to the other priorities in Federal acquisition." Although the Report does not provide implementation guidance, it does provide strategic guidance and it unambiguously communicates the government's desire that cybersecurity be "built in" to products and services. It also explains that DoD and GSA are willing to accept a higher up-front cost to obtain cybersecurity measures under the philosophy that such risk mitigation measures will lower the total cost of ownership.

This new cost-risk trade-off appears to be the result of the government's perception that cybersecurity risk in its acquisition system is unacceptably high. According to the Report, the "government and its contractors, subcontractors, and suppliers at all tiers of the supply chain are under constant attack" and adversaries are targeting businesses "deep in the government's supply chain." Once these adversaries have infiltrated the government's supply chain, they "'swim upstream' to gain access to sensitive information and intellectual property."

THE RECOMMENDATIONS

To address this unacceptable level of cybersecurity risk in the Federal Acquisition System, the Report makes six recommendations:

(1) *Institute baseline cybersecurity requirements as a condition of contract award for appropriate acquisitions.*

CONTINUED ON NEXT PAGE

Federal Contractors: Meet the New Cybersecurity Standards or Lose Your Government Book CONTINUED

Calling baseline "cybersecurity hygiene" a concept that is "broadly accepted across the government and the private sector," the Report discourages the Federal Acquisition Workforce from doing business with organizations that do not practice baseline cybersecurity (*e.g.,* updated virus protection, multiple-factor logical access, and current security software patches). The Report recommends that cybersecurity requirements should be "specifically articulated" in acquisition contracts—not only to set security requirements for the products and services to be delivered to the government, but also to set cybersecurity requirements for a contractor's own operations.

(2) *Address cybersecurity in relevant training.* The Report states explicitly that the government is "changing its buying behavior relative to cybersecurity" and so will require more cybersecurity knowledge from its contractors. This means that contractors may soon be required to take tailored cybersecurity training. In fact, if a Federal acquisition contract involves cyber risk, the government may require such training in order for a contractor even to be considered a qualified bidder for the contract. The Report suggests that such training could mirror the mandatory training the GSA requires for contractors seeking to submit proposals for certain contracts. Additionally, the Report recommends that contractors, under certain circumstances, would be required to complete cybersecurity training throughout the performance of a contract.

(3) *Develop common cybersecurity definitions for Federal acquisitions.* The Report calls for improving the clarity of key cybersecurity terms in the Federal acquisition process so that a common language can bridge both the private and public sectors and the cyber, legal, and acquisition communities. Rather than attempting to define specific terms, the Report refers to "consensus based, international standards" as "a good baseline" if such standards can be harmonized with the Federal Acquisition Regulation.

(4) *Institute a Federal acquisition cyber risk management strategy.* The Report calls for an "interagency acquisition cyber risk management strategy" that would fall under the umbrella of the government's enterprise risk management strategy. The strategy would align with the methods and procedures addressing cyber risk that are outlined in the Cybersecurity Framework created by the National Institute of Standards and Technology ("NIST"). An important component of this strategy is the development of "overlays"—security requirements and guidance that would allow the government to adopt standard cybersecurity requirements across market segments and similar procurement types while maintaining its ability to tailor security requirements based on specific conditions or technologies for an individual acquisition. These overlays would be developed with industry participation.

(5) *Include a requirement to purchase from original equipment manufacturers, their authorized retailers, or other "trusted" sources, whenever available, in appropriate acquisitions.* Recognizing that original equipment manufacturers ("OEMs") have a heightened incentive to ensure the authenticity of their products, and thus to mitigate cybersecurity risks throughout their supply chain, the Report recommends that items be obtained from OEMs where possible and otherwise through trusted sources identified through the use of qualified products, bidders, or manufacturers lists ("QBL"). The government will determine whether a contractor is a "trusted" source based on several criteria, including long-term business viability, quality control systems, order placement and fulfillment processes, customer support, customer return policies, and a contractor's record of performance on government contracts.

(6) *Increase government accountability for cyber risk management.* This final recommendation places increased accountability on government acquisition managers to ensure cybersecurity risks are considered and mitigated at every stage of the acquisition. Specifically, the Report recommends that acquisition managers address cyber risk from requirement design and analysis through solicitation, source selection, and other cyber-related post-award contract performance matters. Ultimately, key acquisition decision makers will be "accountable for decisions regarding the threats, vulnerabilities, likelihood, and consequences of cybersecurity risks in the fielded solution." As a result of their increased accountability, these acquisition decision makers are likely to place increased pressure on their contractors to provide them with better cyber risk insight.

Contractors underestimate the significance of these recommendations at their own peril. While the Report states that its recommendations are focused on government acquisition managers, the Report also acknowledges that cyber resilience will not be achieved without cooperation between the public and private sectors and supply chain suppliers and providers.

In sum, these recommendations mean increased scrutiny for Federal contractors and their suppliers, particularly regarding the documentation and execution of their cybersecurity programs. Contractors should be prepared to defend their cybersecurity programs and demonstrate their actual use—or else to find work elsewhere.