COVINGTON

COVINGTON & BURLING LLP

E-ALERT | Government Contracts

January 29, 2014

DOD AND GSA RELEASE JOINT REPORT ON INCORPORATING CYBERSECURITY STANDARDS INTO THE ACQUISITION PROCESS

On January 24, 2014, the Department of Defense ("DoD") and General Services Administration ("GSA") jointly released a final report titled "Improving Cybersecurity and Resilience through Acquisition." The report provides six recommendations focused on "strengthening the cyber resilience of the Federal government by improving management of the people, processes, and technology affected by the Federal Acquisition System." DoD and GSA issued this report in response to Executive Order ("EO") 13636, "Improving Critical Infrastructure Cybersecurity," which President Obama signed on February 12, 2013. Section 8(e) of EO 13636 directed the two agencies to prepare recommendations for the President on the "feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration" within 120 days of the issuance of the EO. The concepts in the final report are very similar to those found in the draft report DoD and GSA released in June 2013.

RECOMMENDATIONS

The report makes six recommendations, many of which incorporate recent cybersecurity-related rulemakings and legislation. The report characterizes the "ultimate goal" of the recommendations as strengthening the "cyber resilience" of the Government by "improving management of the people, processes, and technology." The report acknowledges that the recommendations are not intended to conflict with cybersecurity requirements relating to National Security Systems ("NSS"), as the Committee on NSS has already established acquisition practices for NSS.[1] Additionally, the report notes that the recommendations are intended as only a part of the Government's "comprehensive response to cyber risks." Moreover, the report cautions that a "selective approach" to imposing cybersecurity requirements is necessary because different acquisitions present different levels of risk. Imposing overly restrictive cybersecurity standards could both limit competition and lead to increased costs. Finally, although the report acknowledges that the implementation of the recommendations should align with recent and ongoing changes to the Federal Acquisition Regulation ("FAR") and the Defense Federal Acquisition Regulation Supplement ("DFARS"), the report does not provide detailed guidance as to how that will be accomplished.

Institute Baseline Security Requirements as a Condition of Contract Award for Appropriate Acquisitions

The report first recommends that the Government only do business with organizations that incorporate at least first level baseline cybersecurity measures to deter unauthorized disclosure, loss, or compromise of data in their information systems. The report lists as examples of such measures updated virus protection, access limitations, multiple-factor logical access, methods to ensure confidentiality of data, and current security software patches. The report suggests that the

[1] For example, a DFARS final rule issued in November 2013 regulates supply chain risk management for information technology contracts for NSS only.

requisite baseline measures should be expressed in each acquisition's technical requirements, and should include performance measures to maintain the baseline over the lifetime of the product or service procured. Baseline cybersecurity requirements are meant to apply to both contractor operations and any products or services delivered to the Government.

The report explains that this recommendation for baseline security requirements is intended to be harmonized with the recent DFARS final rule, "Safeguarding Unclassified Controlled Technical Information" and the ongoing FAR rulemaking, "Basic Safeguarding of Contractor Information Systems." As discussed in a prior Covington E-Alert, the recent DFARS final rule sets forth enhanced protections for safeguarding of DoD unclassified controlled technical information ("UCTI").[2] In contrast, the proposed FAR rule was designed to address the basic safeguarding of contractor information systems that contain a broader scope of Government data. As proposed, the FAR rule deals more generally with basic cybersecurity hygiene rather than the enhanced protections referenced in the new DFARS rule. However, several of the standards in the FAR rule are ambiguous, instructing contractors to use "technology and processes that provide the best level of security and privacy available, given facilities, conditions, and environment," without defining what constitutes "best level of security." The final FAR rule is expected in February 2014. Until that final rule is promulgated, it is difficult to evaluate whether these rules will be sufficient to establish the baseline envisioned by this recommendation.

Address Cybersecurity in Relevant Training

Second, the report recommends training for the relevant Government workforce to adapt to new cybersecurity practices and Government outreach to industry stakeholders to make clear that the Government is adopting risk-based cybersecurity acquisition practices and will "require more from industry relative to cybersecurity in certain types of acquisitions." The report does not elaborate on the specifics of what more will be expected from contractors.

Develop Common Cybersecurity Definitions for Federal Acquisitions

Third, the report recognizes that a common set of definitions is needed to successfully implement cybersecurity acquisition standards. The report recommends harmonizing key cybersecurity terms in federal acquisitions to increase the effectiveness of cybersecurity reforms in both the Government and private sectors. According to the report, this recommendation is meant to be harmonized with the DFARS rulemaking, "Detection and Avoidance of Counterfeit Electronic Parts."

Contractors are already subject to a range of cybersecurity standards including those imposed in the international, federal, state, and commercial sectors. Cybersecurity and supply chain risks in the federal market are further segmented into agency-specific standards. These different regulatory regimes often rely on unique terms that are crucial to the applicability of security standards. Often, however, these definitions are not consistent across the regimes. Thus, the report's recommendation for harmonizing terminology is encouraging. However, it is unclear why the report makes specific mention of only the ongoing DFARS rulemaking regarding counterfeit parts. That DFARS proposed rule defines only a few terms, and those terms are applicable only to that rule and its accompanying clause. This recommendation would be improved by including key cybersecurity definitions more broadly in FAR Part 2, so that a common language can be developed in this area.

---

[2] The DFARS rule obligates contractors to comply with 51 specified security controls from the National Institute of Standards and Technology ("NIST") Special Publication 800-53, as well as any other security measures the contractor reasonably determines are necessary to provide adequate security. The DFARS rule, however, provides no guidance as to the standard the contractor should use for determining whether additional security beyond the specified NIST controls are necessary.

Institute a Federal Acquisition Cyber Risk Management Strategy

Fourth, the report recommends the development of a government-wide cybersecurity risk management strategy. The report specifies that the strategy should include a "hierarchy of cyber risk criticality for acquisitions," which would permit the Government to identify those acquisitions presenting the highest cyber risk. The report recommends that this strategy include the creation of "overlays," which are defined as "risk based controls" that "provide the ability to appropriately tailor security requirements for specific technologies or product groups, circumstances and conditions, and/or operational environments." The report suggests that the overlays should be expressed as technical requirements of the procurement and should identify the minimum acceptable security controls that an agency should apply to the acquisition in question. However, the report also warns against directly incorporating standards into contracts, as doing so may "hamper or prevent the evolution of counter measures to address the dynamic threat and technology landscapes."

This report recognizes that not all assets procured by the Government present the same level of cyber risks. Consequently, there is a need for the Government to balance protection from significant threats against the increased costs and reduced competition that will result from more restrictive cybersecurity requirements. Implementation of this recommendation will require the Government to develop guidelines for the development and use of overlays. Overly restrictive solicitations could lead to an increase in pre-award bid protests and/or increased costs to the Government.[3]

Include a Requirement to Purchase from Original Equipment Manufacturers, Authorized Resellers, or Other "Trusted" Sources, Whenever Available, in Appropriate Acquisitions

The fifth recommendation is intended to protect against inauthentic, counterfeit, or non-conforming items by requiring the Government to procure certain items only from original equipment manufacturers ("OEMs"), authorized resellers, or other trusted sources. The report suggests using qualified products, bidders, or manufacturers lists ("QBL") to identify trusted sources. Additionally, the recommendation notes that the criteria for determining which suppliers will qualify as "trusted" sources should include: long term business viability, quality control systems, order placement and fulfillment processes, customer support, customer return policies, and past record, such as by a search in the Government-Industry Data Exchange Program. The report notes that these criteria should be evaluated on a regular basis to ensure that QBL designation is providing continued value for mitigating risk.

One issue raised by this recommendation is what effect its implementation will have on rules requiring full and open competition. Limiting the procurement of certain items to a select number of OEMs and their chosen authorized resellers, restricts competition and will likely result in higher pricing. Small businesses, in particular, may find themselves excluded from competitions. The recommendation recognizes the potentially adverse effects on competition, and suggests limiting this requirement to "types of acquisition that present risks great enough to justify the negative impact on competition or price differences between trusted and un-trusted sources." Further clarifications of when competition may be properly restricted, what constitutes a "trusted" source, and when other than "trusted" sources are permissible are necessary to fully understand the impact this recommendation would have on competition.

---

[3] Some of this strategy may be reflected in a new interim instruction issued by DoD on November 26, 2013. Interim DoD Instruction 5000.02, "Operation of the Defense Acquisition System," integrates aspects of DOD's "Better Buying Power" initiative and, among other things, establishes new cybersecurity requirements spread throughout the acquisition cycle. For example, the instruction also requires DOD to initiate a "cybersecurity risk management framework" pursuant to the DOD Information Assurance Certification and Accreditation Process ("DIACAP") as early as possible in the acquisition process. Similarly, the new instruction requires DOD to institute a cybersecurity strategy for all acquisitions of systems containing information technology.

It remains to be seen how this recommendation will harmonize with recent and ongoing rulemakings regarding supply chain risk management and the detection of counterfeit parts. For example, the report does not discuss the enhanced authority of DoD and the Intelligence Community to exclude suppliers that present unreasonable supply chain risks[4] or the proposed rule DFARS rule on the "Detection and Avoidance of Counterfeit Electronic Parts."

Increase Government Accountability for Cyber Risk Management

In its sixth and final recommendation, the report calls for the integration of security standards into acquisition planning and contract administration to "ensure key decision makers are accountable for decisions regarding threats, vulnerabilities, likelihood, and consequences of cybersecurity risks." The report suggests four steps for acquisition personnel:

1. conduct a cyber risk assessment while defining the requirement and drafting the solicitation;
2. certify that the appropriate cybersecurity requirements are adequately reflected in the solicitation;
3. participate in proposal evaluation to ensure the best value proposal meets the cybersecurity requirements; and
4. certify that any conformance testing, reviews, supply chain risk management measures, or other post-award contract matters were conducted in accordance with prescribed standards.

This recommendation places a significant burden on Government acquisition officials. As a result, much like the controversial Section 515 in the Consolidated Appropriations Act of 2014, a requirement for acquisition officials to personally certify certain actions may make it more likely that those personnel will include more restrictive standards than necessary in solicitations to ensure that they have met that certification requirement. Again, any actions that result in more limited competition and more restrictive standards are vulnerable to increased pre-award bid protests and higher costs to the Government.

IMPACT ON CONTRACTORS

Overall, the report mimics much of the recent regulatory activities in the cybersecurity area. Although the report provides no detailed implementation guidelines, it provides insight into the Government's increasing concerns about cybersecurity and the risks presented by a global supply chain. Contractors will need to keep abreast of proposed cybersecurity initiatives, participate in the public dialogue where possible, and consult legal and technical experts when evaluating implementing new cybersecurity requirements.

---

[4] *See* "New Intelligence Community Directive Addresses Supply Chain Risk Management," *Covington E-Alert* (Jan. 9, 2014); "New DFARS Rules Address Supply Chain Risks and Unclassified Information," *Covington E-Alert* (Nov. 21, 2013).

If you have any questions concerning the material discussed in this client alert, please contact the following members of our government contracts practice group:

Alan Pemberton	+1.202.662.5642	apemberton@cov.com
Susan Cassidy	+1.202.662.5348	scassidy@cov.com
Jennifer Plitsch	+1.202.662.5611	jplitsch@cov.com
Catlin Meade	+1.202.662.5889	cmeade@cov.com