DEPARTMENT OF DEFENSE AND GENERAL SERVICES ADMINISTRATION RECOMMEND NEW CYBERSECURITY REQUIREMENTS IN FEDERAL PROCUREMENTS

Action Follows Recent Adoption of New Requirements for Safeguarding Technical Information Held by Defense Contractors

Kent Bressie & Danielle Piñeres

On January 23, 2014, the U.S. Department of Defense ("DoD") and the U.S. General Services Administration ("GSA") made public their report and recommendations to the President for improving cybersecurity practices in the federal acquisition process. While directed toward changing the behavior of U.S. Government program managers and acquisition decision makers, the report will likely result in further regulatory requirements for U.S. Government contractors, including cybersecurity requirements for contract awards and restrictions on sourcing of components. This report follows DoD's earlier amendments of the Defense Federal Acquisition Regulation Supplement ("DFARS") to impose new requirements on defense contractors for safeguarding unclassified controlled technical information residing on their information technology systems and databases.

The DoD-GSA recommendations and new DoD requirements will likely, or already do, affect compliance with existing government contracts and should be factored into procurement solicitations and diligence conducted on acquisition targets. For acquisitions by foreign persons, these actions will likely heighten scrutiny by the Committee on Foreign Investment in the United States ("CFIUS").

1. DoD-GSA Recommendations

Last year, President Obama issued Executive Order 13636, directing DoD and GSA to address the feasibility and merits of incorporating cybersecurity standards into federal acquisition planning and contract administration. The agencies' resulting report makes six key recommendations:

- *Institute baseline cybersecurity requirements as a condition of contract award for appropriate acquisitions.* DoD and GSA recommend that U.S. Government contractors be required to implement baseline cybersecurity protections like anti-virus protection, multi-factor logical access, methods to ensure the confidentiality of data, and current security software patches, both in their own policies and in products delivered to the U.S. Government. The agencies also recommend that cybersecurity requirements be included in government contracts as part of the technical description of the product or service being acquired, rather than stated in a separate contract section and described only with reference to broadly stated standards.

- *Train U.S. Government and contractor workforces on acquisition cybersecurity requirements.* DoD and GSA recognize that new policies on cybersecurity in acquisition will require training for the federal acquisition work force. The report also recommends that the government reach out to industry stakeholders to provide information about new cybersecurity requirements.
- *Develop common cybersecurity definitions for federal acquisitions and incorporate them into the Federal Acquisition Regulation ("FAR").* The report notes that U.S. Government contracts often include key terms relating to cybersecurity, but that the terms are often ill-defined and that their meaning may vary from contract-to-contract. To encourage clarity and consistency, DoD and GSA recommend that the U.S. Government adopt common definitions for cybersecurity-related terms and amend the FAR to include those definitions.
- *Institute a federal acquisition cyber risk management strategy.* DoD and GSA recommend that the U.S. Government develop an interagency strategy for cyber risk management. Such an approach would include the development of "overlays," or specified sets of security requirements and supplemental guidance that can be adapted for particular types of procurements. A federal cyber risk strategy should leverage existing industry standards and best practices, the report notes, and should be developed in consultation with industry.
- *Require U.S. Government contractors to purchase components from Original Equipment Manufacturers ("OEM"), their authorized resellers, or other "trusted" sources.* The report expresses concern about cyber risk stemming from the acquisition of counterfeit parts and components that may have been tampered with prior to acquisition. To mitigate this risk, DoD and GSA recommend that the U.S. Government and its contractors purchase goods only from OEMs, authorized retailers, and other trusted sources.
- *Increase Government accountability for cyber risk management.* According to DoD and GSA, the federal government must do more to ensure accountability for cyber risk management on the part of those individuals responsible for federal acquisition. This would involve integrating cybersecurity metrics into both acquisition planning and contract administration.

Many federal agencies already require their contractors to comply with the Federal Information Security Management Act ("FISMA") controls recommended in NIST Special Publication 800-53: Recommended Security Controls for Federal Information System and Organizations.

2. New DoD Cyber Safeguards for Unclassified Controlled Technical Information

The DoD-GSA report follows DoD's earlier amendments of DFARS to safeguard unclassified controlled technical information residing on contractor information technology systems and databases. With those amendments, published at 78 Fed. Reg. 69,273 (Nov. 18, 2013), DoD now requires that covered DoD contractors and subcontractors to:

- adopt and implement—regardless of the existence or absence of existing contracting clauses—security standards to protect their information technology systems and databases and technical information residing therein, "includ[ing] research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code";
- self-report to DoD on 13 specific criteria within 72 hours of a "cyber incident," defined as an action "taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein"; and
- maintain certain evidence pertaining to such an incident for a period of 90 days after its occurrence.

DoD requires that contractors flow down these requirements through their supply chains to all subcontractors. DoD also adopted new solicitation provisions and contract clauses to enforce these requirements in its procurement processes.

* * *

For more information about cybersecurity requirements for federal contractors or about Wiltshire & Grannis's cyber- and national security practices, please contact Kent Bressie at +1 202 730 1337 or kbressie@wiltshiregrannis.com or the W&G lawyer with whom you regularly work.

This advisory is not intended to convey legal advice. It is circulated to W&G clients and friends as a convenience and is not intended to reflect or create an attorney-client relationship as to its subject matter.