Smith • Pachter • McWhorter PLC
Attorneys At Law

LEGAL DEVELOPMENTS ALERT

DOD Issues Several Memos on Cybersecurity Compliance

The Department of Defense (DOD) issued four Defense Procurement and Acquisition Policy (DPAP) memoranda on cybersecurity compliance in less than three months, signaling DOD's increased interest in validating contractor compliance with the Defense Federal Acquisition Regulation Supplement (DFARS) cybersecurity rules. Many DOD contractors are subject to the cybersecurity requirements pursuant to the contract clause at DFARS 252.204-7012, *Safeguarding Covered Defense Information & Cyber Incident Reporting*.

DFARS 252.204-7012 imposes security and cyber incident reporting requirements on DOD contractors who have access to covered defense information (CDI). CDI is defined as "unclassified controlled technical information or other information" that requires safeguarding or dissemination controls as described in the National Archives and Records Administration's Controlled Unclassified Information (CUI) Registry. DFARS 252.204-7012(a). Categories of CUI data include: critical infrastructure, defense, financial, procurement and acquisition, proprietary business information, and intelligence. The DFARS clause further requires DOD contractors to implement National Institute of Standards and Technology Special Publication (NIST SP) 800-171 by December 31, 2017.

The recent DPAP memoranda are:

- DPAP Memorandum, *Guidance for Assessing Compliance and Enhancing Protections Required by DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting* (Nov. 6, 2018): Incorporates two "Guidance" documents to assist DOD acquisition personnel in the development of effective cybersecurity evaluation techniques. The Guidance provide clarification on implementing NIST SP 800-171 security requirements and address the impact of "not yet implemented" security requirements on a contractor's unclassified internal information system. The Guidance also require contractors to deliver a system security plan and to track the flow down of cybersecurity requirements to lower-tier subcontractors and/or suppliers. One of the documents includes evaluation criteria *and* encourages DOD officials to "conduct on-site Government assessment of contractor's internal unclassified information system in accordance with NIST SP 800-171A" pre- and post-award.

- DPAP Memorandum, *Strengthening Contract Requirements Language for Cybersecurity in the Defense Industrial Base* (Dec. 17, 2018): Provides DOD program offices with a sample Statement of Work (SOW) to include in solicitations. The SOW requires contractors to deliver a system security plan (or extracts) demonstrating the contractor's compliance with DFARS 252.204-7012. The security plan "must be in effect at the time the solicitation is issued or as authorized by the contracting officer" and "describe the contractor's unclassified information system(s)/network(s) where covered defense information associated with the execution and

performance of this contract is processed, is stored, or transmits."

- DPAP Memorandum, *Addressing Cybersecurity Oversight as Part of a Contractor's Purchasing System* (Jan. 21, 2019): Directs the Defense Contract Management Agency (DCMA) to validate a contractor's compliance with the cybersecurity requirements in DFARS 252.204-7012 and NIST SP800-171. DCMA "will leverage its review of a contractor's purchasing system in accordance with DFARS Clause 252.244-7001, Contractor Purchasing System Administration," to:

    - Review contractor procedures to ensure contractual DOD requirements for marking and distribution statements on DOD CUI flow down appropriately to their Tier 1 Level Suppliers; and
    - Review contractor procedures to assess compliance of their Tier 1 Level Suppliers with DFARS 252.204-7012 and NIST SP 800-171.

- DPAP Memorandum, *Strategically Implementing Cybersecurity Contract Clauses* (Feb. 5, 2019): Notes that DFARS 252.204-7008 requires contractors to represent on a contract-by-contract basis that their implementation of NIST SP 800-171 is complete. This individual contract approach "is inefficient for both Industry and Government, and impedes the effective implementation of requirements to protect DoD's Controlled Unclassified Information for contracts containing DFARS clause 252.204-7012." The memorandum directs DCMA to develop a proposal for achieving the following objectives, among others, for DCMA-administered contracts:

    - Obtaining and assessing contractor system security plans strategically (not contract-by-contract);
    - Determining industry cybersecurity readiness; and
    - Engaging industry to discuss methods to oversee the implementation of DFARS 252.204-7012 and NIST SP 800-171.

    The memorandum also directs Defense Pricing and Contracting (DPC) to develop a similar plan for contracts not administered by DCMA. Any resulting contract modifications or changes to achieve these objectives "will be limited to bilateral modifications that do not result in a change to any contract price, obligated amount, or fee arrangement."

Contractors must be prepared for DOD's continuing emphasis on protecting DOD information and confirming compliance with the DFARS cybersecurity requirements. Contractors should expect DOD to include SOW language in solicitations requiring contractors to develop—and share with DOD—system security plans setting forth the contractor's compliance with DFARS 252.204-7012 and NIST SP 800-171. Cybersecurity compliance is thus a critical consideration in both proposal submission and contract performance.

Contractors should also be prepared for DCMA to include a cybersecurity evaluation as part of the contractor's Purchasing System Review (CPSR). Contractors should review the DPAP memoranda discussed above to ensure familiarity with the DOD standards for assessing and auditing a contractor's cybersecurity compliance. Prime contractors are also required to flow down the DFARS clause to subcontractors and should be prepared to demonstrate compliance in their supply

chain during the CPSR audit.

Our firm will continue to monitor the Government's review of cybersecurity compliance. If you have questions, please contact:

Stephen D. Knight Laura A. Semple

Smith Pachter McWhorter PLC

8000 Towers Crescent Drive, Suite 900 | Tysons Corner, VA 22182 | 703.847.6300 | www.smithpachter.com