CLIENT ALERT

Cybersecurity for Government Contractors: DoD Looking for More Practical Oversight

February 22, 2019

Contractors should note that earlier this month the Under Secretary of Defense for Acquisition and Sustainment (USDAS) directed the Defense Contract Management Agency (DCMA) to develop a way for more efficient implementation of government cybersecurity requirements under Defense Federal Acquisition Regulation Supplement (DFARS).

The directive, contained in a USDAS memorandum titled "Strategically Implementing Cybersecurity Contract Clauses," explained that DFARS clause 252.204-7012 (Safeguarding covered defense information and cyber incident reporting) "is vital to the future security of the United States." The USDAS also stated that DFARS 252.204-7008 (Compliance with safeguarding covered defense information controls) requires contractors to report — on a contract-by-contract basis — the status of their implementation of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171. The new USDAS directive declared that such a contract-by-contract approach is inefficient for both contractors and the Government, and actually impedes the Government's ability to review whether Controlled Unclassified Information is adequately protected as required under the -7012 clause.

Given these difficulties, USDAS instructed DCMA to use its authority under Federal Acquisition Regulation Part 42 and 43 and DFARS 242.302 to develop strategies for cybersecurity implementation. DCMA must take several actions, including recommending how (i) to assess contractor cybersecurity plans strategically and not contract-by-contract, (ii) to grade industry cybersecurity readiness, and (iii) to distribute readiness findings to Department of Defense components. DCMA must discuss with contractors methods to oversee implementation of SP 800-171 and -7012 clause requirements. DCMA also shall develop a way to make block changes to contracts so that the USDAS's policy of more efficient implementation can be achieved. Such block changes must be

bilateral modifications that do not impact contract price, obligated amount, or fee arrangement.

The DCMA's new mandate takes effect on March 1, 2019. Therefore, contractors should be ready to engage DCMA in the coming months. Nichols Liu regularly works with contractors in formulating feedback to the government on cybersecurity issues such as this. Please email us at rnichols@nicholsliu.com if we can assist in any way.

Contacts:

Robert Nichols
202.846.9801
rnichols@nicholsliu.com

Andrew Victor
202.846.9825
avictor@nicholsliu.com