wiley

ALERT

Show Me Your SSPs: DOD to Begin Requesting and Assessing Contractors' System Security Plans

April 8, 2022

WHAT: At a recent Town Hall Meeting hosted by the Cybersecurity Maturity Model Certification Accreditation Body (CMMC-AB), a Defense Contract Management Agency (DCMA) representative announced that DCMA will begin assessing contractors' compliance against the National Institute of Standards and Technology (NIST) 800-171 security controls through the "Medium Assessment" process that the U.S. Department of Defense (DOD) prescribed in the interim rule that created Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7020. The Medium Assessment process is the middle of three types of assessments described in the -7020 clause (Basic, Medium, High). In a Medium Assessment, the Government reviews the contractor's current documentation (primarily the System Security Plan) and the contractor's previous self-assessment, which contractors were required to complete by November 2020. The representative explained that he expects these assessments to begin in "a couple months."

WHAT DOES IT MEAN FOR INDUSTRY: While contractors await the future CMMC 2.0 program announced last year, DOD is taking every opportunity to remind contractors that existing DFARS clauses already require contractors to implement and attest to implementing the security controls prescribed in NIST 800-171. For several years, DFARS 252.204-7012 has required contractors to implement the security controls prescribed in NIST 800-171. In its September 2020 interim rule, DOD added DFARS 252.204-7019 & -7020, which required contractors to score their own compliance and submit that score to DOD. This new initiative is DOD's first large-scale effort to evaluate

Authors

Gary S. Ward
Partner
202.719.7571
gsward@wiley.law

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Teresita Regelbrugge
Associate
202.719.4375
rregelbrugge@wiley.law

Practice Areas

Cybersecurity
Government Contracts
National Security
Privacy, Cyber & Data Governance

whether contractors are complying with these requirements and reporting accurate scores. And although DCMA avoided drawing any connections, this program comes shortly after the U.S. Department of Justice (DOJ) announced plans to "use [its] civil enforcements tools to pursue companies . . . when they fail to follow required cybersecurity standards" under its Civil Cyber-Fraud Initiative.

KEY TAKEAWAYS: Contractors should be prepared for DCMA to request copies of their System Security Plans and any other documents that substantiate their compliance with the NIST 800-171 security controls. Contractors should also ensure that the right people within the organization are familiar with these documents and able to show any assessors how they substantiate the company's compliance with the NIST 800-171 requirements.

Wiley will continue to monitor these developments.