crowell moring

CLIENT ALERT

Navy Makes Waves By Increasing Cybersecurity Requirements for Select Defense Industrial Base Contractors

Nov.01.2018

The Navy has recently issued a policy memorandum calling for heightened cybersecurity requirements and oversight for "critical" defense contractors handling covered defense information (CDI). The memo reflects a continued focus within the DoD on evaluating contractors' compliance with the DFARS 252.204-7012 Clause, as well as a risk-based approach to going beyond it.

The memo expands the Clause requirements in several significant respects, including:

- Requiring *fully implemented* system security plans (SSPs) for government evaluation.
- Ensuring historically challenging cybersecurity requirements such as multifactor authentication are immediately met.
- Imposing new cybersecurity requirements such as encryption at rest.
- Requiring contractors to allow the Naval Criminal Investigative Services (NCIS) to install "network sensors" on contractors' information systems when NCIS intelligence detects a potential vulnerability.

Selected Navy contractors should receive notice of these new requirements before the end of the year and may begin considering potential cost recovery strategies, such as requests for equitable adjustments.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1 202.624.2615
Email: ewolff@crowell.com

Kate M. Growley, CIPP/G, CIPP/US
Counsel – Washington, D.C.
Phone: +1 202.624.2698
Email: kgrowley@crowell.com

Michael G. Gruden, CIPP/G
Associate – Washington, D.C.
Phone: +1 202.624.2545
Email: mgruden@crowell.com