Federal Cybersecurity Requirements – Are you in Compliance?

12.13.2021

As many of you know, all Department of Defense (DoD) contractors that store, process, or transmit *Covered Defense Information* (CDI) are subject to DFAR 252.204-7012. Effective January 1, 2018, the DFAR clause requires that contractors implement the NIST special publication 800-171 standards. Butzel highlighted the key requirements of the NIST standards in a 2017 session: *Supplier Cyber Regulatory Awareness.*

As part of the implementation, a contractor needs to assess its current security protocols versus the NIST 800-171 standards, document that analysis in a System Security Plan (SSP) and develop a Plan of Actions and Milestones (POAM) to address any gaps.

Prime contractors need to confirm that their subcontractors are also in compliance. Contractors and subcontractors that fail to comply face potentially serious consequences, both in terms of getting new awards and continuing performance of current contracts.

Companies have known about these requirements for some time now but struggle to comply. Help is on the way. The Michigan Defense Center (MDC), an operation of the Michigan Economic Development Corporation, is offering Michigan's small and medium sized defense contractors a comprehensive one-stop shop to federal cybersecurity compliance. For more information, please see Michigan Defense Resources.

As the MDC explains, "this program is one of the first in the nation to provide a business solution to this federal mandate and strives to drive standardization, accountability and cost-effectiveness to the process." MDC's Director, Vicki Selva, emphasizes, "this multi-phased approach will help you navigate proven resources to meet your needs no matter what phase you are in and provides guidance to assist you in protecting and growing your business."

Related Services

Aerospace & Defense Industry Team

Aerospace and Defense

Cybersecurity and Privacy Specialty Team

The program not only provides assistance, but small and medium-sized businesses can contract with the pre-approved vendor list to develop gap analysis report at a pre-negotiated discounted cost of $1,500 as the first step toward compliance and Cybersecurity Maturity Model Certification (CMMC). The gap analysis allows companies to submit to SPRS and other requirements. Once the gap analysis is completed with the pre-approved vendor, up to $15,000 in grant funding is available to address any deficiencies in your IT infrastructure and become fully compliant with DoD cybersecurity requirements for all contractors.

Butzel has the expertise to help your business navigate the various programs and resources. For assistance with these critical matters, please contact the author of this Alert, your regular Butzel attorney, or any member of Butzel's Aerospace and Defense Industry Group.

Beth Gotthelf
248.258.1303
gotthelf@butzel.com

Claudia Rast
734.213.3431
rast@butzel.com