FEBRUARY 14, 2018

Practical DFARS Cybersecurity Compliance Tips - 5 KEY TAKEAWAYS

Kilpatrick Townsend's Gunjan Talati, partner in the Government Contracts and Construction & Infrastructure Group, recently moderated a panel for the Association of Corporate Counsel National Capital Region chapter on Defense Federal Acquisition Regulation Supplement (DFARS) cybersecurity requirements. The panel, consisting of both in-house counsel and government officials, discussed the cybersecurity requirements at DFARS 252.204-7012 (the "DFARS Clause"). The panel covered what the DFARS Clause requirements for contractors are and best practices for compliance.
5 key takeaways from the presentation include:

1. The DFARS Clause requires contractors and subcontractors with certain defense contracts to provide "adequate security" for "all covered defense information" in accordance with NIST 800-171. Contractors and subcontractors must also rapidly report security incidents to agencies and perform specific actions in response to such incidents.
2. Contractors can demonstrate compliance with the DFARS Clause by developing a system security plan and plan of action to remedy any applicable deficiencies or vulnerabilities within their system.
3. Contractors should also ensure that any cyber incident response plan has provisions for handling required reporting under the DFARS Clause as well as other forensics requirements such as submitting malicious software in accordance with a contracting officer's direction and preserving and protecting images of impacted information systems.
4. The DFARS Clause also requires contractors to flowdown the requirements of the DFARS Clause to subcontractors when subcontractor performance will involve operationally critical support or covered defense information. Contractors should closely examine their relationship with any cloud service providers to determine whether they would be considered a "subcontractor" for purposes of the DFARS Clause.
5. Each organization's needs for DFARS Clause compliance will vary depending on the type of work they perform but all should consider having a formal compliance plan in place that is reduced to writing and incorporates all other plans, such as an incident response plan, as necessary.