wiley

Cybersecurity

Doing business with defense and intelligence community customers, not to mention several civilian agencies, brings a host of additional regulatory compliance challenges that Wiley's Government Contracts attorneys are uniquely positioned to help clients navigate. Leveraging our extensive Telecom, Media & Technology, National Security, and Privacy, Cyber & Data Governance experience, our attorneys advise our clients on compliance with the National Industrial Security Program Operating Manual (NISPOM); other U.S. Department of Defense (DOD) cybersecurity requirements relating to unclassified information, including Controlled Unclassified Information (CUI); NIST 800-171 DOD Assessments; the Cybersecurity Maturity Model Certification (CMMC) framework; and various supply chain risks, including compliance with Section 889 of the FY19 National Defense Authorization Act and implementing regulations.

Our representative experience includes:

- Advising clients on all aspects of successfully implementing cybersecurity requirements for federal contractors, including DFARS 252.204-7012, Safeguarding Covered Defense Information, NIST 800-171 DOD Assessments, and the CMMC framework.
- Drafting policies and procedures governing compliance with Section 889 restrictions, including communications with subcontractors; assisting with the conduct and documentation of contractors' "reasonable inquiry" into their use of covered equipment or services; and drafting comments on the interim FAR rule to address industry-specific concerns.
- Engaging with agency customers to coordinate FISMA audits of contractor information systems, including negotiating the scope of audits and any potentially malicious penetration testing.
- Assisting clients with incident response handling and management, including mandatory and voluntary disclosures of cyber incidents to federal agency customers, regulators, and affected individuals.
- Helping companies interact with the U.S. Department of Homeland Security (DHS) to share information and assess risks to business operations and critical infrastructure. This includes communications protected by the Cybersecurity Information Sharing Act of 2015 (CISA) and the Protected Critical Infrastructure Information (PCII) program.
- Litigating dozens of matters involving cybersecurity and computer forensic evidentiary issues, including False Claims Act and Computer Fraud and Abuse Act cases. This includes cybersquatting litigation to end domain-name hijacking and other exploitations.

- Defending and successfully resolving whistleblower allegations and a government investigation regarding cybersecurity obligations for sensitive compartmented information systems under ICD 500 and DCID 6/3.
- Investigating and responding to potential data spills involving classified information and classified information systems, including reporting to and coordinating with the Defense Counterintelligence and Security Agency (DCSA) and cognizant security agencies.
- Anticipating and shaping activity across the federal government (NTIA, NIST, FTC, DOJ, FCC, DHS, and the White House) involving cyber initiatives that directly and indirectly impact companies, including CISA, the NIST Framework for Improving Critical Infrastructure Cybersecurity, NIST publications, proceedings on botnets, market transparency, and the security of the communications and internet infrastructure.