SheppardMullin

Cybersecurity & Data Protection

Cybersecurity and data protection have never been more important for companies that interface with the government. Sheppard Mullin's Governmental Cybersecurity and Data Protection Team understands the government's approach to cybersecurity, for its own systems and those of its contractors and critical infrastructure providers.

Our team combines experts in cybersecurity, data protection, national security, data privacy, and government contracts law to provide unparalleled advice to companies that sell products and services to the government (whether directly or indirectly), as they face rapidly-changing cybersecurity standards and requirements from a variety of government agencies. With deep relationships to government officials, we are called on by some of the largest and most prominent companies to guide them through the maze of laws, standards, and agency regulations regarding cybersecurity, cloud computing, and incident response.

We understand that cybersecurity for companies that interface with the government is about protecting sensitive information – whether it's classified data, Covered Defense Information (CDI), or controlled unclassified information (CUI) – as well as securing critical infrastructure and the supply chain, and preparing for and executing comprehensive and effective incident response. Our team closely monitors updates and provides counseling, practical guidance, and training to clients in a number of areas including:

- Federal regulation compliance and best practices (to include FAR 52.204-21, DFARS 252.204-7012, and other agency-specific regulations)
- The Department of Defense (DOD) Cybersecurity Maturity Model Certification (CMMC) Program
- Executive Order No. 14028, Improving the Nation's Cybersecurity
- NIST publications, including NIST SP 800-171 and NIST SP 800-53
- Controlled Unclassified Information (CUI) and Covered Defense Information (CDI)
- Cloud computing, FedRAMP, and the DoD Cloud Authorization Process (SRG)
- Software supply chain and secure software development issues (including attestation and artifact requirements, e.g., SBOMs)
- Critical infrastructure security and resilience (including cyber incident reporting under CIRCIA and CISA regulations)
- Cybersecurity Supply Chain Risk Management (SCRM)
- Voluntary and mandatory information sharing with federal agencies (e.g., the FBI, DoD, and DHS/CISA)
- Contract flow-down requirements to subcontractors and vendors
- Incident response
- DOJ's Civil Cyber Fraud Initiative and regulatory enforcement
- DoD's Joint Certification Program
- Security clearances and the National Industrial Security Program Operating Manual (NISPOM)

- Policies, plans, and procedures to include Data Retention, Data Classification, Incident Response, Information Security, System Security Plans (SSPs), and Plans of Action and Milestones (POA&Ms)