

Cybersecurity for A&D Companies

Cybersecurity touches almost every aspect of a company's operations. Companies in the aerospace and defense (A&D) sector can be subject to greater risks due to the industry's highly technical and sensitive nature – particularly when contractors act as repositories for government data – and face increased pressure to develop and implement robust cybersecurity practices. Safeguarding measures that were reasonable in the recent past are unlikely to meet regulators' future expectations.

Our top-tier cybersecurity team of experienced lawyers and technical professionals provides comprehensive legal, operational, and reputation risk management services to the A&D industry. We understand the legislative and regulatory landscape, and counsel numerous A&D companies on proactive measures they can take to manage legal and regulatory risks in this area.

Representative experience

Advised defense contractors and critical infrastructure owners on utilizing cyber threat information sharing programs.

Advised multiple defense companies on U.S. government safeguarding and incident reporting requirements, including information system

Contacts

Michael F. Mason,
Washington, D.C.

Harriet Pearson,
Washington, D.C.

Michael J. Scheimer,
Washington, D.C.

Stacy Hadeka,
Washington, D.C.

assessments against the NIST 800-171 standards for CUI.

Advised cloud service providers on complying with the FedRAMP program and agency specific cloud security requirements.

Advised on complying with FISMA information security contract requirements including preparing security authorization packages and undergoing numerous agency ATO processes.

Advised an advanced technology company with significant government contracts on the handling of a cybersecurity breach involving ITAR and EAR data.

Assisted multiple government contractors and critical infrastructure entities with comprehensive responses to significant cybersecurity incidents, including incident reporting to US-CERT and DoD.

Advised a major technology company on the handling of an "insider" attack potentially affecting the company's HR databases.

Performed an intensive review of domestic data security safeguards and prepared a strategic plan for a data protection program for a leading global defense contractor.

Conducted a board-level investigation for a publicly held industrial company affected by a nation-state cyberattack on the sufficiency of management's incident response and disclosure.

Conducted data protection compliance assessments and gap analyses for major international corporations and national nonprofit organizations.

Advised clients on federal information security requirements in GSA Schedule offerings and GSA Cloud BPAs.

Latest thinking and events

News

Hogan Lovells partners discuss China's new privacy and security rules with FPF

Hogan Lovells Events

A perfect storm? Handling ransomware and other cybersecurity incidents as a U.S. public company

Hogan Lovells Publications

ADG Insights: Top 5 areas of False Claims Act risk for Aerospace, Defense, and Government Services companies

ADG Insights

Hogan Lovells Publications

ADG Insights | NIST set to enhance contractor cybersecurity duties

ADG Insights

Sponsorships and Speaking Engagements

DOD Cybersecurity Maturity Model Certification (CMMC) Briefing

Awards and Rankings

Hogan Lovells senior associate Stacy Hadeka named among American Bar Association's "On the Rise" honorees