Cybersecurity has become a key focus of both the executive and legislative branches, resulting in significant implications for government contractors. Regulatory agencies are advancing rulemaking for various economic sectors, while the federal government is including cybersecurity requirements in federal acquisition contracts via the Federal Acquisition Regulation (FAR). The U.S. Department of Justice's (DOJ) Civil Cyber-Fraud Initiative highlights the risks of False Claims Act (FCA) cybersecurity noncompliance liability for contractors.

Alexander Canizares, partner in Perkins Coie's Government Contracts practice, and Alex Trafton, managing director of Ankura Consulting Group's National Security practice, discussed emerging regulatory changes for government contractors and key considerations for companies related to cybersecurity. The presentation addressed the following:

- Review of the Biden-Harris National Cybersecurity Strategy.

- Executive Order 14028 and its implementation.
- Status of agency rulemaking across the federal government.
- FCA enforcement risks and compliance challenges for federal acquisition contracts.
- U.S. Department of Defense (DOD) cybersecurity requirements and Cybersecurity Maturity Model Certification (CMMC).

Hosted By:
Perkins Coie LLP and Ankura Consulting Group

Speakers

Alexander Canizares
Partner
Perkins Coie LLP

Alex Trafton
Managing Director
Ankura Consulting Group

Speakers

Alexander O. Canizares

Partner
ACanizares@perkinscoie.com 202.654.1769

Explore more in

Government Contracts