Cyber Incident Response Liabilities and Strategies

written by Lauri Moon | October 11, 2018

The DFARS 252.204-7012 clause “Safeguarding Covered Defense Information and Cyber Incident Reporting” has caused many defense contractors to focus on compliance with the 110 security requirements defined in NIST SP 800-171. However, NIST compliance is only one aspect of the DFARS clause. The regulations also require contractors to handle and report cyber incidents correctly – and there can be significant impacts when breaches occur, including forensic investigations.

DFARS 7012 includes specific requirements for:

- how to handle and report cyber incidents
- how soon a report should be filed after an incident is discovered
- how to register with the government to be able to file reports
- and much more

This webinar will explore the liabilities companies face relating to incident response, as well as recommend strategies to minimize the risk and complexity associated with incident reporting.

Presenters for this webinar include defense contract law specialists Alexander Major and Franklin Turner, McCarter & English LLP; Chief Security Architect Tim Williams, Technical Director, and Larry Lieberman, Cyber Evangelist, eResilience.

Register