Crowell

CLIENT ALERT

New DFARS Safeguards and Reporting Requirements

December 9, 2013

A DFARS final rule (Nov. 18, 2013) on the safeguarding of unclassified, controlled technical information requires contractors, among other things, to report within 72 hours of discovery any "cyber incident" (an action that results in an actual or potentially adverse affect on an information system and/or the information residing therein), preserve relevant data for at least 90 days, conduct an internal review of its network for evidence and extent of any compromise of data, cooperate with DoD "damage assessments," and flow the clause down to subcontractors (even for commercial items) -- all at the contractor's own cost (but included and potentially recoverable as a normal business expense under indirect rates). Given the rampant intellectual property and technology losses due to cyber espionage and other thefts documented in Congressional hearings, intelligence assessments, and industry reports this year, these DFARS requirements will apply additional pressure upon contractors to amend their existing compliance policies and procedures to address how to respond to a cyber incident and comply with these regulations.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

David C. Hammond
Partner – Washington, D.C.
Phone: +1.202.624.2510
Email: dhammond@crowell.com

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1.202.624.2615
Email: ewolff@crowell.com