WILMERHALE

Department of Defense Revises Landmark Cybersecurity Rule, Extends Deadline for Some Compliance Requirements

APRIL 14, 2016

An article by Benjamin A. Powell, Barry J. Hurewitz, Jonathan G. Cedarbaum, Jason C. Chipman and Leah Schloss, published in the May 2016 issue of *Privacy & Cybersecurity Law Report*, explores the new, amended Department of Defense interim cybersecurity rule that prescribes cybersecurity requirements, including mandatory cybersecurity-related contract clauses in all DoD contracts subject to the Defense Federal Acquisition Regulations Supplement. The authors of this article discuss the amended interim rule, which will affect both Defense Industrial Base and other cases, indicating that even as the DOJ has renewed its focus on individuals, it continues to pursue large cases with corporations—and that the SEC continues to broadly define a "thing of value" under the FCPA.

In December 2015, the Department of Defense ("DoD") issued a second interim rule on Network Penetration Reporting and Contracting for Cloud Services, amending an earlier version issued on August 26, 2015. The new, amended DoD interim rule prescribes cybersecurity requirements, including mandatory cybersecurity-related contract clauses in all DoD contracts subject to the Defense Federal Acquisition Regulations Supplement ("DFARS"). Despite its narrow title, the rule remains expansive in scope and prescriptive in application, mandating specific data security controls for sensitive unclassified information throughout the DoD supply chain. As such, the rule, even as revised, will affect both Defense Industrial Base ("DIB") and other companies. Read the full article

Authors

Benjamin A. Powell

PARTNER

Co-Chair, Cybersecurity and Privacy Practice

benjamin.powell@wilmerhale.com

+1 202 663 6770

Barry J. Hurewitz

PARTNER

barry.hurewitz@wilmerhale.com

+1 202 663 6089

Jason C. Chipman

PARTNER

jason.chipman@wilmerhale.com

+1 202 663 6195