Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

What You Should Know About DOD's Cybersecurity Rule

Law360, New York (November 25, 2013, 4:16 PM ET) -- On Nov. 18, the U.S. Department of Defense issued the long-awaited final rule addressing how DOD contractors and subcontractors must safeguard unclassified technical information on their corporate information systems.[1] Although the final rule narrows a proposed rule that the DOD had published in June 2011, the rule still has wide applicability to private sector information systems where DOD technical information is stored or transmitted. The DOD notes in the preamble that the rule "is deemed necessary for the protection of unclassified controlled technical information and it is understood that implementing these controls may increase costs to DoD."

The rule sets forth two main requirements. First, contractors must satisfy security standards established by the National Institute of Standards and Technology to protect "unclassified controlled technical information" (UCTI). The requirements established by the rule are to be incorporated into "all solicitations and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial items."

Second, contractors must report to the DOD cyber incidents that "affect" UCTI "resident on or transiting through the contractor's unclassified information systems." Contractors are responsible for ensuring that subcontractors comply with the rule's requirements, and the new requirements must be incorporated into subcontracts at all tiers. For these purposes, IT vendors, including Internet service providers and cloud service providers, are considered subcontractors.

Cybersecurity Controls

Although the security standards apply only to UCTI, UCTI is a broad enough category that many contractors may possess substantial amounts of UCTI on their corporate networks. The rule defines UCTI as computer software or technical data with military or space application that is subject to controls on access, use, reproduction, modification, performance, display, release, disclosure, or dissemination, and that is marked as controlled information pursuant to DOD rules.

Examples of technical information that could be specially marked as UCTI include "research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code."

The cybersecurity protocols required for UCTI include standards on authentication, training, incident response, contingency planning, and access controls, among others, defined in NIST Special Publication 800-53, ''Security and Privacy Controls for Federal Information Systems and Organizations."[2] If a

required control is not implemented, the contractor must explain in writing to the relevant government contracting officer why either the control is not applicable or an alternative measure is being used to achieve "equivalent protection."

It is unclear how much data may ultimately be covered as UCTI. DOD policies allow for data to be marked as controlled information if it is export controlled, critical technology, operations security data, software documentation, vulnerability information, test and evaluation data, or foreign government information, among other grounds.[3] Most contractors are unlikely to have separately configured networks for housing and transmitting UCTI information. The rule requires that contractors "[i]mplement information systems security in its project, enterprise, or company-wide unclassified information technology system(s) that may have unclassified controlled technical information resident on or transiting through them."

Thus, as a practical matter, the requirements of the new rule may well reach entire corporate networks even when such networks do not contain significant amounts of UCTI (or a contractor does not have a means of tracking and separating UCTI from other information on its corporate networks). The DOD states that audits will be conducted at the discretion of the contracting officer in accordance with the terms of a contract.

Cyber Incident Reporting

Cyber incident reporting obligations turn on, among other criteria, whether a cyber incident could "allow unauthorized access to the Contractor's unclassified information system on which unclassified controlled technical information is resident on or transiting" or "possible" compromise of UCTI. Reports must be sent to the DOD viahttp://dibnet.dod.mil/ within 72 hours of discovery of any cyber incident and must include specific, detailed data about the nature of the intrusion and any government projects possibly implicated.

Contractors are required to preserve data about the cyber incident for 90 days, including "protect[ing] images of known affected information systems and all relevant monitoring/packet capture data for at least 90 days from the cyber incident"; the DOD may elect to conduct a "damage assessment" and may demand access to all of the data collected by the contractor about the incident. The rule requires contractors to share with the DOD all information requested about an incident unless "there are legal restrictions that limit a company's ability to share digital media," in which case the contractor must explain to the contracting officer why information is being withheld.

According to the DOD, data from its current voluntary cyber reporting programs suggest there may be five reports per company per year. The DOD also estimates a 3.5-hour burden per response. Based on our experience, we believe the DOD estimate of the time to prepare a single report across the 13 data points required by the rule may significantly understate the time required to prepare accurate cyber incident reports.

Compliance with the cyber incident reporting requirements will necessarily involve costs, both to preserve data in a forensically sound manner and to assemble information about any intrusion. Responding to damage assessment requests may increase costs for some contractors and will likely increase the need for corporate counsel to assess contractual or other legal restrictions on sharing data about an incident.

Some contractors, especially large companies and institutions with complex computer networks, may be

required to make frequent decisions about whether a particular incident triggers a reporting requirement. The requirement to notify the DOD does not turn on the severity of an incident but instead turns on whether a particular incident may "affect" UCTI either stored on a compromised network or transiting that network. We anticipate that contractors will need to develop protocols for identifying which incidents must be reported to the DOD pursuant to the new rule.

—By Benjamin A. Powell, Jonathan G. Cedarbaum, Barry J. Hurewitz, Randolph D. Moss and Jason C. Chipman, WilmerHale

Benjamin Powell, Jonathan Cedarbaum, Barry Hurewitz and Randolph Moss are partners and Jason Chipman is counsel in WilmerHale's Washington, D.C., office.

[1] 78 Fed. Reg. 69273 (Nov. 18, 2013), accessed at http://www.gpo.gov/fdsys/pkg/FR-2013-11-18/pdf/2013-27313.pdf.

[2] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[3] Department of Defense Inst. 5230.24 (available at http://www.dtic.mil/whs/directives/corres/pdf/523024p.pdf).
