Time to Tighten Up: Pentagon Imposes New Unclassified Technical Data Security Controls and Cyber Incident Reporting Requirements

Legal Alert
November 20, 2013

Related Services

Government Contracts

Garvey Schubert Barer Legal Update, November 20, 2013.

If you are a DoD contractor or subcontractor, now is the time to make sure your cyber security protections and reporting procedures are up to snuff. For contracts awarded after November 18, 2013, you must comply with new DFARS rules on protecting unclassified technical data and reporting certain cyber incidents.

On November 18, 2013, DoD adopted a new final DFARS rule regarding Safekeeping of Unclassified Controlled Technical Information, and a new standard DFARS contract clause (252.204-7012). The action reflects DoD's intensifying concern over cyber intrusions targeting private defense and aerospace industries. The Federal Register Notice of Final Rule may be found here.

"Controlled technical information" ("CTI") means unclassified technical data, computer software, and other technical information subject to control by DoD Distribution Statements under DoD Directive 5230.24. It can include any unclassified technical information marked in a manner which restricts release to the public, including, for example, limited/restricted rights or government purpose rights data or software, export controlled information, or FOUO information. The rule applies to CTI resident on, or transiting through, contractor and subcontractor unclassified IT systems.

The Rule and clause requires contractors and subcontractors to provide "adequate security" to safeguard unclassified CTI kept on or transiting through their IT systems. To be considered "adequate," the IT systems' security controls must, at a minimum,

have the capabilities described in certain specified provisions of National Institute of Standards and Technology Special Publication 800-53. (NIST SP 800-53). NIST SP 800-53 controls are the minimum required; the rule permits the contractor to comply by demonstrating that it has more robust controls in all the required areas.

In addition to implementing security controls, contractors must report to DoD certain cyber incidents, including possible exfiltration, manipulation, loss or compromise of, or unauthorized access to, CTI kept on or transiting through the contractor's, or its subcontractors', IT systems. Contractors must also take certain actions, including further reviews, preservation and protection of images and monitoring/packet data for at least 90 days after the incident to allow DoD to request such tracking information, and cooperation with DoD damage assessments.

The new rule and contract clause has far-reaching and important implications for all DoD contractors and subcontractors. The clause and rule applies specifically to commercial item procurements, and must be flowed down to all subcontractors. While there is no evidence that DoD plans to amend existing contracts, ALL contractors and subcontractors whose IT systems will store or handle any CTI under contracts awarded after the November 18, 2013, effective date must comply with the security control and reporting requirements.

Compliance with the new rule will require assessment of IT security controls at all tiers, starting with the contractor's own, and extending down the chain to all subcontractors and suppliers who will receive or generate CTI. DoD recognized that implementation of the rule would likely involve compliance costs, especially on the part of small business contractors and subcontractors. Nevertheless, DoD expressed the view that such costs must be allocated to indirect cost pools, and that the Government would not directly bear such costs.

DoD specifically noted that ISPs and "cloud" service providers are considered subcontractors under the rule. Contractors are responsible for assuring that ISPs and cloud providers have in place security controls and reporting obligations meeting the requirements of the regulation. Typically, "cloud" service providers are reluctant to obligate themselves in Service Level Agreements in this manner. Any DoD contractor or subcontractor using "cloud" vendors to store or move CTI should review carefully the service level commitments of the providers, to assure compliance.

Please contact Ben Lambiotte or Scott Warner if you need any assistance in complying with the rule, or reviewing the agreements that may be affected by it.

Ben Lambiotte : blambiotte@gsblaw.com 202.298.2525
Scott Warner : sgwarner@gsblaw.com 206.816.1319