December 16, 2013

The Department of Defense ("DOD") has issued a final rule on contractor responsibility for safeguarding unclassified controlled technical information. The final rule, issued on November 18, 2013, requires contractors to take adequate security measures to protect unclassified controlled technical information that resides on or passes through a contractor's information systems. The final rule also requires the contractor to notify DOD of cyber intrusion events that affect the unclassified controlled technical information.

In issuing the final rule, DOD has narrowed the scope of a proposed rule that covered all unclassified DOD information within a contractor's information systems. The final rule limits coverage to "unclassified controlled technical information," which is defined as technical data or computer software with military or space application that is subject to controls on the use, access, reproduction, modification, performance, display, release, disclosure or dissemination.[1] This includes technical information covered by DOD Directive 5230.24 (Distribution Statements on Technical Documents) and DOD Directive 5230.25 (Withholding of Unclassified Technical Data from Public Disclosures), examples of which are research and engineering data, computer software and documentation, engineering drawings, technical manuals and reports, blueprints, studies and other information that could be used to produce, operate, repair or modify military or space equipment. Technical information is not covered by the new rule if it is lawfully publicly available without restrictions.[2]

Under the final rule, the contractor must provide "adequate security" to safeguard unclassified controlled technical information that resides on or passes through a contractor's systems from any compromise. In order to provide adequate security, the contractor must implement information systems security in its project, enterprise, or company-wide unclassified information technology systems that contain or carry the unclassified controlled technical information. The final rule requires a security program that, at minimum, implements specified National Institute of Standards and Technology ("NIST") security controls or equivalent controls approved by the contracting officer.

The final rule also requires the contractor to report to DOD any cyber incident that affects the unclassified controlled technical information within 72 hours of its discovery. Reportable cyber incidents include (i) a cyber incident involving the possible exfiltration, manipulation, or other loss or compromise of any unclassified controlled technical information that resides or passes through the contractor's or one of its subcontractor's information systems or (ii) any other activities that allow unauthorized access to the contractor's information systems on which unclassified controlled technical information resides or transits. The rule also specifies further steps that the contractor must take to investigate the potential cyber intrusion and to support any DOD damage assessment activities.

The final rule addresses numerous issues raised in response to the initial proposed rule. First, under the final rule, the release of unclassified controlled technical information to an internet service provider or cloud service provider constitutes the release of such information to a subcontractor. Assuming the release of the information to such vendors is otherwise permissible, the contractor would be required to flow down the new clause to such providers, thereby subjecting those vendors to the new rule's requirements. Given the responsibility for subcontractors placed on a contractor by the new rule, a contractor that releases unclassified controlled technical information to an internet or cloud service provider must understand the security practices and systems of its internet or cloud service providers. Second, DOD rejected the request to institute a safe harbor provision related to reported cyber intrusions as part of the final rule. Third, DOD notes in the final rule that costs to comply with the security controls mandated by the rule may be allowable under federal cost principles. Even though there may be increased costs of complying with the additional cybersecurity requirements, the NIST controls are regarded as mainstream industry practice. It is likely that, pursuant to federal cost principles, any additional reasonable costs to implement these security controls will be allowable and therefore recoverable by the contractor.

The regulation, **Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified Controlled Technical Information** (DFARS Case 2011-D039), appears at 78 Federal Register 69273 (Nov. 18, 2013).

Please contact one of the attorneys listed above with any questions.

Notes

1. DFARS § 252.204-7012(a).
2. DFARS § 252.204-7012(a).

Key Contacts

Christopher Kimball Washington, DC	ckimball@cooley.com +1 202 842 7892