THE
NATIONAL LAW REVIEW

Data Security Advisory for Federal Contractors: Safeguarding Unclassified Controlled Technical Information

Wednesday, December 11, 2013

The **Department of Defense (DoD)** has published its new final rule governing the security measures imposed on DoD unclassified technical information resident on or passing through the unclassified information systems of its contractors and subcontractors. This final rule will require contractors to safeguard unclassified controlled technical information and to report the compromise of such information to the DoD.

The rule, which is now incorporated in part 204 of the DFAR, was originally published for comment in June 2011 and has taken 18 months to reach final publication, partly because it imposes significant new burdens on federal contractors. It requires DoD contracting officers to include a new clause, DFAR 252.204-7012, in any contract that involves the use of technical data, computer software or other technical information described in DoD Instructions as unclassified controlled technical information. Contractors subject to the clause are required to implement data security controls identified in National Institute of Standards and Security (NIST) publication SP 800-53 or provide a convincing case why a proposal alternative is acceptable to achieve equivalent protection.

Article By
Privacy & Security Practice Group at Mintz Levin
MintzGovernment Contracts Alert

Government Contracts, Maritime & Military Law
UCC
Communications, Media & Internet
Labor & Employment
All Federal

Under the final rule, unclassified controlled technical information includes all unclassified technical information with a military or space application that is marked by the DoD as anything other than “approved for public release” or is otherwise lawfully publicly available without restrictions. The examples of technical information provided in the rule are very broad, and 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 and source code.

There are no exceptions for commercial items. If the DoD shares unclassified controlled technical information with a contractor, that information is subject to the requirements of the rule, even if the contractor supplies a commercial off-the-shelf item to satisfy the contract requirements.

Contractors are responsible for assuring that their subcontractors that are provided with controlled technical information also comply with the data security standards. The new contract clause is a mandatory “flow-down” clause to subcontractors. This includes so-called “cloud” data storage providers.

DoD understands that the costs of items it obtains may increase as a result of contractors having to incur additional costs to implement the data security requirements of the NIST guidance, but the department will not provide additional line item cost reimbursement for such added costs.

In the event of a breach of data security involving controlled technical information, the contractor is required to report the incident to the DoD within 72 hours of discovery. The contractor is required to identify the compromised computers and the data accessed during the incident, and to preserve all relevant system monitoring and packet capture data for DoD examination.

The rule is effective immediately, and contractors who receive controlled technical data that have not examined the NIST SP 800.53 guidance should start thinking hard about how to prepare technically and administratively for their next contract that involves the use of such data.

Source URL: https://www.natlawreview.com/article/data-security-advisory-federal-contractors-safeguarding-unclassified-controlled