wiley

ALERT

New DOD Final Rule Imposes Cyber-Reporting Obligations and Basic Safeguarding Protocols for "Unclassified Controlled Technical Information"

November 20, 2013

On November 18, 2013, the U.S. Department of Defense (DOD) issued a final rule imposing new reporting requirements for certain cyber incidents and strengthening DOD's data security requirements for "unclassified controlled technical information" that resides on or transits across contractors' unclassified information systems. *See* 78 Fed. Reg. 69273. The final rule represents a significant reduction in scope from earlier proposed versions of the rule, which would have applied broadly to any "unclassified DOD information" and imposed multiple tiers of data security requirements depending on the type of information on a contractor's system. The final rule has a more narrow scope that provides better guidance to contractors regarding the type of information that will be subject to the rule. Contractors should be attuned to the new security requirements and, in particular, the circumstances that could trigger DOD's new incident reporting obligations. Key aspects of the final rule are highlighted below.

New Rule and Clause Effective Immediately. The final rule adds to the Defense Federal Acquisition Regulation Supplement (DFARS) a new subpart (DFARS 204.73—Safeguarding Unclassified Controlled Technical Information) and corresponding contract clause (DFARS 252.204-7012 Safeguarding of Unclassified Controlled Technical Information). This clause will be included in all DOD contracts beginning November 18, 2013, and prime contractors must include the clause in all subcontracts from that point on, including subcontracts for commercial items.

Authors

Kevin J. Maynard
Partner
202.719.3143
kmaynard@wiley.law

Jon W. Burd
Partner
202.719.7172
jburd@wiley.law

Gary S. Ward
Partner
202.719.7571
gsward@wiley.law

Practice Areas

Government Contracts

New Data Security Requirements. The data security component of the rule requires contractors to implement security programs on any systems that store or transmit "unclassified controlled technical information." The new category of "unclassified controlled technical information" includes all technical data and computer software (as defined in DFARS 252.227-7013) with military or space application that is subject to DOD access controls. This includes, for example, research and engineering data, engineering drawings, specifications, manuals, technical reports, and computer software. The final rule requires affected contractors to "provide adequate security to safeguard unclassified controlled technical information from compromise." The minimum standards to be applied to affected unclassified information technology systems are drawn from fairly standard commercial practices outlined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 to control and protect affected systems. The NIST SP 800-53 standards are already fairly ubiquitous in DOD contracts, and DOD anticipates that the new requirements will therefore come at little additional cost to the industry, overall. At a minimum, contractors must implement access controls, awareness and training, contingency planning, identification and authentication, and maintenance.

New Cyber Incident and Compromise Reporting. The new reporting component requires contractors to report cyber incidents to DOD within 72 hours of discovering the incident. This is the first that DOD has imposed a regulatory reporting obligation for cyber incidents, although DOD previously implemented a voluntary cyber incident disclosure program for defense industrial base participants. Under the new rule, contractors must report incidents where "unclassified controlled technical information" residing on or transiting through a contractor's unclassified system is potentially exfiltrated, manipulated, or otherwise lost or compromised. Contractors must also report any incidents resulting in unauthorized access to its covered systems. One potential criticism of the mandatory disclosure requirement is that these triggering events are subject to some ambiguity.

When reporting an incident, contractors must include the information outlined in DFARS 252.204-7012(d)(1), including the DUNS number, affected contract numbers, facility CAGE code, relevant points of contact, clearance level, DOD systems involved, type of compromise, and a description of technical information compromised. After reporting an incident to DOD, a contractor will also be required to support DOD in assessing the damage. Specifically, the contractor will be required to conduct a further review of its unclassified network, review the data accessed during the incident, and preserve and protect images of known affected information systems as well as all relevant monitoring/packet capture data for at least 90 days. DOD may also conduct its own damage assessment and require the contractor to share affected files and images absent any legal restriction limiting the contractor's ability to share digital media.

More Rulemaking Anticipated. DOD's initial proposed rule had included additional "basic" security requirements for a broader range of unclassified nonpublic information. That aspect of the rule was subsequently overtaken by a proposed Federal Acquisition Regulation (FAR) rule, FAR case 2011-020, Basic Safeguarding of Contractor Information Systems, which would impose similar safeguarding requirements on all federal contractors. In its preamble comments on the final rule, DOD indicated that a final FAR rule would be forthcoming addressing those "basic" safeguarding requirements. As a practical matter, many DOD contractors are already subject to these "basic" safeguarding requirements, which have been incorporated by

reference into many DOD contracts by reference to DOD Instruction 8582.01, Security of Unclassified DOD Information on Non-DOD Information Systems (June 6, 2012).