wiley

ALERT

Department of Defense Issues Sweeping Interim Rule To Expand Cybersecurity Safeguarding Requirements, Reporting Obligations, and Cloud-Based Security

August 27, 2015

The U.S. Department of Defense (DOD) released yesterday an interim rule that imposes sweeping changes to DOD contractor cybersecurity and reporting requirements. The rule significantly expands the breadth and scope of the existing DFARS clause 252.204-7012, meaning that substantially more DOD information and far more DOD contractors will be subject to the information safeguarding requirements of that provision. The clause also reforms the baseline security obligations that contractors must implement when covered DOD information will reside on their information systems—abandoning the previous baseline in the National Institute of Standards and Technology (NIST) Standard Publication 800-53, in favor of NIST Standard Publication 800-171. In addition, the interim rule expands the cybersecurity breach reporting obligations and establishes new requirements for contractors utilizing cloud-based computing services to fill DOD information technology service requirements.

New Guidelines for Safeguarding DOD Information, Adequate Security, and Cyber Incident Reporting. Many contractors are still adapting to the information safeguarding requirements DOD imposed in 2013 for "unclassified controlled technical information." The new interim rule may undercut much of that effort based on several prominent changes. The key takeaways appear to include:

- **A new IT security baseline for "adequate security":** The previous version of DFARS clause 252.204-7012 included a seemingly random selection of 51 baseline security standards

Authors

Jon W. Burd
Partner
202.719.7172
jburd@wiley.law

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Government Contracts

from NIST 800-53. The new rule abandons the NIST 800-53 baseline and adopts instead the framework outlined in NIST 800-171. DOD notes that this will result in a 30% reduction in required tasks, as NIST 800-171 is "specifically tailored for use in protecting sensitive information residing in contractor information systems" and presents requirements in "an easier to use format."

- **An expanded scope of information that requires "adequate security"**: Whereas the previous version of DFARS 252.204-7012 applied only to "unclassified controlled technical information," the new interim rule expands the scope of the clause to include "covered defense information," which broadly includes any information that is controlled technical information, "critical information," or "export control" information. The clause also applies to "[a]ny other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls." Notably, whereas the previous version of the clause arguably applied only to information received from DOD, the clause now clearly applies to information that is "collected, developed, received, used, or stored by or on behalf of the contractor in support of the performance of the contract."
- **More responsibility on contractors to identify covered information:** The interim rule revises the definition of "unclassified controlled technical information" to eliminate the marking requirement. Previously, contractors were required to safeguard unclassified controlled technical information that bore a restrictive distribution legend pursuant to DOD Instruction 5230.24. Now, contractors will be required to safeguard controlled technical information that "would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth" in the Instruction. This suggests that information must be safeguarded regardless of whether it bears a restrictive legend. Likewise, the interim rule includes a new "catch all" provision requiring the safeguarding of other information, "marked or otherwise," that the contract requires the contractor to safeguard.
- **A more formal process for obtaining permission to use "alternate" safeguarding procedures:** The previous version of DFARS clause 252.204-7012 permitted a contractor to provide the contracting officer with "a written explanation" any time it implemented "an alternative control or protective measure" that could achieve "equivalent protection" to the specified NIST standards. Now, the interim rule will require a contractor to obtain written approval "prior to contract award" by "an authorized representative" of the DOD Chief Information Officer of any "alternative but equally effective security measures." This imposes a significantly higher standard on contractors and will require proactive consideration prior to contract award.
- **New cybersecurity breach reporting obligations and processes:** In addition to the expanded scope of information that is subject to DOD's "adequate security" requirements, more contractor IT systems will now be subject to DOD's 72-hour cyber incident reporting obligation. The interim rule also introduces new protections for subcontractor and contractor proprietary information that is reported to DOD, and states that DOD is working to implement a new cyber incident reporting portal.

New Cloud Computing Requirements. In addition to changes to the baseline for safeguarding DOD information and reporting cybersecurity incidents, the interim rule imposes new requirements for contractors that plan to utilize cloud-based computing services to meet Government information technology services

requirements. Contractors intending to fulfill DOD IT services requirements with a cloud-based solution will have to make a representation to that effect in the proposal, and DOD will permit contracts/subcontracts for cloud-based services to be awarded only to service providers that have obtained provisional authorization from the Defense Information Systems Agency (DISA). If a contractor proposes to use cloud computing services after award, it must first obtain approval from the contracting officer.

Contractors who utilize cloud-based services must comply with the security protocols outlined in DISA's Cloud Computing Security Requirements Guide. Service providers would be required to store all Government cloud-based data within the United States, unless the data is physically located on DoD premises or the contracting officer grants prior approval. Contractors and their service providers would be required to provide the Government with access to the relevant data, contract personnel, and related facilities during any Government audit, inspection, investigation, or similar activity. Cloud-based information services would also be subject to cyber incident reporting and response requirements. Contractors must report any cyber incidents, discovery of malicious software, spillage, or requests for access to data from third parties, including from any Federal, State, or Local agency. In the event of a cyber incident, contractors must preserve images of all known affected systems for at least 90 days after the submission of the cyber incident report. Contractors also need to provide DoD access to any information or equipment necessary for a forensic analysis.

The Interim Rule is effective now. Finally, the interim rule is in effect as of August 26, 2015. DOD citied the urgent need for protecting government information from cyber threats as the basis for issuing an interim rule prior to the public comment period. Industry may submit comments on the interim rule by October 26, 2015, and should expect modest revisions to address those comments in any forthcoming final rule. In the meantime, however, these new standards apply and DOD contractors should take immediate steps to understand how they affect existing IT policies and procedures, and where any gaps may exist between these standards and a contractor's current capabilities.

DOD's interim rule focuses on the defense contracting community and those interacting with government systems and handling government information, but the federal government's interest in cybersecurity reaches all sectors of the U.S. economy. Policymakers at all levels are grappling with myriad data and network security issues. While efforts to identify best practices, improve incident responses, and promote improve information-sharing are underway, in the meantime the government is looking to its procurement and oversight authorities to raise the bar for the private sector. We expect policymakers at all levels of government, including civilian agencies, will look to DOD for best practices, so DOD's new approach may have broader impact, both within civilian agency acquisitions and in other industry segments.