Bloomberg BNA

Federal Contracts Report™

Reproduced with permission from Federal Contracts Report, 104 FCR 1041, 10/13/15. Copyright © 2015 by The Bureau of National Affairs, Inc. (800-372-1033) http://www.bna.com

DOD

Recent Increases to DoD Contractors' Cyber Security Reporting Obligations

By Marcia G. Madsen and Luke Levasseur

With incursions into government and commercial information systems in the news frequently, cyber security—which has been a serious focus for the government and its contractors—has become a critical concern. Because contractors possess so much government information and interact with their government customers routinely, it has also become a substantial compliance issue, with new and increasing rules and regulations changing the applicable requirements in this crucial area (and several legislative proposals each congressional session potentially making broader changes). Government contractors, as well as their subcontractors and suppliers, must understand the sense of urgency that has developed regarding cyber security and must be prepared to devote substantial resources to this issue.

Recently, the largest government buyer of goods and services, *i.e.*, the Department of Defense (DoD), issued a series of new regulations that have placed the already ''on guard'' contractor community on high alert. This article focuses on those important new DoD regulations—which contractors (and subcontractors) doing defense-related work must understand and for which they should have detailed compliance programs. Notably, other parts of the government (*e.g.*, the Department of Homeland Security and law enforcement agencies) are extremely focused on cyber threats as well, and are working to coordinate efforts of government agencies (sometimes more successfully than others), while imposing additional regulations on government contractors.

This article addresses two recent regulations implemented by DoD: (1) the DFARS provisions issued at the end of August and imposing reporting obligations related to network penetrations and cloud computing; and (2) the October 2 regulations related to DoD Defense Industrial Base (DIB) cyber security activities.

Marcia G. Madsen is a partner in, and the head of, Mayer Brown LLP's Government Contracts Washington, D.C. practice group; Luke Levasseur is a counsel in that group.

DFARS Provisions Imposing Contractor Reporting Obligations for Cyber Incidents. In late August 2015, DoD issued interim rules amending the Defense Federal Acquisition Regulations (DFARS) with respect to ''network penetration reporting and contracting for cloud services.'' The new rules became effective when they were issued and are now found in the electronic version of the DFARS; any comments on these provisions are due to DoD by October 26, 2015.

Parts of two National Defense Appropriation Acts, section 941 of the FY 2013 NDAA and section 1623 of the FY 2015 NDAA, imposed requirements that had to be implemented by changes to the DFARS. DoD sought to address those requirements with its interim rules. Substantively, these provisions revise several definitions that are applicable to numerous parts of the DFARS, expand the incident reporting requirements applicable to contractors, and impose security requirements applicable to cloud computing.

New Definitions. Three regulatory definitions were added to the DFARS, expanding and clarifying contractors' security obligations.

First, ''compromise'' of a system is defined as a ''disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.''

Second, a ''cyber incident'' means ''actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing'' within that system.

Third, ''media'' is defined as ''physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which covered

COPYRIGHT © 2015 BY THE BUREAU OF NATIONAL AFFAIRS, INC. ISSN 0014-9063

defense information is recorded, stored, or printed within a covered contractor information system.''

The interim rules' use of phrases like ''may have occurred'' and ''potentially adverse'' in the definitions of ''compromise'' and ''cyber incident'' (as emphasized above) should give contractors pause with respect to the degree of certainty to which one will be expected to investigate and understand whether a system has been compromised—or a cyber incident has occurred. It is not clear what is required for those thresholds to be satisfied, and contractors will be reasonably concerned that agencies' after-the-fact judgments about what should have been reported may be more expansive than contractors' real-time assessments.

Enhanced Reporting Obligations. The DFARS clause included in the interim rules implements statutory requirements that cleared defense contractors must report penetrations of networks and information systems—and that they must provide DoD personnel with access to equipment and information to assess the impact of such penetrations. Specifically, the rules require *contractors and subcontractors* to report any cyber incident that results in an actually or potentially adverse effect on:

- ''a covered contractor information system''; or
- ''covered defense information residing'' within a covered contractor system; or
- the ''contractor's ability to provide operationally critical support.''

Each phrase used to describe these obligations is defined in the first part of the new contract clause, DFARS 252.204-7012(a), and must be carefully analyzed by a contractor to understand its reporting obligations. When a contractor discovers a ''cyber incident'' raising these issues, it is required to ''[c]onduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts.'' The contractor also must ''analyz[e] covered contractor information system(s)'' and information systems on its networks that may have been accessed, analyze the extent of the intrusion, and ''[r]apidly report cyber incidents to DoD.''

Notably, DFARS clause 252.204-7009 is included in the interim rule, limiting the use and disclosure of contractor and subcontractor information that is provided in response to actual or potential cyber incidents. This provision provides some protection to contractors being forced to disclose information about their systems by restricting third-party contractors working cyber security response from disclosing information reported by another contractor—and provides penalties for improper disclosures.

Cloud Computing. DoD's interim rule also imposes a series of new requirements regarding how DoD can acquire cloud-based computing services. ''Generally, the DoD shall acquire cloud computing services using commercial terms and conditions that are consistent with Federal law, and the agency's needs'' (subject to the restrictions imposed by the rule). A company wishing to provide cloud-based services to DoD must obtain at least a ''provisional authorization by Defense Information Systems Agency, at a level appropriate to the requirement'' it is seeking to satisfy.

One cloud-related restriction important to service providers is the new DFARS 239.7602-2, which (for ''all government data that is not physically located on DoD premises'') requires storage of DoD data within the United States or outlying areas. Contracting officers can permit storage outside the United States, though they must do so via written notification to the contractor. The interim rule also imposes a series of new security requirements related to cloud-based data storage.

DoD's interim rule also has cloud-based rules that will be of interest to contractors that are not cloud services providers. For instance, DFARS 252.239-7009 requires contractors providing various types of services to make representations about whether they ''anticipate that cloud computing services will be used in the performance of any contract or subcontract resulting from this solicitation.'' This certification will need to be carefully considered (and a careful examination of subcontractors' cloud storage should be made) before submission of any proposal.

DoD's Interim Final Rule on DIB Cyber Security Activities. Since late 2013, DoD has participated conducted a ''cybersecurity information sharing program'' under which participants ''share unclassified and classified cyber threat information.'' According to DoD, the goal of the program is ''to enhance and supplement DIB participants' capabilities to safeguard DoD information that resides on or transits DIB unclassified networks or information systems.'' In short, DoD's program ''is designed to improve DIB network defenses, reduce damage to critical programs, and increase DoD and DIB cyber situational awareness.''

The principal effect of the new regulations is to make clear that much of the sharing that was formerly voluntary under the DIB program is now mandatory. The new regulations use many of the same definitions and apply the same requirements as the interim rule already applicable to contractors (as discussed above). In short, the regulation ''requires all DoD contractors to rapidly report cyber incidents involving covered defense information on their covered contractor information systems or cyber incidents affecting the contractor's ability to provide operationally critical support.''

Notably, DoD's imposition of mandatory requirements did not eliminate the voluntary DIB program. The new rules ''modif[y] the eligibility criteria'' with the asserted goal of ''permit[ting] greater participation in the DoD-DIB CS information sharing program,'' under which contractors may continue to share cyber security information [beyond what is required under the regulations] with DoD and other participants in the program.

Conclusion. Cyber security is an increasing concern not just for DoD and other parts of the government, but for all government contractors and the companies in their supply chains (as well as for individuals). DoD is implementing new rules to address these important threats—and more legislation and regulations are certain to be implemented to address these important issues. Government contractors will have to work hard to remain up-to-date on the evolving ''rapid[] reporting'' requirements—and will need to their compliance obligations accordingly.

 COPYRIGHT © 2015 BY THE BUREAU OF NATIONAL AFFAIRS, INC. FCR ISSN 0014-9063