Holland & Knight

GOVERNMENT CONTRACTS

DoD's New Cybersecurity and Cloud Standards and Reporting Requirements

August 28, 2015

By
Mary E. "Mary Beth" Bosco|
Norma M. Krayem

HIGHLIGHTS:

The Department of Defense (DoD) released interim rules on Aug. 26, 2015, implementing provisions of the 2013 and 2015 National Defense Authorization Acts.

The interim rules cover a broad range of DoD contractors and subcontractors. All DoD contractors are covered by the interim rule – no exception is provided for small businesses.

Covered contractors must report cyber incidents within 72 hours of discovery.

The Department of Defense (DoD) released interim rules implementing provisions of the 2013 and 2015 National Defense Authorization Acts. The rules, released on Aug. 26, 2015, are effective immediately and establish the following:

information system security requirements
mandatory cyber incident reporting
cloud computing standards and procedures

They contain new Defense Federal Acquisition Supplement (DFARS) clauses covering each of these areas. While the rules are now effective, DoD is providing until Oct. 26, 2015, for the submissions of comments to be considered when DoD formulates a final rule.

The DoD regulations are the third set of cybersecurity regulations issued this summer affecting government contractors. As explained further below, both the National Records and Administration Agency (NARA) and the Office of Management and Budget (OMB) recently issued guidance for the safeguarding of controlled unclassified information (CUI) intended to be incorporated in the

Federal Acquisition Regulation (FAR).

Standards for Cybersecurity Protections

The DoD rules' basic requirement is that contractors storing or using "covered defense information" must provide "adequate security" for that information. (DFARS Clause 252.204-7012.) All DoD contractors are covered by the interim rule – no exception is provided for small businesses. Covered defense information encompasses a large portion of non-classified DoD information that transits or is stored in a contractor's IT system. More specifically, covered defense information is any unclassified information that is either provided by DoD to the contractor or is collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of performance of its contract. There are four types of covered defense information:

1 controlled technical information, which means technical information with military or space application that is subject to controls on its access, use, reproduction or release

2 critical information relating to the security of military operations, such as information that would assist adversaries in learning about the military's intentions, activities and capabilities (for example, information about equipment transport by private carriers)

3 export controlled information, which includes information about commodities or technologies that are subject to the export administration regulations, international traffic in arms regulations and munitions lists, license applications, and sensitive nuclear information

4 any other information, marked or otherwise identified in a contract as subject to safeguarding or dissemination limitation required by law, regulation, or government policy, including proprietary business information and technical information such as specifications

(DFARS 252.204-7102(a).)

The standards governing security protection for covered defense information depend on the type of information system. If the contractor is operating a system or service on behalf of the government, then cloud computing services must meet DoD's interim cloud computing security requirements (see below) and other IT services and systems must meet specific requirements that will be set forth in the contract for those services or systems. Other contractor information systems that support a covered DoD contract must meet the standards contained in National Institute of Standards and Technology (NIST) Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.

Mandatory Breach Reporting

Under the new rules, covered contractors must report any cyber incidents within 72 hours of discovery and must conduct an investigation to gather evidence of the scope of the incursion. Importantly, a cyber incident covers not just intrusions into information systems or data, but also circumstances that affect the contractor's ability to perform the requirements of a contract that is designated as operationally critical support. (DFARS 252.204-7012(c).) The new DFARS provisions do not expand on what constitutes discovery of an incident, such as whether the contractor's time period runs from confirmation that a breach incident has occurred or from the first notice that an incident occurred, whether ultimately validated, confirmed or not.

Reports must be submitted to the DoD-DIB Cyber Incident Reporting & Cyber Threat Information Sharing Portal. In order to submit a report, a contractor must have or acquire a "DoD-approved medium assurance certificate" for reporting cyber incidents. In addition to the reporting requirement, the new DoD regulations obligate contractors to:

- submit to DoD any malicious software they are able to isolate
- preserve and protect images of all known affected information systems and relevant monitoring/packet capture data for at least 90 days from the submission of the incident report
- permit DoD access in order to perform its own forensic investigation or damage analysis

For its part, while DoD commits to protect against unauthorized use or release of contractor incident report information, the agency also warns contractors to remove, to the extent possible, proprietary or identification information from the reports. The regulations authorize DoD to share information concerning the breach that is not created by or for DoD with the following:

- entities whose missions that may be affected by the information
- organizations assisting with diagnosis, detection, or mitigation of the incident
- counterintelligence or law enforcement personnel
- entities with national security purposes, including the Defense Industrial Base participants
- support services contractors with appropriate protections

(DFARS 252.204-7012(i).) In contrast, DoD may share information that *is* created by or for it (including the report) with each entity described above, as well as for "any other lawful Government purpose or activity."

Finally, prime contractors must flow down the cyber protection and reporting clause to their subcontractors. Subcontractors are required to submit cyber incident reports to both their prime contractor and DoD, and lower-tier subcontractors must submit them to their upper-tier subcontractors until they reach DoD.

Cloud Computing Requirements

The new DoD cloud computing clause requires contract awardees to make a representation as to whether or not they intend to use cloud computing in the performance of the contract or subcontract. If a contractor indicates that it will not use cloud computing, but later decides to make use of cloud services, the contractor must obtain the contracting officer's approval prior to utilizing such services on the contract. The clause defines cloud computing as:

[a] model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provided interaction. This includes other commercial terms, such as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. It also includes commercial offerings for software-as-a-service, infrastructure-as-a-service, and platform-as-a-service.

(DFARS 252-239-7009(a)(b) and (c).)

Contractor cloud computing safeguards and controls must meet those set forth in the Cloud Computing Security Requirements Guide. Unless the government grants an exception, all government data that is not physically located on DoD premises must be maintained within the United States or outlying areas. In addition, contractors must report cloud computing security breaches in accordance with the breach notification and protocols described above.

No One-Size-Fits-All Process for Cybersecurity Compliance

The new DoD interim rules follow two other recent cybersecurity pronouncements for federal government contractors. On Aug. 11, 2015, OMB released a draft guidance document titled Improving Cybersecurity Protection in Federal Acquisitions. (See Holland & Knight's alert, "OMB Issues Guidance on Government Contractors' Cybersecurity Systems," Aug. 14, 2015.) The OMB Guidance, which covers CUI for all agencies, calls for compliance with NIST Publication 800-171 for certain types of contractor systems, and compliance with NIST Publication 800-53 (which is more stringent) for others. This contrasts with the DoD rules' reliance on NIST Publication 800-171 and specific contract standards. NARA's CUI proposal uses both NIST Publication 800-171 and 800-53 to set its standards.

A government contractor with both DoD and civilian contracts, that handles both CUI and covered defense information on the same system, could be facing multiple and conflicting standards. That data could be subject to one standard under a DoD contract and another standard under a civilian agency contract. Accordingly, there is no one-size-fits-all process for determining what cybersecurity compliance will look like for government contractors. At this point, a contractor may want to determine the most stringent controls potentially

applicable to its mix of contracts and types of information and measure the adequacy of its information assurance systems against that standard.