Kilpatrick

Insights: Alerts

Department of Defense (DoD) Issues Final Rule on Safeguarding Covered Defense Information and Related Information Security Compliance Requirements

OCTOBER 26, 2016 Written by Gunjan R. Talati

On October 21, 2016, the Department of Defense ("DoD") issued a final rule (the "final rule") codifying the specific actions DoD contractors and subcontractors must take to adequately safeguard "covered defense information" ("CDI") and to report and respond to cyber incidents on "covered contractor information systems," including those leveraging the cloud. The final rule updates several provisions of the Defense Federal Acquisition Regulation Supplement ("DFARS") including two significant interim clauses DoD issued in late 2015: DFARS 252.239-7010 ("Cloud Computing Services") and DFARS 252.204-7012 ("Safeguarding Covered Defense Information and Cyber Incident Reporting") (herein referred to as the "interim clauses"). The interim clauses largely overhauled DoD's scheme for information security on contractor systems, including cloud-based systems. This Client Alert comes as the latest in a series of alerts members of our team have made as the Government continually updates its approach to information and data security to counter increasingly dangerous cyber-risks.

Following the interim rulemaking, many Federal contractors and subcontractors were surprised by the interim clauses, which came without notice or opportunity to comment. The contractor community also had mixed-to-negative reactions to the interim clauses because they imposed new, seemingly burdensome security controls, required contractors to "rapidly report" cyber incidents to DoD within 72 hours of discovery, and required contractors to observe a host of seemingly burdensome forensic preservation requirements. They also struggled with the broad applicability of the clauses, which applied to any "contractor information system" handling a broad universe of data and information DoD termed "covered defense information" or "CDI." In addition, many commercial cloud service providers ("CSP") expressed concern that the clauses imposed standards more invasive and burdensome than what they had developed in the commercial marketplace.

The final rule revises and reissues several sections of the DFARS dealing with information security. While not an exhaustive listing, the major changes in the final rule address the following:

Applicability of DFARS Clauses: The final rule exempts solicitations or contracts "solely for the acquisition of commercially available off the shelf [COTS] items" from the requirements of 252.204-7008 (Compliance with Safeguarding Covered Defense Information Controls) and 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting).

Definition of CDI: The final rule revises and clarifies the definition of "CDI" to include "unclassified controlled technical information" as described in the National Archives and Records Administration's ("NARA") CUI Registry. This definition somewhat narrows the interim rulemaking's definition of CDI and requires that the Government mark

or otherwise identify CDI it provides to contractors. But the final rule continues to require contractors to recognize and self-identify CDI they may develop in the course of performing their contract(s) and protect that information in accordance with the DFARS clauses.

Applicability of Various Security Standards: The final rule assigns different information security standards based on whether the information system is (a) operated on behalf of the Government or (b) owned and operated by the contractor in carrying out a Government contract.

Contractor information systems operated on behalf of the Government are subject to "the security requirements specified elsewhere in [the DoD contract]." Cloud computing services operated on behalf of the Government are subject to DFARS 252.239-7010, Cloud Computing Services, which incorporates the DoD's Security Requirements Guide (SRG) for cloud services.

In contrast, contractor systems owned and operated by the Contractor are subject to the security controls set forth in the National Institute of Standards and Technology (NIST) 800-171. In addition, prime contractors whose solutions include using external CSPs to store, process, or transmit CDI must, at a minimum, utilize a CSP meeting of FedRamp moderate baseline security requirements. Prime contractors must also require and ensure (by including in CSP contracts) that external CSPs comply with DFARS 252.204-7012's requirements relating to cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.

Flow-Down Requirements: As before, DFARS 252.204-7012 requires prime contractors to flow-down the clause in its entirety, without alteration, but now it is further refined to apply to subcontracts where the information required for subcontract performance "retains its identity as [CDI]." It permits prime contractors to consult with the Contracting Officer as necessary to determine whether flow-down is necessary in a given situation.

Security Controls Variance: Like its interim rule predecessor, the final DFARS 252.204-7012 requires contractors subject to NIST 800-171 to implement those security controls "as soon as practicable but not later than" December 31, 2017. Prior to October 1, 2017, contractors may notify the DoD Chief Information Officer (CIO) within 30 days of award indicating what 800-171 controls the contractor has not implemented as of the date of contract award. In addition to this temporary notification period, the clause permits contractors to seek authorization from the CIO to vary from the NIST 800-171 requirements. Contractors seeking a variance must obtain an adjudication from the CIO that the security requirement for which the contractor seeks variance is not applicable or that the contractor will implement an "alternative but equally effective security measure" in its place.

At a minimum, defense contractors subject to the final rule should take the following steps to ensure compliance with the final rule and corresponding DFARS clauses:

(1) Analyze the final rule
(2) Review their DoD contracts to identify whether affected DFARS clauses apply
(3) Review their information systems to determine whether they own or operate covered information systems handling CDI
(4) Evaluate how the final rule affects their compliance with their DoD Contracts, DFARS, and incorporated standards (such as NIST, FedRamp, and DISA's Security Requirements Guide for Cloud Computing (SRG))
(5) Evaluate flow-down obligations to downstream subcontractors and vendors

It bears noting that this final rule applies to DoD and its various branches and agencies, not civilian agencies. Civilian agencies have their own specific information security clauses, making it critical that contractors review and become familiar with the regulations and clauses applicable to them. Nonetheless, DoD has taken up the forefront of Government information security measures and contractors would be well-advised to consider DoD's final rule as an indication of where other agencies may be heading in terms of information security, cyber incident reporting and response.

Kilpatrick Townsend's Government Contracts group regularly assists contractors in assessing information security compliance capabilities and implementing compliant systems.

Related People



Gunjan R. Talati
t 404.815.6503
gtalati@ktslaw.com