Cooley

DoD Contractors Required to Meet Cybersecurity Requirements by Year End

October 4, 2017

The window for Department of Defense (DoD) contractors to bring themselves into compliance with cybersecurity requirements is closing. Specifically, changes to the Defense Federal Acquisition Regulation Supplement (DFARS) published in late 2016 require that DoD contractors and subcontractors provide "adequate security" on "covered information systems." The new rule also imposes reporting requirements for cyber incidents. Failure to comply with these requirements could result in loss of government contracting opportunities and civil and criminal liability for responsible companies and individuals.

Background

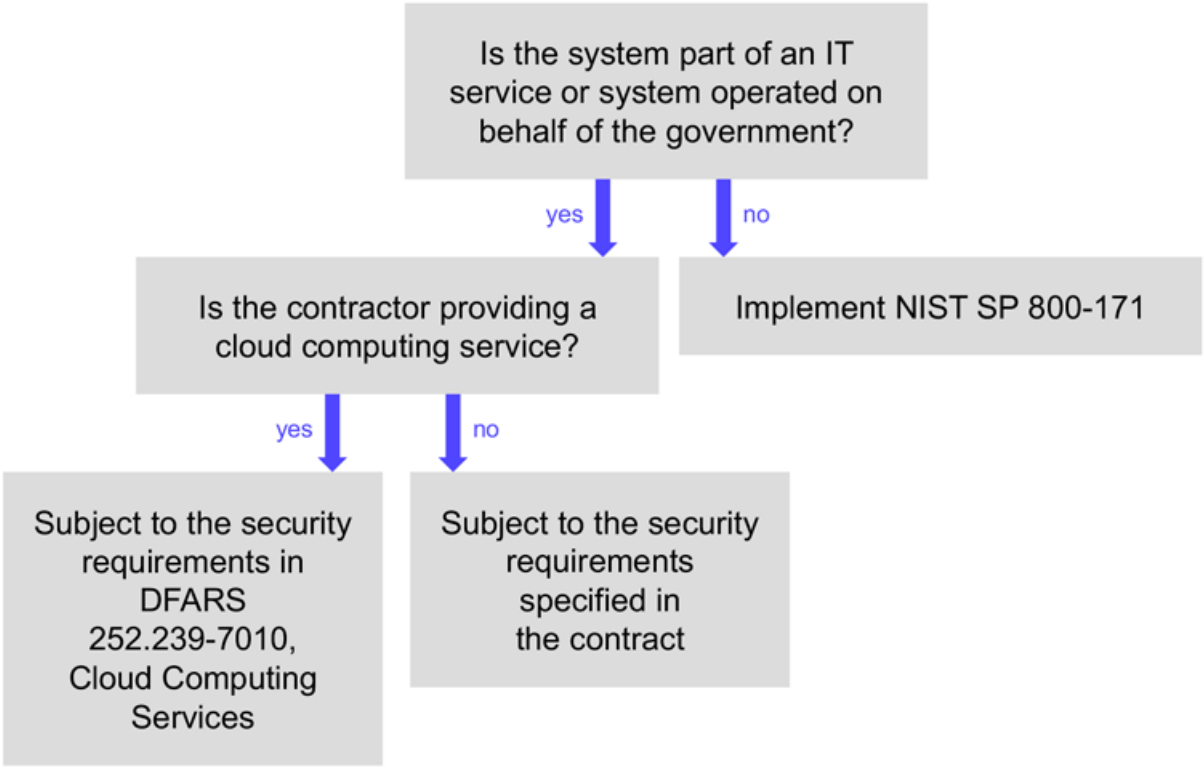
On October 21, 2016, DoD published a final rule significantly expanding the obligations of private industry with respect to cybersecurity on contractor information systems that host certain government and other sensitive data. 81 Fed. Reg. 72986 (Oct. 16, 2016). Specifically, the new rule amends the contract clause at DFARS 252.204-7012, which addresses "Safeguarding Covered Defense Information and Cyber Incident Reporting." According to DoD, "[t]he objectives of the rule are to improve information security for DoD information stored on or transiting contractor information systems as well as in a cloud environment." *Id.* at 72996. ***The amended DFARS clause imposes a critical and fast-approaching compliance deadline for DoD contractors and subcontractors to implement specific security measures on their "covered systems" by December 31, 2017.***

The new contract clause at DFARS 252.204-7012 mandates that DoD contractors and their subcontractors "provide adequate security" on all "covered contractor information systems." DFARS 252.204-7012(b). The relevant definitions are as follows:

- "***Covered contractor information system***" means "an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores or transmits covered defense information." DFARS 252.204-7012(a).
- "***Covered defense information***" means "unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations and government-wide policies, and is – (1) marked or otherwise identified in the contract, task order or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or (2) collected, developed, received, transmitted, used or stored by or on behalf of the contractor in support of the performance of the contract." *Id.*
- "***Controlled technical information***" means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions." *Id.*

The measure of “adequate security”

As illustrated in our diagram below, the new contract clause contemplates different measures of "adequate security," the application of which depends on whether the contractor's "covered information system" is part of an IT service or system "operated on behalf of the government."



If a contractor's covered information system *is not* part of an IT service or system operated on the government's behalf, "adequate security" requires, at a minimum, implementing the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-171 ***"as soon as practical, but not later than December 31, 2017."*** DFARS 252.204-7012(b)(2)(ii)(A). NIST SP 800-171, called "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," provides more than 100 performance-based security requirements grouped into 14 families of controls. Contractors must implement security measures beyond NIST SP 800-171 as required "in a dynamic environment or to accommodate special circumstances … and any individual, isolated or temporary deficiencies based on an assessed risk or vulnerability." DFARS 252.204-7012(b)(3). Requests to vary from NIST SP 800-171 may be submitted to the contracting officer, for review by DoD's Chief Information Officer, if a particular security requirement is inapplicable or if the contractor proposes to use "an alternative but equally effective" measure of security. DFARS 252.204-7008(c)(2).

If the covered information system *is* part of an IT service or system operated on the government's behalf, and the contractor is providing cloud computing services, the relevant "adequate security" requirements are specified in DFARS 252.239-7010, Cloud Computing Services. DFARS 252.204-7012(b)(1)(i). The clause at DFARS 252.239-7010 mandates that the contractor comply with the Cloud Computing Security Requirements Guide. DFARS 252.239-7010(b)(2). On the other hand, if the covered information system is part of an IT service or system operated on the government's behalf, but the contractor is *not* providing cloud computing services, DoD will specify the relevant security requirements in the contract itself. DFARS 252.204-7012(b)(1)(ii).

Cyber incident reporting obligations

The amended DFARS clause also imposes specific cyber incident reporting requirements. ***If a contractor discovers that a cyber incident has occurred impacting a covered information system or covered defense information, the contractor must investigate, and "rapidly report" such incidents to DoD within 72 hours of discovery.*** DFARS 252.204-7012(c)(1). The clause provides the DoD website where contractors should report such incidents, the required elements of which include identifying information about the contractor, where the compromise took place, a narrative describing the incident, the type of compromise, what technique was used, the DoD programs or systems involved, and the impact on covered defense information. The contractor must provide any isolated malicious software to DoD, preserve images of known affected systems and allow DoD access to information or equipment as necessary to conduct its own forensic analysis. DFARS 252.204-7012(d)-(f).

Other key requirements

Contractors must flow the DFARS 252.204-7012 clause down to subcontracts at any tier that will involve covered defense information. The clause also applies to contracts and subcontracts of any dollar value, with small businesses and for commercial items. DFARS 252.204-7012(m)(1). The clause is not required in contracts or subcontracts for commercially available off-the-shelf (COTS) items. DFARS 204.7304(c).

At this point, contractors and subcontractors self-certify compliance with the new requirements, and therefore the ramifications of a compliance failure are potentially severe. The government could terminate a contract over noncompliance. There could also be civil or criminal liability for a knowing misrepresentation of compliance, such as pursuant to the False Claims Act. Contractors and subcontractors must therefore be proactive in ensuring information systems are adequately secured and processes are in place to quickly respond in the event of an incident.

Cooley has significant experience in government contracts and cybersecurity and with helping companies navigate the legal and business challenges presented by security breaches. Our cybersecurity and privacy practice is consistently ranked among the best in the country. Please contact one of the lawyers identified on this alert for more information or assistance.

Key Contacts

Christopher Kimball Washington, DC	ckimball@cooley.com +1 202 842 7892
Kevin King Washington, DC	kking@cooley.com +1 202 842 7823
Andrew Lustig Reston	alustig@cooley.com +1 703 456 8134
Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090