Government Contracting Insights **By Susan Cassidy and Patrick Stanton**

Cybersecurity Requirements Clarified

On Jan. 27, the Defense Department issued an updated frequently asked questions regarding the application and requirements of Defense Federal Acquisition Regulation Supplement 252.204.7012 "Safeguarding Covered Defense Information and Cyber Incident Reporting."

Though questions remain regarding various nuances of the rule, the update is a helpful document for those contractors still working on its implementation. Divided into three sections — General Application, Security Requirements and Cloud Computing — the update provides answers to 59 commonly asked questions and provides greater clarity on a number of important points.

As the department has now issued multiple versions of this rule over the last several years, some imposing different security standards, vendors may have contracts that require different and conflicting security requirements on the same internal networks. The FAQ acknowledges this reality and informs contractors that the department has instructed its contracting officers to work through these issues with contractors, with the goal of working toward consistent implementation of the most recent version of the DFARS clause. Contractors with older versions of the rule in their contracts are therefore well advised to engage their contracting officers and work toward a modification of outdated security requirements.

What is the application to commercial item contracts? The update clarifies that DFARS 252.204.7012 is not required for solicitations and contracts where the only items being procured are commercial-off-the-shelf items. However, the clause is required for all other solicitations and contracts where covered defense information is involved, including the acquisition of commercial items that include it. The FAQ does not address directly whether the clause must be flowed to subcontractors where the prime contract may not be solely for COTS items but where the subcontract is.

In September, the National Archives and Record Administration issued a final rule regarding the protection of controlled unclassified information. The NARA Rule is consistent with the update, as it is unclassified information that requires safeguarding or dissemination controls pursuant to laws and regulations.

Furthermore, both items establish National Institute of Standards and Technology Special Publication 800-171 as the minimum security standard for protecting them. Thus, the two rules are not in conflict.

The protections required to protect government information are dependent upon the type of information being protected and the type of system on which the information is processed or stored. Thus, different information is subject to different protections depending upon whether it is housed on contractor or Defense Department systems.

One of the primary differences between the security requirements imposed by earlier versions of the rule and the current version is the addition of multifactor authentication as a minimum security standard. The update clarifies that this requirement necessitates authentication using a combination of something you know — such as a password — something you have, like a fob, smart-card, or a mobile app on a smartphone — and a biometric marker such as a fingerprint or iris.

The update notes that the physical location of an individual does not fall under one of these three categories. Accordingly, presence within a secure facility cannot be used as a substitute for one of the factors under multifactor authentication.

The update provides three points of clarification on how to handle smartphones and tablets. First, multifactor authentication is not required for access to these devices, regardless of whether covered defense information is stored on the device or the device is merely used to access systems with it. Second, when such information is stored on the device, it must be encrypted to segregate it from the other information on the device. Third, when the device is used to access information systems with covered defense information, the system must be protected by multifactor authentication, which can be entered through the device.

The FAQ clarifies that there are three potential security standards that may apply when a contractor uses a cloud solution.

First, the DoD Cloud Computing Security Requirements Guide applies when a cloud solution is being used to process data on the department's behalf. When the department is contracting directly with a cloud service provider to host or process data in the cloud, or a cloud solution is being used for processing that the department normally conducts but has outsourced.

Second, NIST SP 800-171 standards apply when a contractor uses an internal cloud as part of its internal enterprise network systems to process data when performing under a Defense Department contract requirement such as designing a new aircraft and using the cloud solution internally — not a third party — for the engineering design.

Third, a contractor is only required to flow down the update in its entirety when a cloud service provider is considered a subcontractor for a specific contract and will be handling classified information. However, where the provider is not a subcontractor but nonetheless is provided access to the information, the contractor must flow down security requirements equivalent to the federal risk and authorization management program moderate baseline as well as comply with requirements in DFARS 252.204-7012 for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.

The FAQ notes that the right to physical access requirement to cloud computing data centers in order to conduct forensic analysis implements a statutory requirement that the department cannot waive. Nonetheless, DoD notes that it "normally will not require physical access" if the cloud service provider preserves images of all the systems known to be affected by a cyber incident.

Susan Cassidy is a partner and Patrick Stanton is an associate in Covington and Burling's government contracts group.