COVINGTON

Department of Defense Issues Final Rule - Network Penetration Reporting and Contracting for Cloud Services

October 24, 2016

Government Contracts

Overview

On October 21, 2016, the Department of Defense (DoD) issued its long awaited Final Rule—effective immediately—imposing safeguarding and cyber incident reporting obligations on defense contractors whose information systems process, store, or transmit covered defense information (CDI). The Final Rule has been years in the making, starting with the promulgation of an initial rule in November 2013, followed by two interim rules in August 2015 and December 2015. DoD also clarified a number of issues with regard to contracting for cloud computing services arising from the August 2015 interim rule.

The Final Rule implements section 941 of the Fiscal Year (FY) 2013 National Defense Authorization Act (NDAA) and section 1632 of the FY 2015 NDAA. Section 941, which applies to "cleared defense contractors," and section 1632, which applies to contractors designated as "operationally critical," imposed certain reporting requirements on federal contractors with regard to cyber incidents involving contractor information systems that contain DoD information. As with the two interim rules, the Final Rule applies these and other cybersecurity requirements to all covered DoD contractors and subcontractors, not just to the "cleared contractors" and "operationally critical contractors" referenced in the 2013 and 2015 NDAAs.

The Final Rule does not address the third-party liability protections for the reporting of cyber incidents included in section 1641 of the FY 2016 NDAA for certain defense contractors, which are now incorporated in 10 U.S.C. § 391 (operationally critical contractors) and 10 U.S.C. § 393 (cleared contractors). As discussed below, these liability protections are the subject of a separate, but related, DFARS case currently under regulatory review, and DoD confirmed that the regulatory implementation of these liability protections "will be addressed through future rulemaking activities to ensure the opportunity for public comment." 81 Fed. Reg. 68316. Given that the DFARS clause and its requirements apply to all DoD contractors, it is unclear how these liability provisions will be implemented given the narrower application of liability protections in the statutory provisions.

Key substantive changes in the Final Rule include the following:

- Adds new definitions or clarifies existing definitions for "covered defense information," "covered contractor information system," "export control," the "other" category of CDI, and "operationally critical support."

- Directs that DFARS provisions 252.204-7008 and 252.204-7012 should not be used in solicitations and contracts "solely" for commercial-off-the-shelf (COTS) items.
- Amends DFARS 252.204-7000 to clarify that fundamental research, by definition, does not involve any CDI.
- Amends DFARS 252.204-7012 to:
  - provide guidance on requests to vary from NIST SP 800-171 security controls and mandate that subcontractors notify the prime contractor (or next higher tier subcontractor) when submitting such a variance request;
  - clarify that contractors must implement safeguarding requirements on all covered contractor information systems, not just those that support the performance of work on the contract;
  - confirm that contractors are not required to implement any security requirements if an authorized representative of the DoD Chief Information Officer (CIO) has adjudicated a request to vary or determined that a security control is not applicable;
  - require contractors to ensure that external cloud service providers (CSPs) used in performance of a contract to store, process, or transmit any CDI must: (i) meet security requirements equivalent to those established by the Government for FedRAMP moderate baseline; and (ii) comply with DFARS 252.204-7012's reporting, protection, and access requirements; and
  - clarify that the clause must be flowed down to subcontractors when CDI is necessary for performance of the subcontract.
- Modifies DFARS 239.7602-1 to provide two exceptions where a contracting officer may award a contract to acquire cloud services from a CSP that has not been granted a provisional authorization by the Defense Information System Agency (DISA).

Comparison of Interim (Dec. 2015) and Final (Oct. 2016) Versions of DFARS 252.204-7012

The chart below summarizes the December 2015 and the October 2016 versions of DFARS 252.204-7012 and highlights key differences between the two.

Requirement	252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (DEC 2015)	252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (OCT 2016)	Key Differences
Applicability	The clause is prescribed for use in DoD solicitations, contracts, and certain subcontracts, including those for the acquisition of commercial items. The safeguarding requirements apply to all "covered defense information" on "covered contractor information systems that support the performance of work on the contract."	The clause is prescribed for use in DoD solicitations, contracts, and certain subcontracts except for those "solely for the acquisition of COTS items." (Per revision to DFARS 204.7304). The safeguarding requirements apply to "all covered contractor information systems."	The Final Rule clarifies that although the clause is applicable to general commercial item procurements, it is "not prescribed for use in solicitations or contracts that are solely for the acquisition of commercially available off-the-shelf (COTS) items." Additionally, the Final Rule clarifies that the "adequate security" requirement applies to all covered contractor information systems, not just CDI on information systems that support the performance of work on the contract.
Key Terminology	Defines "covered defense information" as information that: ▪ (1) is provided to the contractor by or on behalf of DoD or "collected, developed, received, used or stored" in support of contract performance; and ▪ (2) falls within one of the following four categories: (i) controlled technical information, (ii) critical information, (iii) export control information, or (iv) any additional	Defines "covered defense information" as unclassified controlled technical information or other information described in the Controlled Unclassified Information (CUI) Registry "that requires safeguarding or dissemination controls," and is either: ▪ (1) "[m]arked 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 Final Rule changes the definition of "covered defense information" to track the National Archives and Record Administration's recently published final rule on CUI, which lists 23 categories (and 83 subcategories) of information that are considered CUI. The revised definition also adds an affirmative requirement for the Government to mark or identify all CDI that is being provided to the contractor, while requiring the contractor to identify and protect all CDI that it develops during

	information marked or otherwise identified in the contract that is subject to controls imposed by law, regulation, or government-wide policy. Defines "covered contractor information systems" as a contractor-owned system that processes, stores, or transmits CDI.	the performance of the contract"; or ■ (2) "[c]ollected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract." Defines "covered contractor information systems" as an unclassified contractor-owned system that processes, stores, or transmits CDI.	the course of performance. The Final Rule clarifies that "covered contractor information systems" do not include classified systems.
Adequate Security	For covered systems operated on behalf of the U.S. Government (USG): ■ Cloud computing services are subject to the requirements in clause 252.239-7010; and ■ IT services other than cloud computing are subject to "security requirements specified elsewhere in [the contract]." For covered systems not operated on behalf of the USG, contractors must implement: ■ The security requirements in NIST SP 800-171; or	For systems operated on behalf of the USG, there is no material change in requirements. For covered systems not operated on behalf of the USG, contractors must implement: ■ The security requirements in NIST SP 800-171 unless the DoD CIO determines that one or more security requirements is non-applicable or has an "alternative, equally effective, security measure that may be implemented in its place."[1] ■ "If the Contractor intends to use	The primary security requirements remain largely the same, but the Final Rule contains notable clarifications and additions, including: ■ A requirement that external CSPs used by the contractor in the course of performance meet FedRAMP Moderate baseline and comply with DFARS 252.204-7012's reporting, safeguarding, and access requirements; ■ A clarification that contractors can submit a request to vary from NIST SP 800-171 *after* contract award, and guidance on the process of validating a previously granted

[1] The Final Rule provides guidance on the process of requesting recognition of a previously granted variance from NIST SP 800-171: "If the DoD CIO has previously adjudicated the contractor's requests indicating that a requirement is not applicable or that an alternative security measure is equally effective, a copy of that approval shall be provided to the Contracting Officer when requesting its recognition under this contract." DFARS 252.204-7012(b)(2)(ii)(C).

	▪ "Alternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement" approved in writing by the DoD CIO. The contractor is also required to apply other security measures it deems necessary to provide "adequate security."	an external [CSP] to store, process, or transmit any [CDI]," that CSP must "meet[] security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline . . . [and] compl[y] with [DFARS 252.204-7012(c)–(g)]." The contractor is also required to apply other information systems security measures it deems necessary to provide adequate security or to accommodate special circumstances (*e.g.*, medical devices) and any "individual, isolated or temporary deficiencies."	variance from NIST SP 800-171 requirements; and ▪ Greater specificity regarding circumstances in which contractors may need to adopt additional security measures (such as with medical devices) and notes that the risks can be addressed in a system security plan.
Cyber Incident Reporting	A reportable cyber incident is one that "affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support[.]" Upon discovery of such an incident, the contractor must: ▪ Conduct a review for evidence of compromise of covered defense information, including identifying compromised computers, servers, data, and user accounts. The	No material change.	N/A

	review should include an analysis of the covered information system as well as any other information systems on the contractor's network that may have been compromised; ▪ "Rapidly report" a cyber-incident to http://dibnet.dod.mil within 72 hours of discovery.		
Post-incident Investigation	Contractors must preserve and protect images of all known affected information and systems for at least 90 days from reporting to allow DoD to determine whether it will conduct a damage assessment. Contractors must provide DoD access to additional information or equipment necessary to conduct a forensic analysis. If the contractor discovers any malicious software related to the cyber incident, it "shall submit the malicious software in accordance with instructions provided by the Contracting Officer."	The Final Rule retains the requirement that contractors preserve and protect images of all known affected information and systems for at least 90 days from reporting to allow DoD to determine whether it will conduct a damage assessment. The Final Rule retains the requirement that contractors provide DoD access to additional information or equipment necessary to conduct a forensic analysis. The Final Rule provides that if the contractor discovers any malicious software related to the cyber incident, it must "submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer. Do not send the malicious software to the Contracting Officer."	Although the bulk of the post-investigation procedures and requirements remain unchanged, the Final Rule provides more explicit -- and more cautious -- guidance concerning the handling of any malicious software connected to a cyber incident, including a pointed warning not to send any identified malicious software to the contracting officer. DoD also clarified in comments preceding the Rule that DoD access to additional information or equipment "necessary to conduct a forensic analysis" is limited to that needed to "determine if DoD information was successfully exfiltrated from a network or information system of such contractor and, if so, what information was exfiltrated."
Subcontractors	Contractors are required to flow down this clause "without alteration, except to	The clause shall be included "without alteration, except to identify parties," in	The Final Rule clarifies the flow down analysis in several ways, including:

	identify parties," in all subcontracts "for operationally critical support, or for which subcontract performance will involve a covered contractor information system." Contractors must require subcontractors to rapidly report cyber incidents directly to DoD (via http://dibnet.dod.mil) and to any higher-tier contractor (including the prime).	all subcontracts for "operationally critical support, or for which subcontract performance will involve covered defense information." In assessing whether they are required to flow down this clause, contractors shall "determine if the information required for subcontractor performance retains its identity as covered defense information," and may "consult with the Contracting Officer," if necessary, in making this determination. Contractors must require subcontractors to rapidly report cyber incidents directly to DoD (via http://dibnet.dod.mil) and to provide the DoD-assigned incident report number to the prime contractor (or next higher-tier subcontractor). Contractors also must notify the prime contractor (or next higher-tier subcontractor) when submitting a request to vary from NIST SP 800-171 to the contracting officer.	▪ Clarifying the term "operationally critical support," as defined in DFARS 252.204-7012(a); ▪ Tying the flow-down requirement to the presence of "covered defense information" -- not "a covered contractor information system"; and ▪ Encouraging contractors to consult the contracting officer for guidance on when to flow down the clause. The Final Rule also modifies a subcontractor's reporting obligations in two ways: (1) removing the requirement to report a cyber incident to the prime in addition to DoD; and (2) adding a requirement to notify the prime when requesting a variance from the NIST SP 800-171 security control requirements.
Implementation	Contractors should implement NIST SP 800-171 controls as soon as possible, but no later than December 31, 2017.	No material change.	N/A
Gap Analysis & 30-Day Notice	Within 30 days of contract award, the contractor must conduct a gap analysis and notify the DoD CIO of any NIST SP 800-171 security requirements that are not implemented at the time of award.	For all contracts awarded prior to October 1, 2017, within 30 days of contract award, the contractor must conduct a gap analysis and notify the DoD CIO of any NIST SP 800-171 security requirements that are not implemented at the time of award.	The Final Rule clarifies that the gap analysis reporting requirement does not apply to awards issued after October 1, 2017.

Analysis of DoD's Comments on Key Aspects of the Final Rule for DFARS 252.204-7012

A total of 25 public comments were submitted in response to the interim rules. DoD's responses to these comments provide additional clarity in some areas but still leave a number of issues unanswered.

New and Clarified Definitions

- *Covered Defense Information (CDI):* As noted, changes the definition of CDI to any data in the CUI Registry that requires "safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government wide policies" and is: (1) "[m]arked or otherwise identified in the contract, task order, or delivery order" and provided to the contractor by or on behalf of DoD; or (2) "collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract." DFARS 252.204-7012(a). The CUI Registry is both dynamic and broad, currently including 23 categories and more than 80 subcategories of information, but the data are now at least defined in a common manner across the Government. Although the Final Rule requires DoD to either mark CDI or otherwise identify the CDI in the contract, 81 Fed. Reg. 72988, it remains to be seen how this rule will be implemented. It is possible, for instance, that such "identification" could be done so broadly (*i.e.*, all information related to performance of the contract) that it is of little practical use. DoD also modified the DFARS clause to impose on the prime contractor the requirement to determine if the information required for subcontractor performance "retains its identity" as CDI and to confer with the contracting officer "if necessary." DFARS 252.204-7012(m)(1).[2]
- *Covered Contractor System:* Clarifies that the DFARS clause applies only to unclassified contractor information systems. DFARS 252.204-7012(a).
- *Export Control:* Responds to questions from commenters about the breadth of the definition by confirming that only export controlled information, as defined in the CUI Registry, that is provided to a contractor or collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of a DoD contract needs to be protected as CDI. 81 Fed. Reg. 72988.
- *"Other" category of CDI:* Notes that the security requirements of the DFARS clause set a "baseline" standard and that, as noted in the CUI Registry, certain data may be subject to additional protections. 81 Fed. Reg. 72989. Thus, for example, contractors may be subject to additional safeguarding requirements under HIPAA or the Health Information Technology for Economic and Clinical Health (HITECH) Act if they have personal health information of service members on their covered contractor information systems.
- *Operationally Critical Information:* Acknowledges that because operationally critical information is not included as a category of data in the CUI Registry, it can no longer be designated as CDI. 81 Fed. Reg. 72988. Nonetheless, section 1632 of the FY 2015

[2] The Final Rule also revises DFARS 252.204-7000 to clarify that contracts for "fundamental research" do not involve CDI. 81 Fed. Reg. 72987.

NDAA and the DFARS clause require contractors and subcontractors to report cyber incidents that result in an actual or potentially adverse effect on their ability to provide operationally critical support. DFARS 252.204-7012(m)(1). Thus, "operationally critical support is an 'activity'—not an information type—performed by the contractor or subcontractor." 81 Fed. Reg. 72989. DoD also notes that operationally critical requirements "must be marked or otherwise identified in the contract, task order, or delivery order." *Id*. This would seem to impose a requirement on DoD to identify these obligations before performance begins.

30-Day Notification and Alternative Controls

In the commentary accompanying the Final Rule, DoD provided additional guidance on securing permission to implement an alternative to a NIST SP 800-171 security requirement. *First,* prior to award, and consistent with DFARS 252.204-7008(c), an offeror may include "a written explanation in their proposal describing the reasons why a security requirement is not applicable, or how alternative, but equally effective, security measures can compensate for the inability to satisfy a particular requirement." The contracting officer will refer the proposed variance to the DoD CIO, who then will approve or reject the proposal (or request additional information). According to DoD, the typical timeframe for a response by the DoD CIO is within five business days. 81 Fed. Reg. 72990.

Second, the Final Rule also contains a new provision that permits a contractor to seek approval for a variance *after* contract award. 81 Fed. Reg. 72990. Under DFARS 252.204-7012(b)(2)(ii)(B), a contractor may submit to the contracting officer a written request for a variance, which the contracting officer will then refer to the DoD CIO for ultimate adjudication. When such a variance is sought by a subcontractor, the subcontractor must "[n]otify the prime contractor (or the next higher-tier subcontractor)" when submitting the request, but the Final Rule does not address the content, format, or detail required in such a notice.

DoD also provided further guidance about the requirement that all contractors and covered subcontractors notify the DoD CIO, within 30 days of contract (or subcontract) award, of any applicable security requirements that are not implemented. DoD's commentary explains that this notification must "only identify the security requirement(s) . . . that is/are not implemented," and "[n]o additional information is required." 81 Fed. Reg. 72991. Additionally, the commentary explains that covered subcontractors are <u>not</u> required to submit their 30-day notification to the prime contractor in addition to the DoD CIO, and that any concern about "[b]ypassing the prime is a matter to be addressed between the prime and the subcontractor." *Id*. However, the DFARS clause is amended to clarify that the prime must require subcontractors to notify it (or the next higher-tier subcontractor) of any requests for variance submitted directly to the contracting officer. DFARS 252.204-7012(m)(2)(i). Notably, the clause does not indicate if the subcontractor needs to provide the substance of the notice or just the fact that a request was made.

Incident Reporting and Damage Assessment

A number of commenters on the interim rule expressed concern that the 72-hour reporting requirement is unrealistic and unduly burdensome, especially given the requirement to report "potentially adverse effects" on an information system even absent an actual compromise of CDI. 81 Fed. Reg. 72991. DoD was largely unmoved by these arguments, reemphasizing the need for rapid reporting and reiterating its commitment to the 72-hour requirement. However, in a tacit acknowledgement of the burden that this requirement imposes on contractors, DoD

stated that a contractor "should report whatever information is available" within 72 hours, even if it "does not have all the information required on the Incident Collection Form (ICF)." *Id*. The commentary also noted that a contractor can supplement an initial ICF by "submit[ting] a follow-on report with [any] added information" when it becomes available. *Id*. Subcontractors are only required to provide primes with the ICF number of any cyber incident reported to DoD.

Access to Contractor Information and Systems

Multiple parties submitted comments on the interim rule expressing concern that the rule did not appropriately limit the Government's access to contractor systems and failed to adequately protect sensitive contractor data. In response, DoD stated that access to contractor information is essential to investigating and assessing any potential cyber incident, and that this principle undergirds the fundamental requirement that contractors provide the Government with "access to additional information and equipment that is necessary to conduct a forensic analysis." DFARS 252.204-7012(f). However, the commentary also recognized that, consistent with requirements in 10 U.S.C. sections 391 and 393, DoD's access is limited to "determin[ing] if DoD information was successfully exfiltrated from a network or information system of such contractor and, if so, what information was exfiltrated." 81 Fed. Reg. 72991.

Protection and Use of Contractor Proprietary Information

Citing the potential exposure of proprietary information that they may be required to report to DoD in the event of a cyber incident, a number of commenters recommended that the Final Rule specifically address how DoD would safeguard any contractor data provided. In the Final Rule, DoD declined to provide such specifics. Instead, it simply stated that "DoD protects against unauthorized use or release of cyber incident reporting information" and "complies with 10 U.S.C. 391 and 393," which provide, in general terms, for the protection of certain commercial or financial information (*e.g.*, trade secrets) and personally identifiable information. DoD indicated, however, that contractors bear some responsibility for the protection of their own information, stating that contractors "should identify and mark attributional/proprietary information and personal information to assist DoD in protecting this information." 81 Fed. Reg. 72992. However, DoD did not address concerns raised as to marking information when contractors are preserving images with large amounts of data, nor did DoD address concerns raised about compliance with foreign data privacy laws.

Relatedly, several commenters also raised questions about third-party support contractors gaining access to sensitive information that might be reported following a cyber incident, and urged DoD to adopt additional procedures to guarantee the nondisclosure of such information. DoD responded that existing rules already "subject[] support service contractors . . . to restrictions on use and disclosure obligations." 81 Fed. Reg. 72992; *see also* DFARS 252.304-7009.

Liability Protections

DoD also received at least one comment recommending that the Final Rule integrate the liability protections set forth in section 1641 of the FY 2016 NDAA, which specifies liability protections for cleared defense contractors and operationally critical contractors when reporting cyber incidents. In response, DoD indicated that it already was working to implement these statutory protections, citing open DFARS Case 2016-D025, Liability Protections When Reporting Cyber Incidents. 81 Fed. Reg. 72993. This DFARS case was opened in April 2016, and an internal

report concerning text of a proposed rule is due on October 26, 2016. Given this ongoing activity, contractors should expect to see further rulemaking on this subject in the near future.

Subcontractor Flowdowns

A number of commenters requested clarification about when and how to flow down the requirements of the clause to subcontractors. In response, DoD amended the Final Rule in several ways. Most notably, DoD clarified that DFARS 252.204-7012 must be flowed down where a subcontractor provides "operationally critical support" or where subcontract performance will involve CDI. 81 Fed. Reg. 72993. The Final Rule included new language encouraging contractors to consult the contracting officer for guidance on when to flow down the clause. Finally, commentary accompanying the Final Rule reinforced the rigid requirement to include DFARS 252.204-7012 in any covered subcontract. Specifically, DoD stated that "[f]lowdown is a requirement of the terms of the contract with the Government, which should be enforced by the prime contractor," and that CDI "shall not be on [the] information system" of any subcontractor that does not agree to comply with DFARS 252.204-7012. *Id.*

Provision of Malicious Software

As noted above, the Final Rule was revised during the comment period to provide more explicit guidance concerning the handling of any malicious software connected to a cyber incident. The Final Rule specifies that if a contractor discovers malicious software related to a cyber incident, it must "submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer." Additionally, the Final Rule includes a pointed admonition not to send any identified malicious software to the contracting officer.

The Final Rule Clarifies Requirements and Procedures When Contracting for Cloud Computing Services

Overview

In addition to the changes noted above, DoD also clarified a number of issues associated with contracting for cloud computing services. In particular, DoD addressed comments relating to access to Government data and contractor facilities, when DFARS 252.204-7012 (contractor internal systems) applies versus 252.239-7010 (cloud computing systems), cyber incident reporting requirements for cloud service providers (CSPs), and exceptions to the requirement that CSPs have provisional FedRAMP authorization.

Government Access

At least one commenter tried to distinguish CSPs from other contractors, suggesting that third-party access to data centers for infrastructure-as-a-service (IaaS) providers should be limited to accredited FedRAMP third-party assessment organizations and law enforcement activities. 81 Fed. Reg. 72993. In response, DoD indicated that the Government is entitled access to "all Government data and Government related data, access to contractor personnel involved in performance of the contract, and physical access to any Contractor facility with Government data" for purposes of audits, investigations, and inspections "as authorized by law or regulation." *Id.* As addressed above, the provisions of 10 U.S.C. sections 391 and 393 permit DoD access to "determine if DoD information was successfully exfiltrated from a network or information system of such contractor and, if so, what information was exfiltrated." 81 Fed. Reg. 72992.

Applicability of DFARS 252.204-7012 to Cloud Computing Services

The Final Rule provides some clarifications on how DFARS 252.204-7012 applies to cloud computing solutions. When cloud computing services are being operated "on behalf" of the Government, CSPs are required to comply with the requirements of the Cloud Computing Security Requirements Guide (SRG), also known as FedRAMP+. When cloud computing services are not being operated "on behalf" of the Government, DoD modified DFARS 252.204-7012 to provide that these CSPs must meet the FedRAMP Moderate baseline requirements and otherwise comply with the "cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment" in the 7012 clause. *See* DFARS 252.204-7012(b)(2)(ii)(D).

DoD also clarified that the prime contractor is required to include in its gap analysis any security requirements in NIST SP 800-171 not implemented by an external CSP performing this function.[3] 81 Fed. Reg. 72994. Finally, DoD noted that the requirement to comply with DFARS 252.204-7012 could apply to ancillary cloud services such as cloud migration and eDiscovery if CDI was involved. *Id*.

Cyber Incident Reporting for CSPs

In its comments preceding the Final Rule, DoD clarified that CSPs are required to report cyber incidents related to CDI to the DIBNet web portal in addition to any independent reporting requirements that exist under FedRAMP or the SRG. 81 Fed. Reg. 72994. DoD rejected claims by commenters that if a contractor is using an external FedRAMP-compliant CSP to store, process, or transmit CDI, the CSP needs only to report cyber incidents to the prime or higher-tier contractor. 81 Fed. Reg. 72995.

DoD also rejected a suggestion that CSPs should only be responsible for reporting incidents that "result in an actual, or reasonably suspected, unauthorized disclosure of customer data." 81 Fed. Reg. 72995. DoD noted that "[c]yber incidents that impact the environment could have an impact on the CSP's security accreditation and DoD data, which is the reason that all incidents that are on shared services and infrastructure should be reported." *Id.* Similarly, DoD stated that to the extent these requirements conflict with standard commercial practices, the CSP is responsible for modifying those commercial terms and conditions.

Finally, in response to comments that IaaS providers have no insight into the nature of the data being stored or processed, DoD asserted that "any breach would be considered a cyber incident given the potential impact it could have on information or the information system." *Id.* Moreover, DoD noted that "[b]ecause the IaaS providers deliver shared services, any cyber-incident on the shared infrastructure and services would be the responsibility of the IaaS provider and they are obligated to report those incidents." *Id*.

Exceptions to Requirement that CSPs Have Provisional FedRAMP Authorization

In general, contracting officers can only award contracts to CSPs that have been granted provisional authorization by the Defense Information Systems Agency, at the appropriate level in accordance with the SRG. The Final Rule modified DFARS 239.7602-1 to allow for two

---

[3] Note that this is different from the requirement for "subcontractors," who are required to submit variance requests and 30-day gap analyses directly to DoD CIOs.

exceptions to this requirement: (1) if the DoD CIO waives the requirement, or (2) if the cloud computing service requirement is for a private, on-premises version that will be provided from U.S. Government facilities. Under this second circumstance, the CSP must obtain a provisional authorization prior to operational use.

Conclusion

The Final Rule incorporates years of comments and experience by DoD and its contractors. Although the Rule clarified some areas of concern, implementation challenges still remain. Contractors will need to review their internal processes and contract terms with subcontractors to confirm compliance and ensure that they are prepared to prevent and, if necessary, respond to a cyber incident.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Government Contracts practice:

Susan Cassidy	+1 202 662 5348	scassidy@cov.com
Michael Wagner	+1 202 662 5496	mwagner@cov.com
Julia Lippman	+1 202 662 5714	jlippman@cov.com