WILMERHALE

Department of Defense Issues Final Version of Key Cybersecurity Rule

NOVEMBER 1, 2016

On October 21, 2016, the Department of Defense (DoD) issued its final rule on *Network Penetration Reporting and Contracting for Cloud Services*,[1] amending an interim version issued on August 26, 2015, and revised on December 30, 2015.[2] While the final rule narrowed the scope of parts of the rule's coverage, the rule remains expansive in scope and prescriptive in application, including mandatory cybersecurity-related contract clauses to be included in DoD contracts and subcontracts.[3]

Revised Definition of Covered Defense Information

The final version of the rule revises the definition of "covered defense information" (CDI), a term central to the rule's scope, in order to align it more closely with the rule on controlled unclassified information (CUI) recently issued by the National Archives and Records Administration.[4]

DoD revised the CDI definition in two key respects. *First*, the prior version of the rule covered information "[p]rovided to the contractor by or on behalf of DoD in connection with the performance of the contract," without any marking requirement. Now, information provided by or on behalf of DoD will constitute CDI only if it is marked or otherwise identified in the contract (though contractors will still be responsible for identifying CDI that they collect, develop, receive, etc.).

Second, under the prior version, information constituted CDI if it was either controlled technical information, "critical information (operations security)," or export controlled information, all as defined by the rule, or "[a]ny other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government[-]wide policies (e.g., privacy, proprietary business information)." The new definition applies to categories of information identified in the CUI Registry, which *does not* include "critical information (operation security)," but does include controlled technical information and export controlled information, as well as 20 other categories and numerous subcategories of information, ranging from critical infrastructure information to information systems vulnerability information, intelligence information, private information, or proprietary business information.

As such, while the revised rule puts the onus on the government to identify covered information it provides to contractors, contractors continue to be obligated to identify CDI they generate or otherwise possess, with more categories of information expressly constituting CDI.[5]

Other Key Revisions to the Rule

Other significant changes in the final version of the rule include:

- ***Exception for Contracts for COTS Items.*** While the interim rule required the contract clauses to be included in all contracts, including for commercial items, the final rule includes an exception for contracts solely for commercially available off-the-shelf (COTS) items.[6] While this will exclude a number of prime contractors, the final rule notably does not appear to extend this exception to subcontractor flow-down requirements. Thus, while prime contracts exclusively for COTS items will be exempt from the scope of the rule, prime non-COTS contractors appear to continue to be required to flow-down the contract terms to all subcontractors, even those providing COTS items, if the subcontractor will be collecting, developing, receiving, transmitting, using, or storing CDI in support of the performance of the contract (or providing "operationally critical support"). In light of the data categories covered by the CUI Registry, the rule will continue to significantly affect companies throughout the DoD supply chain.
- ***Clarifying Process for Deviating from NIST SP 800-171.*** In addition to maintaining the "grace period" for compliance with NIST SP 800-171 included in the December 2015 revision to the rule,[7] the final rule allows contractors to implement "[a]lternative, but equally effective, security measures," which, under the interim rule, had to be accepted in writing by an authorized representative of the DoD Chief Information Officer (CIO). The final rule revises this language and clarifies how deviations can be approved. Specifically, the final rule provides that a contractor submit such requests in writing to the Contracting Officer (CO), for consideration by the DoD CIO.[8] When the 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 the approval shall be sent to the CO.[9] The preamble to the final rule states that the DoD CIO will typically respond to such requests within five business days.[10]
- ***Assistance with Flow-Down Determinations.*** Under the final rule, contractors may consult with the CO to determine if the information required for subcontract performance retains its identity as CDI such that flow-down of the contract clauses is required.[11]
- ***Clarifying Subcontractor Reporting.*** The final rule clarifies the processes for two subcontractor reporting requirements. *First*, if subcontractors submit a request to vary from a NIST 800-171 requirement, they are required to notify the prime contractor (or next higher-tier subcontractor).[12] *Second*, when subcontractors notify DoD of a cyber incident, they are only required to provide the prime contractor (or next higher-tier subcontractor) with an incident report number automatically assigned by DoD.[13]

The Cloud

The final rule also includes a number of changes specifically regarding cloud computing services,

either by contractors or when such services are acquired by DoD. The most significant changes include:

- ***Exceptions for Cloud Computing Provisional Authorization.*** While the rule generally prohibits COs from awarding a contract for cloud computing services to cloud service providers (CSPs) unless the CSP has been granted "provisional authorization" by the Defense Information Systems Agency,[14] the rule adds exceptions when (1) this requirement is waived by the DoD CIO,[15] or (2) the cloud computing service is for a private, on-premises version that will be provided from government facilities, in which case the provisional authorization must be obtained prior to operational use.[16]
- ***Requirements for Contractor Cloud Use.*** The final rule requires contractors that are using external CSPs to store, process, or transmit CDI in performance of a contract to "require and ensure that the [CSP] meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline . . . and that the [CSP] provider complies with requirements" included in the rule's non-cloud contract clause related to cyber incident reporting, submission of identified malicious software, media preservation and protection, DoD access to information and equipment for forensic analysis, and cooperation with DoD cyber incident damage assessments.[17]

Looking Forward

- ***Different Versions of the Clauses.*** In the preamble to the final rule, DoD notes that "[s]everal respondents commented that the new rule could leave contractors subject to different security standards depending on which version of [the "safeguarding information" contract] clause . . . appears in their contracts and subcontracts," and some even suggested that DoD issue a "block change" to all contracts that included the August 2015 clause to adopt the December 2015 clause.[18] (This problem is now further exacerbated by the changes included in the final rule.) DoD responded that mass modifications were not appropriate for this type of non-administrative change, but noted that "[t]here is nothing that precludes a [CO] from considering a modification of the contract upon request of the contractor."[19] As such, contractors wishing to ensure consistent security-related clauses across contracts may wish to approach COs to discuss contract modifications.
- ***Rules on Liability Protection.*** The FY 2016 National Defense Authorization Act added new liability protection for information-sharing between defense contractors and DoD.[20] The preamble to the final rule notes that a separate Defense Federal Acquisition Regulations Supplement case was opened in April 2016 to implement these protections.[21]

---

[1] 81 Fed. Reg. 72986 (Oct. 21, 2016), available here.

[2] 80 Fed. Reg. 51739 (Aug. 26, 2015), available here; 80 Fed. Reg. 81472 (Dec. 30, 2015), available here. For more information on the earlier versions of the rule, see the WilmerHale client alert available here.

[3] The final rule includes revisions to DFARS clauses 252.204-7000, 252.204-7009, 252.204-7012, 252.239-7009, and 252.239-7010.

[4] As revised, CDI is now defined as “unclassified controlled technical information or other information (as described in the Controlled Unclassified Information (CUI) Registry [available here] 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.” 48 CFR 204.7301. “Controlled technical information” is defined in the CUI Registry as "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 is to be marked with one of the distribution statements B through F, in accordance with Department of Defense Instruction 5230.24, 'Distribution Statements of Technical Documents.' The term does not include information that is lawfully publicly available without restrictions. 'Technical Information' means technical data or computer software, as those terms are defined in Defense Federal Acquisition Regulation Supplement clause 252.227-7013, 'Rights in Technical Data - Noncommercial Items' (48 CFR 252.227-7013). Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.” CUI Registry.

[5] While these other categories of information arguably fell under the catch-all in the prior version of the rule (“[a]ny other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government[-]wide policies (e.g., privacy, proprietary business information)”), the fact that these categories are now expressly referenced leaves little room for interpretation as to the scope of information covered.

[6] 48 CFR 204.7304.

[7] Pursuant to the rule, where compliance with NIST SP 800-171 is required under the rule by December 31, 2017, contractors not in full compliance with the rule are required to report to the DoD CIO, within 30 days of award, which requirements they have not implemented. *Id*. 252.204-7012(b)(2)(ii). The preamble to the rule clarifies, consistent with guidance provided during the DoD industry day in fall 2015, that “[t]he list need only identify the security requirement(s) (e.g., NIST SP 800-171 security requirement 3.1.1) that is/are not implemented. No additional information is required.” 81 Fed. Reg. 72991. Furthermore, “[n]othing precludes the contractor from providing a corporate-wide update to the status of requirements not implemented on a periodic basis, assuming it meets the requirements of the clause.” *Id*.

[8] 48 CFR 252.204-7012(b)(2)(ii)(B).

[9] *Id*. 252.204-7012(b)(2)(ii)(C).

[10] 81 Fed. Reg. 72990.

[11] 48 CFR 252.204–7012(m).

[12] *Id*. 252.204-7012(m)(2)(i). The preamble to the rule further clarifies that, to the extent a subcontractor is not in compliance with NIST SP 800-171 prior to December 31, 2017, it is required to report to the DoD CIO within 30 days of the prime contractor's award to the subcontractor. Whether

this notification should bypass the prime contractor or not is “a matter to be addressed between the prime and the subcontractor.” 81 Fed. Reg. 72991.

[13] 48 CFR 252.204-7012(m)(2)(ii). The preamble notes, however, that requirements for subcontractors to provide more information to prime contractors can be addressed between the parties. 81 Fed. Reg. 72993.

[14] 48 CFR 239.7602-1(b)(1).

[15] *Id*. 239.7602-1(b)(2)(i).

[16] *Id*. 239.7602-1(b)(2)(ii).

[17] *Id*. 252.204-7012(b)(2)(ii)(D)

[18] 81 Fed. Reg. 72989.

[19] *Id*.

[20] *See* National Defense Authorization Act for Fiscal Year 2016, Pub. L. No. 114-92, Section 1641(a).

[21] 81 Fed. Reg. 72993 (referencing DFARS Case 2016-D025, Liability Protections when Reporting Cyber Incidents).

Authors

Benjamin A. Powell

PARTNER

Co-Chair, Cybersecurity and Privacy Practice

Co-Chair, Artificial Intelligence Practice

benjamin.powell@wilmerhale.com

+1 202 663 6770

Barry J. Hurewitz

PARTNER

barry.hurewitz@wilmerhale.com

+1 202 663 6089

Stephen W. Preston

PARTNER

Chair, Defense, National Security and Government Contracts Practice

stephen.preston@wilmerhale.com

+1 202 663 6900

Jason C. Chipman

PARTNER

jason.chipman@wilmerhale.com

+1 202 663 6195