LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Government Contracts Practice

December 21, 2017 | Number 2262

New DoD Cybersecurity Requirements Go Into Effect

The DFARS final rule requires contractors to safeguard information systems and imposes investigation and reporting requirements in the case of cyber incidents.

As of December 31, 2017, many United States government contractors face a new compliance requirement involving cybersecurity. This requirement will govern most new Department of Defense (DoD) contracts and, significantly, will also apply to many current DoD contracts that include the applicable standard contract clause.

On October 21, 2016, DoD issued a final rule, Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012 (DFARS Rule), which is intended to address "enhanced safeguarding for certain sensitive DoD information."[1] The DFARS Rule was, in general, effective immediately, and imposed safeguarding and cyber incident reporting obligations on contractors who have contracts with DoD, and whose information systems process, store, or transmit "covered defense information" (CDI).[2] However, one of the major changes implemented through the DFARS Rule — requiring contractors to comply with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 — goes into effect at the end of this month.

The DFARS Rule imposes on contractors the requirement to have "adequate security" on all covered contractor information systems,[3] and applies to all solicitations and contracts — including those for commercial items (other than commercial off-the-shelf (COTS) items).[4] In particular, the DFARS Rule focuses on protecting CDI — which it defines broadly.[5] Moreover, CDI includes both information that the government marked as CDI, and information "collected, developed, received, transmitted, used or stored by or on behalf of the contractor in support of the performance of the contract."[6] For contractors subject to both the DFARS Rule and the Federal Acquisition Regulation (FAR) cybersecurity regulation — which was promulgated in May 2016, FAR 52.204-21 (FAR Rule) — the DFARS Rule likely imposes more extensive security controls and requirements than the FAR Rule does. Specifically, the DFARS Rule requires the investigation and reporting of cyber breaches that are not included in the FAR Rule.

Significantly, the DFARS clause defines the basic security requirements a defense contractor must implement and maintain. As of December 31, 2017, a defense contractor generally must implement the security requirements in the version of NIST SP 800-171[7] then in effect at the time of the solicitation. However, cloud service providers (CSP) using a cloud solution to store data on DoD's behalf — which have to comply with DFARS 252.239-7010, Cloud Computing Services[8] — are exempt from this change.

The NIST SP 800-171 security requirements[9] were developed for use on contractors' internal systems and should enable contractors to comply with the requirements using their existing systems and practices — rather than forcing contractors to build a new system and develop practices from scratch in order to be in compliance.[10] DoD's guidance regarding these new requirements is that contractors who were in

compliance with the previous security requirements can comply with the NIST SP 800-171 requirements "by policy/process changes or adjusting the configuration of existing IT."[11]

Compliance with the New DFARS Rule

In light of the new rules implementation, contractors need to revisit the DFARS Rule's requirements and ensure compliance. Since the DFARS Rule was implemented, there has been additional guidance on these requirements that contractors should also take into consideration.

On June 23, 2017, DoD held an Industry Day during which it addressed cybersecurity challenges and went over the new DFARS rules. On September 21, 2017, the Director of the Defense Pricing/Defense Procurement Acquisition Policy (DPAP) issued guidance to DoD acquisition personnel in anticipation of the December 31, 2017 deadline for contractors to be in compliance with the DFARS Rule.[12]

On November 28, 2017, NIST released a draft SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information with the goal of better educating contractors, third parties, and government agencies on SP 800-171's requirements.[13] This guidance outlined ways in which a contractor can come into compliance with the requirements.

On December 1, 2017, DoD's Office of Defense Procurement and Acquisition Policy updated its Procedures, Guidance, and Information (PGI) with guidance regarding DFARS 252.204-7012.[14] Though the PGI is internal guidance for DoD contracting officers, the PGI provides contractors with insight into how DoD interprets and plans to apply the DFARS Rule. Based on the DFARS Rule and this updated guidance, contractors should take the following steps prior to the December 31, 2017 implementation deadline:

- Examine the requirements of the DFARS Rule to determine which requirements the contractor is in compliance with and which ones it still needs to meet
- Assess compliance with NIST SP 800-171. In particular, while NIST's November 28 draft SP 800-171A remains available for public comment until January 15, 2017[15], contractors should consult this guidance, among other resources, when evaluating compliance with NIST SP 800-171.
- Assess whether the contractor would prefer to submit a written request to the contracting officer to implement an "[a]lternative but equally effective, security measure"[16] rather than comply with NIST SP 800-171.
- Determine if additional requirements apply. For example, the preamble to the DFARS Rule explained that for internal DoD information systems the security requirements from CNSSI 1253, based on NIST SP 800-53, apply.[17]
- Implement other security measures that a contractor deems necessary, in addition to either complying with NIST SP 800-171 or using "equally effective security measures"
- Make applicable changes to policies and information technology (IT) configuration, and add software and hardware, to support increased protection of covered defense information, as needed
- Develop a System Security Plan (SSP) to document implementation of NIST SP 800—171.[18] NIST SP 800-171, revision 1 — which was finalized in December 2016 – added the SSP as a specific

requirement. However, contractors should note that DoD recently issued guidance that provides that "[e]ven without Revision 1 of the NIST SP 800-171 — the contractor may still document implementation of the security requirements with a system security plan."[19]

- If the contractor's request to use an "alternative but equally effective, security measure" is favourably adjudicated, include DoD's assessment to this effect in the contractor's SSP[20]

- Develop a plan of action and milestones to implement the requirements and document any "plans of action to describe how and when any unimplemented security requirements will be met, how any planned mitigations will be implemented, and how and when [a contractor] will correct deficiencies and reduce or eliminate vulnerabilities in the systems."[21] A contractor can document its SSP and plans of action as separate or combined documents and in any chosen format.

- Retain copies of the SSP and any associated plans of action in the event the responsible federal agency or contracting officer requests these documents, as they demonstrate the contractor's implementation or planned implementation of the security requirements.[22] DoD has indicated that DoD or the responsible federal agency may consider an offeror's implementation of NIST SP 800-171 in the source selection process in a few key ways. Because this could include establishing the implementation of NIST SP 800-171 as a separate technical evaluation factor, contractors will want to retain all applicable documents to show their compliance with NIST SP 800-171.[23]

- Mark any SSPs or plans of action as "Confidential" or "Proprietary," as needed, to protect a company's sensitive information that would otherwise potentially be incorporated as part of the contract and potentially be available to the public.[24]

Contractors should note that, by submitting a proposal to a solicitation that contains the DFARS Rule after December 31, 2017, they are representing that they are in compliance with the requirements.[25] While the regime is a self-certification process and DoD will not be independently certifying that a contractor is compliant with the security requirements,[26] contractors must still be prepared for later audits or government reviews.

Prime Contractors Must Flowdown the DFARS Rule, When Applicable

In addition to their own compliance, contractors are also responsible for ensuring that their subcontractors are aware of these requirements. In the final DFARS Rule, DoD clarified that the DFARS Rule directs that DFARS 252.204-7012 be flowed down to all subcontracts for "operationally critical support, or for which subcontract performance will involve 'covered defense information.'"[27] At DoD's June 23, 2017 Industry Day, DoD recommended that a prime contractor should minimize the flowdown of covered defense information to subcontractors unless the information is required for subcontractor performance. Additionally, if a subcontractor does not agree to comply with the terms of the DFARS Rule for any reason, the prime contractor should not share covered defense information with the subcontractor or otherwise allow the information to reside on the subcontractor's system(s).[28] If a defense contractor is unsure about when it needs to flowdown this requirement to subcontractors, the DFARS Rule encourages contractors to consult the contracting officer.[29]

Conclusion and Outlook

Some government contractors are already in compliance with the DFARS Rule. However, many government contractors that are — or might be — in non-compliance are still scrambling to review the requirements and implement adequate safeguards to ensure compliance.

Contractors should take steps to ensure compliance with the new rules, as they could face a variety of consequences if they are not in compliance, including: loss of a contract award, a bid protest, a breach of a contract allegation, liability under the False Claims Act, default termination, negative past performance reviews, and suspension and/or debarment.

Finally, with continued changes to the cybersecurity requirements expected, contractors need to continue to monitor and develop adequate safeguards on an ongoing basis. Latham will continue to provide updates on related developments in this fast-evolving climate.

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Jennifer C. Archie
jennifer.archie@lw.com
+1.202.637.2205
Washington, D.C.

Serrin A. Turner
serrin.turner@lw.com
+1.212.906.1330
New York, N.Y.

Kyle R. Jefcoat
kyle.jefcoat@lw.com
+1.202.637.2152
Washington, D.C.

Dean W. Baxtresser
dean.baxtresser@lw.com
+1.202.637.2110
Washington, D.C.

Morgan L. Maddoux
morgan.maddoux@lw.com
+1.202.637.3318
Washington, D.C.

You Might Also Be Interested In

We've Got Washington Covered

Call for Cybersecurity Guidelines in International Arbitration

New Executive Order on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"

Ransomware Attacks: When Is Notification Required?

Endnotes

[1] 81 Fed. Reg. at 30440.

[2] *See* 81 Fed. Reg. 72986 (Oct. 21, 2016). "Covered defense information" ("CDI") is defined as "unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html, 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.

[3] DFARS 252.204-7012 defines the term "covered contractor information system" as "unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.

[4] *See* DFARS 252.204-7012; *see also* Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018), Frequently Asked Questions (FAQs) Regarding the Implementation of DFARS Subpart 204.73 and PGI Subpart 204.73 and DFARS Subpart 239.76 and PGI Subpart 239.76 ("DFARS FAQs") (Jan. 27, 2017), *available at* http://www.acq.osd.mil/dpap/pdi/docs/FAQs_Network_Penetration_Reporting_and_Contracting_for_Cloud_Services_(01-27-2017).pdf.

[5] Contractors should note that the CUI Registry contains a broad range of categories and subcategories of information that is now considered CDI. For example, the CUI Registry includes a "Privacy" as a category with several subcategories, including "Health Information" and "Student Records," which are two types of information one would not traditionally view as covered defense information.

[6] DFARS 252.204-7012(a).

[7] NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" is available at http://dx.doi.org/10.6028/NIST.SP.800-171.

[8] DoD has also provided additional guidance on when DFARS 252.239-7010 may apply: "DFARS clause 252.239-7010 is included in contracts for information technology services and applies when a contractor is using cloud computing to provide information technology services to DoD in the performance of the contract. It does not apply to cloud computing data centers operated as an extension of a contractor's internal IT system. DFARS clause 252.204-7012 is included in all DoD contracts (except those solely for COTS items) and a reference to DFARS clause 252.239-7010 is provided at paragraph (b)(1)(i) to notify contractors of the security requirements that must be followed when DoD is contracting for cloud services." *Id.* at 26.

[9] *See* DFARS FAQs at 12.

[10] *See id.*

[11] *Id.* at 13. One addition to the security requirements that could require additional software or hardware is the implementation of multifactor authentication, which DoD discusses in more depth in its FAQs. DoD also sets forth a reasonable approach for how companies unfamiliar with or new to the requirements can evaluate and come into compliance.

[12] Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, Office of the Under Secretary of Defense, September 21, 2017, available at https://www.acq.osd.mil/dpap/policy/policyvault/USA002829-17-DPAP.pdf.

[13] Ron Ross, *et al.*, Assessing Security Requirements for Controlled Unclassified Information, Draft NIST Special Publication 800-171A (November 2017), available at https://csrc.nist.gov/CSRC/media/Publications/sp/800-171a/draft/sp800-171A-draft.pdf.

[14] *See* DoD's office of Defense Procurement and Acquisition Policy Procedures, Guidance, and Information ("PGI") (revised Dec. 1, 2017), available at https://www.acq.osd.mil/dpap/dars/pgi/pgi_htm/current/PGI204_73.htm.

[15] *Id.* at i.

[16] DFARs 252.204-7012(b)(2)(i)-(ii).

[17] *See* DFARS FAQs at 11.

[18] Cybersecurity Challenges: Protecting DoD's Unclassified Information, DoD Industry Information Day, June 23, 2017, at 61, available at http://dodcio.defense.gov/Portals/0/Documents/Public%20Meeting%20-%20Jun%2023%202017%20Final.pdf?ver=2017-06-25-022504-940.

[19] Note Regarding NIST Special Publication 800-171, Revision 1, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: Security Requirement 3.12.4, System Security Plan, available at http://dodprocurementtoolbox.com/cms/sites/default/files/resources/2017-11/Note%20Regarding%20NIST%20Special%20Publication%20800-171%20System%20Security%20Plan.pdf.

[20] *Id.*

[21] *See* NIST SP 800-171, Security Requirement 3.12.2; *see also* Cybersecurity Challenges: Protecting DoD's Unclassified Information, DoD Industry Information Day, June 23, 2017, at 61, available at http://dodcio.defense.gov/Portals/0/Documents/Public%20Meeting%20-%20Jun%2023%202017%20Final.pdf?ver=2017-06-25-022504-940.

[22] Cybersecurity Challenges: Protecting DoD's Unclassified Information, DoD Industry Information Day, June 23, 2017, at 61, available at http://dodcio.defense.gov/Portals/0/Documents/Public%20Meeting%20-%20Jun%2023%202017%20Final.pdf?ver=2017-06-25-022504-940.

[23] *Id.* at 62.

[24] Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, Office of the Under Secretary of Defense, September 21, 2017, available at https://www.acq.osd.mil/dpap/policy/policyvault/USA002829-17-DPAP.pdf.

[25] *Id.*

[26] Cybersecurity Challenges: Protecting DoD's Unclassified Information, DoD Industry Information Day, June 23, 2017, at 60, available at http://dodcio.defense.gov/Portals/0/Documents/Public%20Meeting%20-%20Jun%2023%202017%20Final.pdf?ver=2017-06-25-022504-940.

[27] 252.204-7012(m)(1).

[28] Cybersecurity Challenges: Protecting DoD's Unclassified Information, DoD Industry Information Day, June 23, 2017, available at http://dodcio.defense.gov/Portals/0/Documents/Public%20Meeting%20-%20Jun%2023%202017%20Final.pdf?ver=2017-06-25-022504-940.

[29] *Id.*