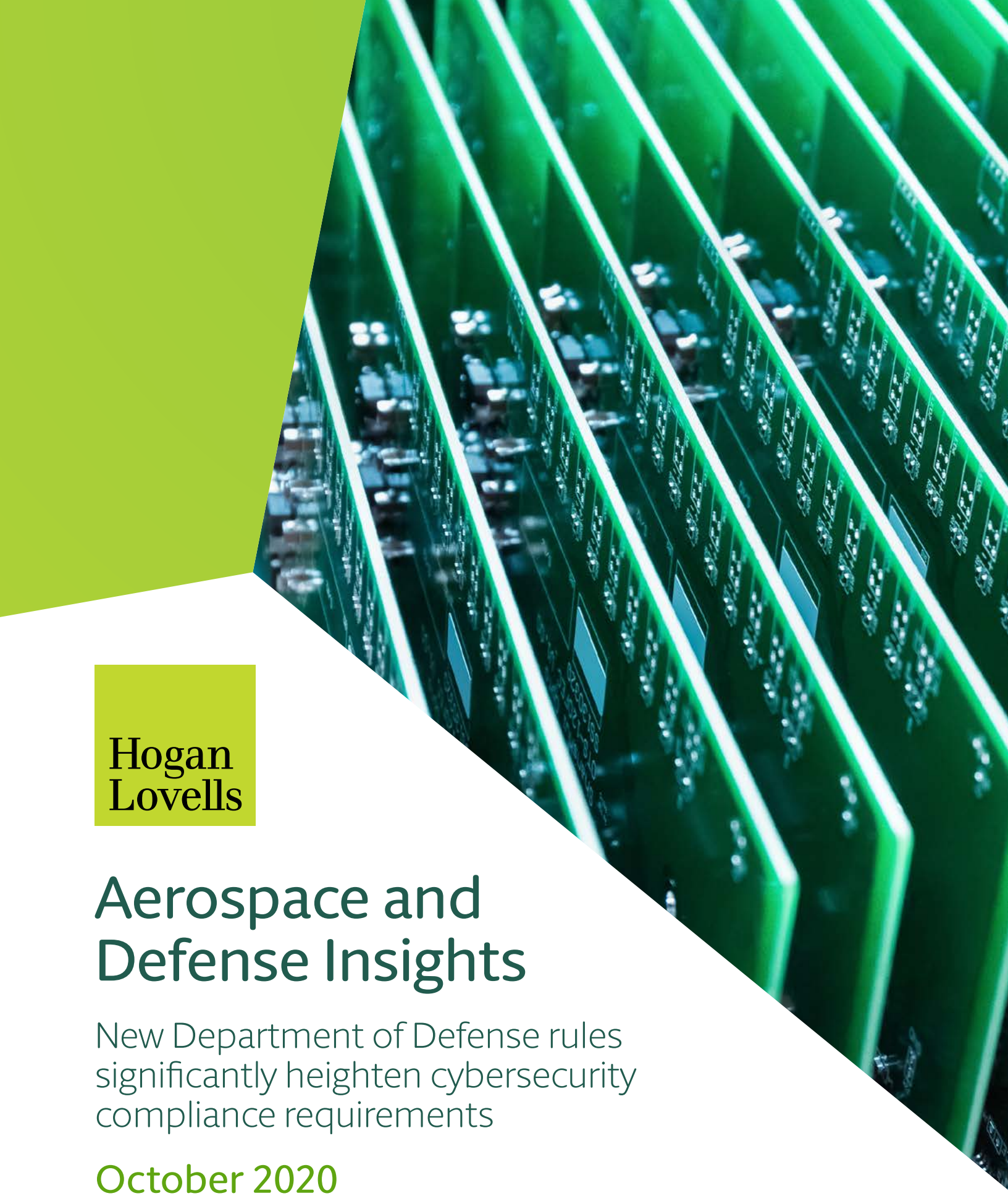


Hogan Lovells

Aerospace and Defense Insights

New Department of Defense rules significantly heighten cybersecurity compliance requirements

October 2020

Stacy M. Hadeka, Michael J. Scheimer, and Michael F. Mason

Through Aerospace and Defense Insights, we share with you the top legal and political issues affecting the aerospace and defense (A&D) industry. Our A&D industry team monitors the latest developments to help our clients stay in front of issues before they become problems, and seize opportunities in a timely manner.

Introduction

On 29 September 2020, the Department of Defense (DoD) issued an interim rule amending the Defense Federal Acquisition Regulation Supplement (DFARS), *Assessing Contractor Implementation of Cybersecurity Requirements* (DFARS Case 2019–D041), 85 Fed. Reg. 61,505 (29 September 2020), available here. The interim rule establishes a two-pronged approach to assess and verify the Defense Industrial Base's (DIB) ability to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) on contractor information systems or networks based on:

- The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 DoD Assessment Methodology; and
- The Cybersecurity Maturity Model Certification (CMMC) framework.

The rule establishes a requirement for DoD contractors to have a current NIST SP 800-171 DoD Assessment and the appropriate CMMC level certification prior to contract award and during contract performance. This will allow DoD to assess contractor implementation of cybersecurity requirements and enhance the protection of sensitive unclassified information within the DoD supply chain.

The rule amends the DFARS and adds three new DFARS clauses to the existing realm of safeguarding provisions.

Current DFARS clauses	New DFARS clauses
252.204-7008, *Compliance with Safeguarding Covered Defense Information Controls*	252.204-7019, *Notice of NIST SP 800-171 DoD Assessment Requirements*
252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*	252.204-7020, *NIST SP 800-171 DoD Assessment Requirements*
252.239-7010, *Cloud Computing Services*	252.204-7021, *Cybersecurity Maturity Model Certification Requirements*

These new DFARS clauses will apply to all DoD contracts and subcontracts, including those for the acquisition of commercial items and to acquisitions valued at or below the simplified acquisition threshold, but greater than the micro-purchase threshold. The only exception pertains to contracts or subcontracts exclusively for the acquisition of commercially available off-the-shelf (COTS) items.

The rule becomes effective on 30 November 2020. Contractors are invited to submit comments by that date to be considered in the formation of a final rule.

Part I: The NIST SP 800-171 DoD Assessment Methodology

Background

The Federal Acquisition Regulation (FAR) and DFARS currently prescribe contract clauses to protect FCI and CUI within the DoD supply chain. Specifically, FAR 52.204-21, *Basic Safeguarding of Covered Contractor Information Systems*, requires all contractors and subcontractors to apply basic safeguarding requirements when processing, storing, or transmitting FCI in or from covered contractor information systems. We have previously written about these requirements here.

DoD contractors are subject to additional requirements set forth in DFARS 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*, which requires defense contractors and subcontractors to provide "adequate security" on information systems or networks that store, process, or transmit DoD CUI[1], and to report cyber incidents that affect these systems or networks. We previously discussed these requirements here and here. In providing adequate security, a contractor must implement, at a minimum, the security requirements in NIST SP 800-171, *Protecting CUI in Nonfederal Systems and Organizations*. Contractors can document their implementation of NIST SP 800-171 in a system security plan (SSP), in addition to associated plans of action and millstones (POA&M) that address how and when any unimplemented security requirements will be met. The current regulations enable contractors and subcontractors to process, store, or transmit CUI without having implemented all 110 security requirements in NIST SP 800-171 and without establishing enforceable timelines for addressing any gaps. Moreover, neither the FAR nor DFARS clauses provide for DoD verification of a contractor's implementation of basic safeguarding requirements or the security requirements in NIST SP 800-171 prior to contract award, as contractors merely self-attest to their compliance.

DIBCAC assessments

In February 2019, the Under Secretary of Defense for Acquisition and Sustainment directed the Defense Contract Management Agency (DCMA) to develop a standard methodology to assess contractor implementation of the cybersecurity requirements in NIST SP 800-171 at the corporate or entity level.[2] In November 2019, DoD unveiled the standard DoD-wide methodology for assessing DoD contractor implementation of the security requirements in NIST SP 800-171.[3] Over the last year, DCMA's Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) conducted over 70 NIST SP 800-171 assessments of the DIB covering over 500 commercial and government entity codes.[4] According to DCMA, only twenty-five percent of the companies assessed met all 110 requirements.

The DIBCAC leverages the NIST SP 800-171 DoD Assessment Methodology (currently version 1.2.1),[5] which provides for the assessment of a contractor's implementation of NIST SP 800-171

1. DoD is transitioning from the use of the term "covered defense information" in the DFARS to "DOD Controlled Unclassified Information (CUI)," consistent with the Department's updated CUI guidance in DoDI 5200.48, *Controlled Unclassified Information* (CUI) (6 March 2020).
2. DoD Memorandum, *Strategically Implementing Cybersecurity Contract Clauses* (5 February 2019), available at https://www.acq.osd.mil/dpap/pdi/cyber/docs/USA000261-19%20USD%20Signed%20TAB%20A.pdf.
3. DoD Memorandum, *Assessing Contractor Implementation of Cybersecurity Requirements* (14 November 2019), available at https://www.acq.osd.mil/dpap/pdi/cyber/docs/14%20Nov%202019%20USD(A&S)%20Memo%20Assessing%20Contractor%20Implementation%20of%20Cybersecurity%20Requirements.pdf.
4. DoD Memorandum, *Supplier Performance Risk System for National Institute of Standards and Technology Special Publication 800-171 Department of Defense Assessment* (1 July 2020), available at https://www.acq.osd.mil/dpap/policy/policyvault/USA001243-20-DPC.pdf.
5. NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1 (24 June 2020) available at https://tinyurl.com/y2vz44mn.

security requirements, as required by DFARS clause 252.204-7012. The assessment uses a standard scoring methodology, which reflects the net effect of NIST SP 800-171 security requirements not yet implemented by a contractor, with a perfect score of 110.[6] There are three assessment levels – Basic, Medium, and High – which use the same scoring system and reflect the depth of the assessment performed and the associated level of confidence in the score resulting from the assessment. A Basic assessment is a self-assessment completed by the contractor, whereas Medium or High assessments are completed by the government.

DIBCAC logs the assessment results in the Supplier Performance Risk System (SPRS).[7] In July 2020, DoD announced the deployment of a cyber assessment capability module within SPRS in support of NIST SP 800-171 compliance.[8] With this deployment, authorized representatives of a contractor may enter results for Basic (self) assessments, while DIBCAC may enter summary results for Medium and High assessments. The deployment also allows for a virtual process, driven by COVID-19, for DIBCAC to evaluate a company's cybersecurity status versus the traditional in-person reviews.

Assessments are completed for each covered contractor information system that is relevant to the offer, contract, task order, or delivery order. Historically, the ability to conduct an assessment has been included in Sections C and L of solicitations, which would require the contractor to permit a government cyber assessment team to perform an on-site review for compliance with DFARS 252.204-7012 of contractor systems that would be processing, storing, transmitting, or displaying CUI.

The DIBCAC has indicated that it plans to assess up to 90 companies in 2021.

Basic assessment	Medium assessment	High assessment
A contractor's self-assessment of its implementation of NIST SP 800-171 that: • Is based on the contractor's review of their system security plan(s) associated with covered contractor information system(s); • Is conducted in accordance with the NIST SP 800-171 DoD Assessment Methodology; and • Results in a confidence level of "Low" in the resulting score, because it is a self-generated score.	An assessment conducted by the government that: • Consists of — A review of a contractor's Basic assessment; — A thorough document review; — Discussions with the contractor to obtain additional information or clarification, as needed; and • Results in a confidence level of "Medium" in the resulting score.	An assessment that is conducted by government personnel using NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information that: • Consists of — A review of a contractor's Basic assessment; — A thorough document review; — Verification, examination, and demonstration of a contractor's system security plan to validate that NIST SP 800-171 security requirements have been implemented as described in the contractor's system security plan; — Discussions with the contractor to obtain additional information or clarification, as needed; and — Results in a confidence level of "High" in the resulting score.

6. A company that has fully implemented all 110 NIST SP 800-171 security requirements would have a score of 110 to report in SPRS for their Basic assessment. A company that has unimplemented requirements will use the scoring methodology to assign a value to each unimplemented requirement, add up those values, and subcontract the total value from 110 to determine their score.
7. This was first updated in November 2019 to capture assessment information, including the scope of the information system/system security plan(s) assessed mapped to contractor CAGE codes, total summary score assessed, and date expected to achieve a score of 110.
8. DoD Memorandum, Supplier Performance Risk System (SPRS) for NIST SP 800-171 DoD Assessment (1 July 2020), available at https://www.acq.osd.mil/dpap/policy/policyvault/USA001243-20-DPC.pdf.

New developments

Effective 30 November 2020, the rule implements a standard methodology to assess contractor implementation of the cybersecurity requirements in NIST SP 800-171. The methodology provides a means for DoD to assess contractor implementation of these requirements as DoD transitions to full implementation of CMMC, and a means for companies to self-assess their implementation of the NIST SP 800-171 requirements prior to either a DoD or CMMC assessment.

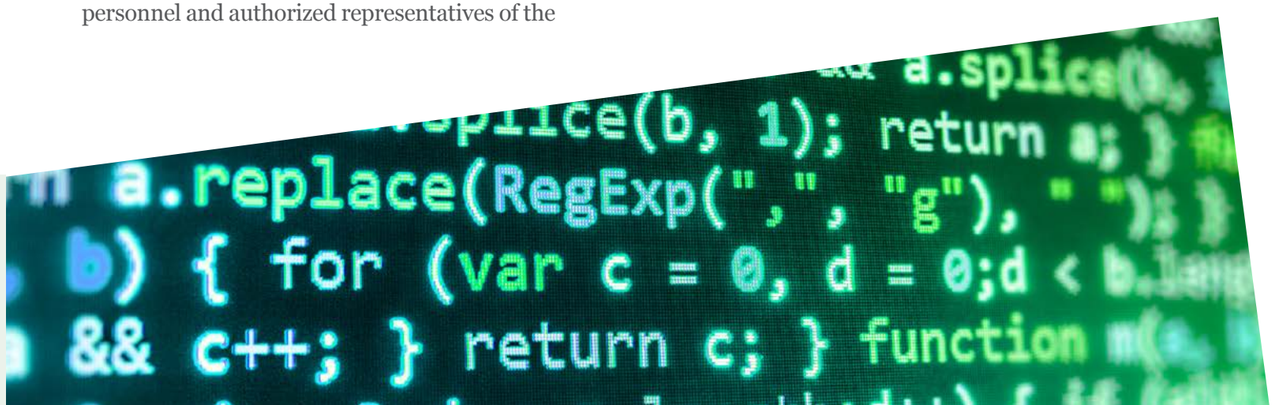
Specifically, the rule amends DFARS subpart 204.73, *Safeguarding Covered Defense Information and Cyber Incident Reporting*, to implement the NIST SP 800-171 DoD Assessment Methodology, which leverages the current DIBCAC assessment process. The new coverage in the subpart directs contracting officers to verify in SPRS that an offeror has a current NIST SP 800-171 DoD assessment on record prior to contract award, if the offeror is required to implement NIST SP 800-171 pursuant to DFARS clause 252.204-7012. The rule also directs a contracting officer to include the new DFARS clauses 252.204-7019, *Notice of NIST SP 800-171 DoD Assessment Requirements*, and 252.204-7020, NIST SP 800-171 *DoD Assessment Requirements*, in solicitations and contracts, including FAR part 12 commercial item acquisitions, except for solicitations solely for the acquisition of COTS items.

The new DFARS 252.204-7019 clause advises offerors of the requirement to have a current (not older than three years) NIST SP 800-171 DoD assessment on record in order to be considered for award. The clause also requires offerors to ensure the results of assessments are posted in SPRS and provides offerors with additional information on conducting and submitting an assessment when a current one is not posted in SPRS. The rule notes that only DoD personnel and authorized representatives of the contractor will have access to SPRS, and that the assessment scores are considered protected.

The new DFARS clause 252.204-7020 requires a contractor to provide the government with access to its facilities, systems, and personnel when it is necessary for DoD to conduct or renew a higher-level assessment. The clause also requires the contractor to ensure that applicable subcontractors also have the results of a current assessment posted in SPRS prior to awarding a subcontract or other contractual instruments. The clause outlines how a subcontractor can conduct and submit an assessment when one is not posted in SPRS, and requires the contractor to include the requirements of the clause in all applicable subcontracts or other contractual instruments.

At a minimum, all offerors that are required to implement NIST SP 800-171 on covered contractor information systems are required to complete a Basic assessment and upload the resulting score to SPRS. The requirement for the Basic assessment will be imposed through incorporation of the new solicitation provision and contract clause in new contracts and orders. As such, the requirement to have completed a Basic assessment is expected to phase-in over a three-year period. To submit the Basic assessment, a contractor is required to complete six fields:

- System security plan name (if more than one system is involved);
- CAGE code associated with the plan;
- A brief description of the plan architecture;
- Date of the assessment;
- Total score; and
- The date a score of 110 will be achieved.



After a contract is awarded, DoD may choose to conduct a Medium or High assessment based on the criticality of the program or the sensitivity of information being handled by the contractor. DoD expects that the Medium and High assessments will be conducted on a finite number of awardees each year based on the capacity of the government to conduct these assessments. Under both the Medium and High assessments, DoD will review the contractor's SSP describing how each NIST SP 800-171 requirement is met and will identify any descriptions that may not properly address the security requirements. The contractor must provide DoD access to its facilities and personnel (either physically or virtually), if necessary, and should prepare for and participate in the assessment conducted by the DoD. Under a High assessment a contractor will be asked to demonstrate their SSP. DoD will ultimately post the results in SPRS,[9] but at the end of these assessments, the contractor has 14 business days to provide additional information to demonstrate that they meet any security requirements not observed by the assessment team or to rebut the findings that may be of question. Once finalized, DoD components will use the scores in SPRS to evaluate quotes and offers received under all solicitations for supplies and services.[10]

Part II: The Cybersecurity Maturity Model Certification (CMMC) framework

Background

Building upon the NIST SP 800-171 DoD Assessment Methodology, the CMMC framework adds a comprehensive and scalable certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level.[11] CMMC will provide increased assurance that contractors can adequately protect FCI and CUI, including such information that flows down to subcontractors throughout the supply chain. We previously wrote about CMMC here.

CMMC assessments

The CMMC model (currently version 1.02) consists of five levels, cumulatively made up of maturity ***processes*** and cybersecurity best ***practices***.[12] The CMMC model encompasses the basic safeguarding requirements for FCI specified in FAR 52.204-21 and security requirements for CUI per DFARS clause 252.204-7012. The CMMC model includes an additional five processes and 61 practices across Levels 2 through 5 that demonstrate a progression of cybersecurity maturity. A contractor can achieve a specific CMMC level for its entire enterprise network or particular segment(s) or enclave(s), depending upon where the information to be protected is processed, stored, or transmitted.

CMMC assessments are to be conducted by CMMC Third-Party Assessor Organizations (C3PAOs), which are accredited by the CMMC Accreditation Body (CMMC-AB). C3PAOs provide CMMC assessment reports to the CMMC-AB, which will then issue CMMC certificates at the appropriate CMMC level upon the resolution of any disputes or anomalies identified during the assessment.

In order to achieve a specific CMMC level, a contractor must demonstrate both process institutionalization or maturity and the implementation of practices commensurate with that level. The levels consist of the following:

Level 1: The practices map directly to the basic safeguarding requirements specified in the clause at FAR 52.204-21.

Level 2: The practices encompass 48 of the 110 security requirements of NIST SP 800-171 and seven additional cybersecurity requirements. In addition, CMMC Level 2 includes two process maturity requirements.

Level 3: The practices encompass all 110 security requirements of NIST SP 800-171, as well as 13 additional cybersecurity requirements above Level 2. In addition, CMMC Level 3 includes three process maturity requirements.

9. *See* Supplier Performance Risk System available at https://www.sprs.csd.disa.mil/; see also Supplier Performance Risk System Awardee User Guide, Version 3.2.11 (September 2020) available at https://www.sprs.csd.disa.mil/pdf/SPRS_Awardee.pdf;
10. 85 Fed. Reg. 53,748 (31 August 2020).
11. *See* Pub. L. 116-92 § 1648 (requiring the Secretary of Defense to develop a risk-based cybersecurity framework for the DIB sector as the basis for a mandatory DoD standard).
12. *See* Office of the Under Secretary of Defense for Acquisition & Sustainment Cybersecurity Maturity Model Certification, available at https://www.acq.osd.mil/cmmc/index.html.

Level 4: The practices encompass all 110 security requirements of NIST SP 800-171 and 46 additional cybersecurity requirements. CMMC Level 4 adds 26 enhanced security requirements above CMMC Level 3, of which 13 are derived from Draft NIST SP 800-171B (now NIST SP 800-172). In addition, CMMC Level 4 includes four process maturity requirements.

Level 5: The practices encompass all 110 security requirements of NIST SP 800-171 and 61 additional cybersecurity requirements. More specifically, CMMC Level 5 adds 15 enhanced security requirements above CMMC Level 4, of which four are derived from Draft NIST SP 800-171B.[13] In addition, CMMC Level 5 includes five process maturity requirements.

New developments

The interim rule formalizes the CMMC framework and its application to DoD contractors. DoD is implementing a five-year phased rollout of CMMC through 30 September 2025. Over the next five years, DoD will include the new DFARS clause 252.204-7021, *Cybersecurity Maturity Model Certification Requirements*, in select solicitations and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial items and excluding acquisitions exclusively for COTS items, if the requirements document or statement of work requires a contractor to have a specific CMMC level.[14] For these solicitations, contractors will be required to have the stated CMMC certification level at the time of contract award. DoD expects to assess and certify 15 companies in 2021.

CMMC will apply to all DoD solicitations and contracts, including those for the acquisition of commercial items (except those exclusively COTS items) valued at greater than the micro-purchase threshold, starting on or after 1 October 2025.[15] At a minimum, contractors will be required to obtain a CMMC Level 1 certification. The certification will appear in SPRS to enable the verification of an offeror's certification level and currency (i.e., not more than three years old) prior to contract award.[16] DoD will require CMMC level certification at the time of award, and CMMC certification requirements are required to be flowed down to subcontractors at all tiers, based on the sensitivity of the unclassified information flowed down to each subcontractor.

Practical considerations

With the approaching effective date for the interim rule, contractors and subcontractors that are required to implement NIST SP 800-171 pursuant to DFARS clause 252.204-7012 are encouraged to immediately conduct and submit a Basic self-assessment.[17] Moreover, those contractors that have not fully implemented the FAR basic safeguarding requirements should begin addressing gaps immediately.

As noted by DFARS 252.204-7012, a DoD NIST SP 800-171 assessment is inapplicable to those contractors that do not process, transmit, or store DoD CUI. Thus, contractors and subcontractors should seek to clarify and limit the type of information they receive and also document as to why they may not need a Basic assessment. Those contractors will at the very least, however, be required to obtain a CMMC Level 1 certification. For those contractors required to conduct a Basic assessment, it is unclear how the government will view an error or incorrectly reported self-assessment score, although potential liability under the False Claims Act poses a risk.

The rule requires the flow down of the DoD NIST SP 800-171 assessment and CMMC framework to subcontractors, but prime contractors will not have access to subcontractor or supplier assessment information in SPRS, so contractors should obtain

13. On 6 July 6 2020, NIST released NIST SP 800-172, *Enhanced Security Requirements for Protecting Controlled Unclassified Information - A Supplement to NIST Special Publication 800-171*, which supersedes DRAFT NIST SP 800-171B, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations - Enhanced Security Requirements for Critical Programs and High Value Assets.*
14. Inclusion of a CMMC requirement in a solicitation during this time period must be approved by the Office of the Under Secretary of Defense for Acquisition and Sustainment.
15. Contracting officers will not be allowed to award, or exercise an option on a contract, if the offeror or contractor does not have current (i.e., not older than three years) certification for the required CMMC level.
16. CMMC dispute resolution will be handled by the CMMC-AB, which will follow a formal, but yet to be finalized, process to review the adjudication request and provide a preliminary evaluation to the contractor and C3PAO. If the contractor does not accept the CMMC-AB preliminary finding, the contractor may request an additional assessment by the CMMC-AB staff.
17. Although the interim rule has a delayed effective date (i.e., 30 November 2020), in the preamble DoD encourages its contractors to conduct and submit the Basic level self-assessment described in the interim rule "immediately." 85 Fed. Reg. 61,518.

certifications from their lower-tier subcontractors as to whether an assessment has been completed. DoD also recommends obtaining a copy of a subcontractor self-assessment as a way to document their status, but this may receive push back from lower-tier contractors, especially since the High assessment itself will be considered to involve CUI or should be protected against unauthorized use and release.[18] The rule also notes that prime contractors must determine the CMMC level for subcontractors and identify that level which is appropriate for the information that flows down to the subcontractor. There is no guidance on how contractors should determine this.

There are also outstanding questions related to both the DoD assessment and CMMC scoring. For instance, the ultimate impact of the score is unclear, i.e., whether DoD will require a minimum score and if it will use such score as a pass/fail. It is also unclear whether the government will give deference to higher assessment scores or CMMC levels. More clarity is needed on these issues.

Lastly, contractors should be cognizant of the potential expansion of the cybersecurity assessment requirements to civilian agencies. For instance, in July 2020, GSA included a CMMC requirement in its Streamlined Technology Acquisition Resource for Services (STARS III) contract. There is also an open CUI FAR rule, FAR Case 2017-016, which may ultimately apply these security requirements in a more expansive manner. Contractors should thus continue to monitor the application of these requirements throughout the government.

Conclusion

The government has issued several resources to assist contractors and subcontractors with NIST 800-171 compliance:

- NIST Handbook 162, *NIST MEP Cybersecurity Self-Assessment Handbook For Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements*;
- NIST SP 800-171A, *Assessing Security Requirements for Controlled Unclassified Information*; and
- NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1.

Contractors should be prepared to conduct a Basic assessment if planning to receive a DoD contract award after 30 November 2020. Contractors should also continue to close the gaps on their POA&Ms.

Other notable developments

Throughout the first three quarters of 2020, there were several other cybersecurity and CUI safeguarding developments relevant to Aerospace and Defense contractors. We highlight a few below:

- DoD issued a CUI website at https://www.dodcui.mil/.
- NIST released Revision 5 of NIST SP 800-53 on 23 September 2020.
- DoD updated its Frequently Asked Questions (FAQs) regarding the implementation of cybersecurity requirements on 30 July 2020.
- NIST renamed NIST SP 800-171B to NIST SP 800-172 on 6 July 2020.
- DoD issued Instruction 5200.48 on 6 March 2020, which replaces DoD Manual 5200.01, Volume 4, DoD Information Security Program: Controlled Unclassified Information (24 February 2012). DoDI 5200.48 establishes policies, responsibilities, and procedures for CUI, as well as a DoD CUI repository (see the DoD CUI website). DoD is also in the process of developing a guide for industry on the handling of CUI.
- NIST released Revision 2 of NIST SP 800-171 on 21 February 2020.

18. The rulemaking states that information from High assessments may be DoD CU and will be protected from release, including through the exercise of applicable exemptions under the Freedom of Information Act (e.g., Exemption 4 covers trade secrets and commercial or financial information obtained from a contractor that is privileged or confidential). 85 Fed. Reg. 61,521

Stacy M. Hadeka
Senior Associate | Washington, D.C.
T: +1 202 637 3678
E: stacy.hadeka@hoganlovells.com

Michael J. Scheimer
Senior Associate | Washington, D.C.
T: +1 202 637 6584
E: michael.scheimer@hoganlovells.com

Michael F. Mason
Partner | Washington, D.C.
T: +1 202 637 5499
E: mike.mason@hoganlovells.com

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta*
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Riyadh*
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar*
Warsaw
Washington, D.C.
Zagreb*

*Our associated offices
Legal Services Center: Berlin

www.hoganlovells.com