BRIEFING PAPERS® SECOND SERIES

PRACTICAL TIGHT-KNIT BRIEFINGS INCLUDING ACTION GUIDELINES ON GOVERNMENT CONTRACT TOPICS

# CMMC And The Future Of Cybersecurity In The Defense Industrial Base

*By Tom Pettit, Ron Lee, and Tirzah Lollar**

The Department of Defense (DoD) has long been concerned about cybersecurity within the Defense Industrial Base (DIB) and been a leader within the U.S. Government for establishing cybersecurity standards. DoD was among the first agencies to require contractors to implement National Institute of Standards and Technology (NIST) security standards, including NIST Special Publication (SP) 800-171, and to report cyber incidents. In recent years, DoD (and the Government more broadly) has become concerned about contractor compliance with those requirements. Enter the Cybersecurity Maturity Model Certification (CMMC), which is, at its core, a cybersecurity compliance certification and verification program. This BRIEFING PAPER discusses (1) the history and underpinnings of CMMC, (2) CMMC requirements, (3) enforcement risks, (4) key takeaways for defense contractors, and (4) practical guidelines.

## The Development Of CMMC

The underpinnings of CMMC date back to when the Federal Acquisition Regulation (FAR) Council issued FAR 52.204-21, "Basic Safeguarding of Covered Contractor Information Systems," and DoD issued Defense FAR Supplement (DFARS) 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting." Those clauses establish the foundational substantive cybersecurity requirements for CMMC.

In May 2016, the FAR Council created FAR 52.204-21.[1] That clause applies to all "solicitations and contracts when the contractor or a subcontractor at any tier may have Federal contract information residing in or transiting through its information system" except for contracts for commercially available off-the-shelf (COTS) items.[2] Information qualifies as federal contract information (FCI) if it is (1) "not intended for public release"; (2)

**Tom Pettit is a Senior Associate and Ron Lee is a Partner in the Government Contracts and National Security Practice at Arnold & Porter. Tirzah Lollar is a Partner in the White Collar Defense & Investigations Practice at Arnold & Porter. They have extensive experience advising government contractors on cybersecurity compliance and representing government contractors facing cybersecurity challenges, including cyber incidents, contract disputes, and government investigations.*

## IN THIS ISSUE:

| | |
|---|---|
| The Development Of CMMC | 1 |
| CMMC 2.0 | 3 |
| Compliance Risks | 5 |
| Key Takeaways | 6 |
| Guidelines | 7 |

"is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government"; and (3) is not "simple transactional information, such as [information] necessary to process payments."[3] This definition is intentionally broad, and there are no markings for FCI, meaning if there is any possibility that a contractor information system will store, process, or transmit FCI, the contractor should implement FAR 52.204-21.[4] To implement FAR 52.204-21, prime contractors and subcontractors with covered contractor information systems must implement 15 security controls, which include information system and facility security controls.[5]

In November 2013, DoD issued DFARS 252.204-7012, which imposes information system security and cyber incident reporting requirements.[6] Most relevant to CMMC, DFARS 252.204-7012 requires contractors that will store, process, or transmit covered defense information (CDI),[7] which includes controlled unclassified information (CUI) that is "[c]ollected, developed, received, transmitted, used, or stored by or on behalf of the contractor in performance of the contract," to "provide adequate security on all covered contractor information systems."[8] For unclassified contractor information systems, that means complying with NIST SP 800-171.[9] Although NIST has issued Revision 3 of NIST SP 800-171, DoD requires compliance with Revision 2 for purposes of DFARS 252.204-7012 (and now for CMMC).[10] For external cloud service providers that store, process, or transmit CDI in connection with contract performance, adequate security means meeting the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline.[11] DFARS 252.204-7012 also requires contractors to report cyber incidents.[12]

Based on concerns about contractor compliance with cybersecurity requirements, DoD issued an interim rule effective November 30, 2020, establishing DoD NIST SP 800-171 assessment and reporting requirements and the initial CMMC program (CMMC 1.0).[13] DoD implemented those requirements through three new clauses: DFARS 252.204-7019, "Notice of NIST SP 800-171 DoD Assessment Requirements"; DFARS 252.204-7020, "NIST SP 800-171 DoD Assessment Requirements"; and DFARS 252.204-7021, "Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirement."

DFARS 252.204-7019 and DFARS 252.204-7020, which remain in effect today, require defense contractors (both prime contractors and subcontractors) to meet DoD NIST SP 800-171 assessment requirements for covered contractor information systems. Specifically, defense contractors must use the NIST SP 800-171 DoD Assessment Methodology to measure the extent to which they have implemented NIST SP 800-171 security controls for covered contractor information systems. There are three assessment levels: Basic, Medium, and High. For a Basic Assessment, the contractor reviews its system security plans (SSPs) for covered contractor information systems.[14] DoD has "low confidence" in a Basic Assessment's accuracy because it is performed by the contractor. For a Medium Assessment, DoD attempts to verify a contractor's Basic Assessment by reviewing the contractor's Basic Assessment and related documents and seeking clarification as needed.[15] A Medium Assessment results in a Medium level of confidence. A High Assessment requires DoD to conduct its own thorough assessment of the contractor's covered information systems, SSP, and other documents, and a High Assessment results

Editor: Valerie L. Gross



*Briefing Papers® (ISSN 0007-0025) is published monthly, except January (two issues) and copyrighted by Thomson Reuters, 610 Opperman Drive, P.O. Box 64526, St. Paul, MN 55164-0526. Customer Service: (800) 328-4880. POSTMASTER: Send address changes to Briefing Papers, 610 Opperman Drive, P.O. Box 64526, St. Paul, MN 55164-0526.*

in a High level of confidence.[16] Each assessment results in a score between -203 (no NIST SP 800-171 controls implemented) to 110 (full implementation of NIST SP 800-171 controls), and contractors must enter that score into the Supplier Performance Risk System (SPRS). An assessment is current if it is no more than three years old.[17]

In that same interim rule, DoD issued DFARS 252.204-7021 to implement CMMC 1.0. DoD subsequently suspended CMMC 1.0 and began a years-long effort to create CMMC 2.0.

## CMMC 2.0

CMMC 2.0 is the product of a two-part rulemaking. On October 15, 2024, DoD issued a final rule codifying regulations at 32 C.F.R. Part 170 to establish the fundamentals of the CMMC program (the "Program Rule"),[18] and on September 10, 2025, DoD issued a final rule revising the DFARS to implement CMMC into DoD solicitations and contracts (the "DFARS Rule").[19] The CMMC four-phase implementation process begins November 10, 2025, when the DFARS Final Rule takes effect.

### *Applicability*

CMMC applies to all DoD prime contractors and subcontractors that will store, process, or transmit FCI or CUI on unclassified contractor information systems while performing a DoD contract, other than a contract exclusively for commercially available off-the-shelf (COTS) items.[20] (The Program Rule refers to prime contractors and subcontractors subject to CMMC as Organizations Seeking Assessment (OSAs),[21] and we use that term at certain points in this Briefing Paper.) CMMC requirements are not limited to information systems owned by the contractor. External service providers (ESPs), including cloud service providers (CSPs),[22] that will store, process, or transmit FCI or CUI for the contractor must also meet CMMC requirements.

### *CMMC Levels, Assessments, SPRS Data, And Affirmations*

CMMC requirements are divided across three CMMC levels, and the security control and assessment requirements increase with the CMMC level. To be eligible for award in a DoD procurement, an offeror must achieve the CMMC level specified in the solicitation by the time of contract award. DoD contractors must maintain compliance throughout contract performance.

*CMMC Level 1* applies where defense contractors will store, process, or transmit FCI (but not CUI) on their information systems. To achieve CMMC Level 1, contractors must implement each of the 15 security controls in FAR 52.204-21(b). Plans of action and milestones (POAMs) are not allowed for CMMC Level 1.[23]

*CMMC Level 2* applies where defense contractors will store, process, or transmit CUI on their information systems. DoD will accept Conditional CMMC Level 2 status temporarily. To achieve Conditional CMMC Level 2 status, contractors must implement all critical requirements and at least 80% of the NIST SP 800-171 security controls overall.[24] All non-critical security controls that are not met must be documented in a POAM, and the POAM must be closed out within 180 days of the Conditional CMMC Level 2 Status Date. If a contractor does not close out the POAM within 180 days and achieve Final CMMC Level 2 status, which is when the contractor has implemented all NIST SP 800-171 security controls, the Conditional CMMC Level 2 status lapses.[25]

There are two types of CMMC Level 2 assessments: self-assessments and certification assessments. For self-assessments, the contractor evaluates its own information system's compliance with NIST SP 800-171.[26] Certification assessments are performed by CMMC Third-Party Assessment Organizations (C3PAOs).[27] Solicitations and contracts will specify whether a self-assessment or a certification assessment is required. Assessments, whether self-assessments or certification assessments, are valid for three years, but the contractor's Affirming Official (*i.e.*, "the senior level representative" who is responsible for and has authority to affirm continuous compliance with security requirements)[28] must certify continuous compliance annually.[29] Significantly, contractors should not assume that self-assessments will be sufficient. DoD stated in the DFARS Rule that it anticipates 35% of defense contractors will require a CMMC Level 2 certification assessment and only 2% of defense contractors will require a CMMC Level 2 self-assessment. (Another 62% of contractors will require only CMMC Level 1, and the remaining 1% of contractors will require CMMC Level 3.)[30] This shows that when a solicitation or contract

 

requires CMMC Level 2, contractors will almost always need a certification assessment rather than a self-assessment.

*CMMC Level 3* is required for certain contracts where DoD determines that additional security controls are needed to protect CUI from Advanced Persistent Threats. To meet CMMC Level 3, contractors must achieve CMMC Levels 1 and 2 and implement 24 additional requirements from NIST SP 800-172.[31] Contractors can achieve Conditional CMMC Level 3 status if they implement certain critical requirements and at least 80% of the 24 additional requirements overall.[32] As with CMMC Level 2, contractors must document all controls that they have not met in a POAM and closeout the POAM within 180 days or the Conditional CMMC Level 3 status lapses.[33] CMMC Level 3 assessments are performed by the Defense Contract Management Agency, Defense Industrial Base Cybersecurity Assessment Center (DIBCAC).[34] Similar to CMMC Level 2, a CMMC Level 3 status is valid for three years,[35] and the Affirming Official must annually certify continuous compliance.[36]

Regardless of the level, CMMC data (CMMC Level, CMMC Status Date, CMMC Assessment Scope, applicable CAGE code(s), and the compliance result) must be entered into SPRS. For self-assessments, the OSA enters the data into SPRS.[37] For CMMC Level 2 C3PAO assessments, the C3PAO reports the compliance results into eMASS, which transmits the data to SPRS.[38] For CMMC Level 3, DIBCAC reports the compliance results into eMASS, which transmits the data to SPRS.[39]

### *CMMC Scoping*

A critical element of CMMC compliance is identifying the information systems that will fall within the scope of the CMMC assessment. The scoping process depends on the CMMC level pursued.

A contractor that is seeking only a CMMC Level 1 assessment must identify which information systems will store, process, or transmit FCI.[40] The CMMC Level 2 scope is broader and includes CUI Assets, Security Protection Assets (SPAs), Contractor Risk Managed Assets (CRMAs), and Specialized Assets. CUI Assets (*i.e.*, "[a]ssets that process, store, or transmit CUI") must be assessed against all NIST SP 800-171 security controls.[41] SPAs (*i.e.,*"[a]ssets that provide security functions or capabilities to the OSA's CMMC Assessment Scope"), such as firewalls, must be assessed against all NIST SP 800-171 security controls "that are relevant to the capabilities provided."[42] CRMAs (*i.e.,*"assets that can, but are not intended to, process, store, or transmit CUI because of security policy, procedures, and practices in place") are subject to a more limited assessment. CRMAs are not assessed against all NIST SP 800-171 security controls, but CRMAs must be sufficiently documented in the SSP. If that documentation raises concerns, CRMAs can be subject to "a limited check to identify deficiencies."[43] For Specialized Assets (*i.e.,* "[a]ssets that can process, store, or transmit CUI but are unable to be fully secured, including: Internet of Things (IoT) devices, Industrial Internet of Things (IIoT) devices, Operational Technology (OT), Government Furnished Equipment (GFE), Restricted Information Systems, and Test Equipment"), assessments are limited to reviewing SSP documentation.[44] Assets that do not store, process, or transmit CUI; assets that do not qualify as SPAs; and assets that are separated (physically or logically) from CUI assets are out of scope.[45]

The CMMC Level 3 scope builds upon CMMC Level 2. CUI Assets, CRMAs, SPAs, and Specialized Assets are subject to a limited check against NIST SP 800-171 security controls (those assets had to meet those controls as part of CMMC Level 2) and are assessed against all applicable NIST SP 800-172 security controls.[46] Similar to CMMC Level 2, assets that cannot store, process, or transmit CUI; assets that do not qualify as SPAs; and assets that are separated (physically or logically) from CUI assets are out of scope.[47]

As noted above, ESPs are subject to CMMC, and ESP assets that store, process, or transmit CUI or Security Protection Data (SPD) must meet CMMC requirements. Services from ESPs other than CSPs fall within the scope of the OSA's assessment. CSP services that store, process, or transmit CUI must meet at least the Federal Risk and Authorization Management Program (FedRAMP) Moderate Baseline in accordance with DFARS 252.204-7012. FedRAMP authorizations will be increasingly important under CMMC. The Program Rule makes clear that contractors are "not responsible for the CSP's compliance" if the CSP has a FedRAMP Moderate (or higher) authorization.[48] If a CSP's offering is not FedRAMP Authorized at the Moderate Baseline (or higher),

 

then the contractor "is responsible for determining if the CSP meets the requirements for FedRAMP Moderate equivalency as specified in DoD policy,"[49] including the *Federal Risk and Authorization Management Program Moderate Equivalency for Cloud Service Provider's Cloud Service Offerings* memorandum issued in December 2023.[50]

### *CMMC Phase-In*

DoD is implementing CMMC through a four-phase process:[51]

- *Phase 1* begins on November 10, 2025, and during that phase, DoD will include CMMC Level 1 and Level 2 self-assessment requirements in applicable DoD solicitations and new contracts as a condition of contract award. However, DoD will have discretion to require CMMC Level 2 C3PAO certification assessments. DoD also has discretion to require CMMC Level 1 and Level 2 self-assessments for preexisting contracts as a condition of exercising an option period.[52]

- *Phase 2* begins on November 10, 2026, and during that phase, DoD will require CMMC Level 2 C3PAO certification assessments for applicable DoD solicitations and new contracts, but DoD has discretion to delay those certification assessments to an option period.[53]

- *Phase 3* begins on November 10, 2027. DoD will require CMMC Level 2 C3PAO certification assessments for applicable DoD solicitations and contracts (*i.e.,* DoD will no longer have discretion to push CMMC Level 2 C3PAO certification assessments to an option period). DoD will also require CMMC Level 2 C3PAO certification assessments for applicable DoD contracts awarded after November 10, 2025, as a condition of exercising an option.[54]

- *Phase 4* begins on November 10, 2028, and marks full implementation of CMMC.[55]

### *Supply Chain Compliance*

CMMC applies throughout the supply chain to any subcontractor, regardless of tier, if the subcontractor will store, process, or transmit FCI or CUI on its unclassified contractor information systems during performance. Contractors only have access to their own SPRS data, and "[p]rime contractors are expected to work with their suppliers to conduct verifications as they would for any other clause that flows down to subcontractors."[56]

## Compliance Risks

The Government has several tools when it comes to Government contractor compliance with cybersecurity requirements, and, by extension, contractors face exposure to different forms of liability. These tools can be used at the procurement stage, through contract remedies, or through False Claims Act (FCA) enforcement.

### *Procurement-Stage Risks*

Cybersecurity compliance first arises during the procurement process through solicitation terms, proposal evaluations, responsibility determinations, and bid protests. For instance, when a solicitation incorporates DFARS 252.204-7019, offerors must "implement NIST SP 800-171," conduct a NIST SP 800-171 assessment in accordance with the DoD NIST SP 800-171 Assessment Methodology DoD Assessment within the past three years, and input assessment data into SPRS in order to be eligible for award. In 2019, in *American Justice Solutions, Inc., dba CorrectiveSolutions*, the Government Accountability Office (GAO) upheld an agency's decision to disqualify the protester because "the quotation provided no indication that [the protester] had an information security plan to ensure compliance" with information security requirements, including NIST standards.[57] More recently in 2022, GAO held in *American Fuel Cell & Coated Fabrics Co.* that noncompliance with NIST SP 800-171 assessment requirements is disqualifying.[58] Disqualification risks have only increased since DoD issued DFARS 252.204-7024, "Notice on the Use of the Supplier Performance Risk System," in March 2023.[59] That clause states that SPRS "will be used in the evaluation of the Quoter or Offeror's performance" and allows contracting officers to "consider any other available and relevant information when evaluating a quotation or an offer."[60]

Even when offerors succeed in obtaining an award, they could face bid protests risks. As noted above, *American Fuel Cell & Coated Fabrics Co.* shows that offerors

 

could be ineligible for award if they fail to comply with cybersecurity requirements. GAO also recently held in *SMS Data Products Group, Inc.* that an award is unreasonable where the solicitation incorporates DFARS 252.204-7024 but the agency fails to assess risks in accordance with that clause.[61] Importantly, however, agencies and intervenors could have certain defenses depending on the nature of the protest arguments. For instance, GAO held in *Pitney Bowes, Inc.* that questions about whether an awardee will in fact comply with DFARS 252.204-7012 during performance are matters of contract administration outside GAO's bid protest jurisdiction.[62]

### *FCA Risks*

The FCA[63] is one of the Government's most powerful tools to enforce Government contracts requirements; provided, of course, that the Government (or a private whistleblower) can establish the elements for a fraud case. That statute makes it unlawful to, among other things, knowingly present a false or fraudulent claim for payment or approval to the Government, and the FCA allows the Government to recover treble damages plus penalties.[64] A key element of the FCA is that it allows private persons to bring FCA lawsuits on the Government's behalf, effectively acting as private attorneys general.[65] An FCA lawsuit can be brought by a private person or entity (a *qui tam* relator) or the Government, and while most courts have found the FCA's *qui tam* provisions to be constitutional, recent decisions have reignited questions about the constitutionality of *qui tam* actions.[66] Federal law also provides the Government with broad authority to issue civil investigative demands (CIDs) as a tool to investigate suspected FCA violations.[67]

On October 6, 2021, the Department of Justice (DOJ) launched the Civil Cyber-Fraud Initiative to "combine the department's expertise in civil fraud enforcement, government procurement and cybersecurity to combat new and emerging cyber threats to the security of sensitive information and critical systems."[68] DOJ objectives include "[b]uilding broad resiliency against cybersecurity intrusions across the government, the public sector and key industry partners"; "[h]olding contractors and grantees to their commitments to protect government information and infrastructure"; "[e]nsuring that companies that follow the rules and invest in meeting cybersecurity requirements are not at a competitive disadvantage"; "[r]eimbursing the government and the taxpayers for the losses incurred when companies fail to satisfy their cybersecurity obligations"; and "[i]mproving overall cybersecurity practices that will benefit the government, private users and the American public."[69]

DOJ's (and relators') efforts have reaped results in many cases. As of the date of publication, there do not appear to be any cases where a court issued final judgment holding that a contractor was in fact liable under the FCA for violating cybersecurity contract clauses like DFARS 252.204-7012. But since 2021, just over a dozen contractors have reached multi-million dollar settlements with DOJ (typically without admitting liability) to resolve FCA allegations related to noncompliance with cybersecurity requirements, for example for failing to implement NIST SP 800-171 controls, failing to have an SSP, or misreporting its score or POAM completion dates in SPRS.[70]

### *Contract Remedies*

The Government can also have contractual remedies where contractors violate cybersecurity requirements. For instance, agencies may be able to terminate contracts for default and pursue damages through the contract disputes process where there is a contractual breach.[71] Agencies may also be able to initiate suspension or debarment proceedings in accordance with FAR Subpart 9.4 under some circumstances.

## Key Takeaways

*Preparing for CMMC Compliance*: Current and prospective DoD contractors that have not yet achieved the CMMC level(s) that they anticipate will apply to the types of contracts they hold (or seek to hold) should immediately work to achieve those CMMC levels. As noted above, contractors must be CMMC-compliant by the time of award, but offerors should aim to be CMMC-compliant as early in the procurement process as possible (and preferably before proposal submission) because it is impossible for offerors to predict with certainty how long it will take for DoD to make an award decision in a particular procurement. For CMMC Level 2, contractors should assume they will need a C3PAO certification assessment (potentially even during CMMC Phase 1) because, as explained above, DoD anticipates only 2% of

 

contractors will need a CMMC Level 2 self-assessment but anticipates 35% of contractors will require a CMMC Level 2 C3PAO certification assessment (the remaining will require CMMC Level 1 or CMMC Level 3).[72] Offerors could face challenges trying to become compliant on a compressed timeline if they are racing against an unknown award clock. Contractors that are concerned about their ability to meet CMMC requirements based on their current information technology (IT) environments should consider engaging CMMC-compliant ESPs to handle CUI that cannot be stored, processed, or transmitted using the contractors' own information systems. Using ESPs can streamline—but will not eliminate—CMMC compliance requirements.

*Information Security Compliance Programs*: Contractors should create holistic information security compliance programs. Those programs should address employee and supplier obligations for identifying, safeguarding, and handling CUI; training requirements; monitoring and assessing compliance; and reporting obligations. While implementing applicable security controls is important (and required), those security controls are only effective if contractors ensure that personnel understand their obligations and follow applicable requirements (*e.g.,*avoiding CUI spillage). Additionally, with the onset of CMMC, contractors should include within their compliance programs ways to ensure they maintain continuous compliance and, in turn, can make the required annual affirmations.

*Mergers and Acquisitions*: Recent DOJ settlements underscore the importance of accounting for cybersecurity compliance in mergers and acquisitions. For instance, in May 2025, Raytheon and Nightwing settled allegations that a former Raytheon entity, which Nightwing acquired, failed to comply with cybersecurity requirements, including by failing to implement the requirements specified in NIST SP 800-171 and FAR 52.204-21, as well as failing to have an SSP, for $8.4 million.[73] Nightwing was a successor in liability as to the claims against Raytheon and agreed to the settlement even though the facts at issue occurred before the acquisition. That settlement is a reminder that buyers looking to acquire or merge with Government contractors should assess information security compliance risks. Pre-close diligence should assess past, current, and prospective compliance. Buyers should mitigate risks through, among other things, robust representations and warranties, insurance, indemnities, holdbacks, and remedial actions or disclosures, as appropriate. Buyers should also consider how they plan to integrate the target post-close, including managing IT environments. Buyers and sellers also should consider and negotiate the allocation of these risks in the purchase agreement and, if applicable, any post-closing transition services agreements.

*Supply Chain Management*: As explained above, prime contractors and higher tier subcontractors must flow down CMMC (and other information security) requirements to subcontractors that will store, process, or transmit FCI or CUI on their unclassified contractor information systems. DoD has stated that "[p]rime contractors are expected to work with their suppliers to conduct verifications as they would for any other clause requirement that flows down to subcontractors."[74] It goes on to state that the "prime contractor's responsibility is to flow down CMMC assessment requirements. . .and to not disseminate FCI or CUI to subcontractors that have not indicated they meet the CMMC level. . .for the type of information to be shared."[75]

*Subcontract Negotiations*: Prime contractors and subcontractors should ensure that subcontracts include effective protections to mitigate compliance risks. For instance, prime contractors should consider indemnification and other provisions to mitigate against risks of subcontractor misrepresentations regarding cybersecurity compliance. On the other hand, subcontractors that do not intend to store, process, or transmit FCI or CUI on their systems should consider including provisions that require prime contractors to assume the burden of identifying FCI or CUI and the risks of transferring FCI or CUI to the subcontractor without prior notice and a mutually agreed plan for complying with CMMC requirements.

## Guidelines

These *Guidelines* are intended to assist you in understanding CMMC. They do not, however, constitute legal advice and are not a substitute for professional representation in any specific situation.

**1.** Current and prospective DoD contractors that have not achieved the CMMC levels they anticipate needing to meet in order to compete in DoD procurements must work expeditiously to come into compliance. Those that

 

are not compliant may find themselves ineligible for contract award.

**2.** POAMs can still be a helpful tool for contractors when working toward a Conditional CMMC Level 2 or Conditional CMMC Level 3 status, but remember that POAMs must be closed out within 180 days of the conditional status.

**3.** Contractors that anticipate requiring CMMC Level 2 because they store, process, or transmit CUI on their unclassified information systems should assume they will need CMMC Level 2 C3PAO certification assessments rather than self-assessments. As noted above, the DFARS Rule anticipates that only 2% of contractors will be able to use CMMC Level 2 self-assessments.

**4.** Proper scoping is critical to planning for CMMC assessments. Contractors need to accurately identify which systems will store FCI and which systems will store CUI and develop processes and procedures to avoid spillage onto out-of-scope information systems.

**5.** ESPs can be important partners for achieving CMMC compliance, but choose ESPs wisely. That means finding ESPs that are themselves compliant with applicable security controls and, in the case of CSPs, consider using CSPs with FedRAMP Moderate authorizations if possible.

**6.** Supply chain compliance is critical. DFARS 252.204-7021 requires contractors to "ensure that the subcontractor has a current CMMC certificate or current CMMC status" at the appropriate level. Prime contractors and higher tier subcontractors should structure subcontracts to address risks of lower tier subcontractor noncompliance and restrict further subcontracting opportunities unless lower tier subcontractors first verify CMMC compliance in accordance with DFARS 252.204-7021.

**7.** Contractors should create robust, holistic compliance programs to develop appropriate policies and procedures, educate employees on their responsibilities to properly handle and safeguard FCI and CUI, and ensure compliance monitoring.

**8.** Companies looking to acquire or merge with Government contractors must assess the target's information security compliance, including the extent to which the target has implemented applicable security controls. That includes evaluating a target's compliance with CMMC requirements.

**ENDNOTES:**

[1]81 Fed. Reg. 30439 (May 16, 2016).

[2]FAR 4.1903; see FAR 4.1902.

[3]FAR 52.204-21(a).

[4]81 Fed. Reg. at 30441 ("The intent is that the scope and applicability of this rule be very broad, because this rule requires only the most basic level of safeguarding. . ..The focus of the final rule is shifted from the safeguarding of specific information to the basic safeguarding of certain contractor information systems. Therefore, it is not necessary to draw a fine line as to what information was 'generated for the Government,' when the information is received, or whether the information is marked.").

[5]FAR 52.204-21(b)(1).

[6]78 Fed. Reg. 69273 (Nov. 18, 2013).

[7]DFARS 252.204-7012 defines CDI as CUI that 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." DFARS 252.204-7012(a).

[8]DFARS 252.204-7012(b).

[9]DFARS 252.204-7012(b)(2)(i).

[10]See Class Deviation 2024-O0013, Revision 1—Safeguarding Covered Defense Information and Cyber Incident Reporting (May 24, 2024), https://www.acq.osd.mil/dpap/policy/policyvault/USA001074-24-DPC.pdf.

[11]DFARS 252.204-7012(b)(2)(ii)(D).

[12]DFARS 252.204-7012(c).

[13]85 Fed. Reg. 61505 (Sept. 29, 2020).

[14]DFARS 252.204-7020(a).

[15]DFARS 252.204-7020(a).

[16]DFARS 252.204-7020(a).

[17]DFARS 252.204-7019(b) ("In order to be considered for award, if the Offeror is required to implement NIST SP 800-171, the Offeror shall have a current assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) (see 252.204-7020) for each covered contractor information system that is relevant to the offer, contract, task order, or delivery order.").

[18]89 Fed. Reg. 83092 (Oct. 15, 2024).

[19]90 Fed. Reg. 43560 (Sept. 10, 2025).

[20]32 C.F.R. § 170.3(a).

[21]See 32 C.F.R. § 170.4(b) (definition of "Organization Seeking Assessment").

[22]See 32 C.F.R. § 170.4(b) (definition of "Cloud Service Provider").

[23]32 C.F.R. § 170.15(a)(1).

[24]See 32 C.F.R. § 170.21(a)(2).

[25]32 C.F.R. § 170.21(b).

[26]32 C.F.R. § 170.16.

[27]32 C.F.R. § 170.17; see 32 C.F.R. § 170.4(b) (definition of "CMMC Third-Party Assessment Organizations").

[28]See 32 C.F.R. § 170.4(b) (definition of "Affirming Official").

[29]32 C.F.R. § 170.22.

[30]90 Fed. Reg. 43560, 43573 (Sept. 10, 2025).

[31]32 C.F.R. § 170.18.

[32]32 C.F.R. § 170.21(a)(3).

[33]32 C.F.R. § 170.21(b).

[34]32 C.F.R. § 170.21(b).

[35]32 C.F.R. § 170.18(a)(1).

[36]32 C.F.R. § 170.22.

[37]32 C.F.R. §§ 170.15(a)(1), 17.16(a)(1).

[38]32 C.F.R. § 170.17(a)(1).

[39]32 C.F.R. § 170.18(a)(1).

[40]32 C.F.R. § 170.19(b).

[41]32 C.F.R. § 170.19(c).

[42]32 C.F.R. § 170.19(c).

[43]32 C.F.R. § 170.19(c).

[44]32 C.F.R. § 170.19(c).

[45]32 C.F.R. § 170.19(c).

[46]32 C.F.R. § 170.19(d).

[47]32 C.F.R. § 170.19(d).

[48]89 Fed. Reg. 83092, 83139 (Oct. 15, 2024).

[49]89 Fed. Reg. at 83139.

[50] https://dodcio.defense.gov/Portals/0/Documents/Library/FEDRAMP-EquivalencyCloudServiceProviders.pdf.

[51]32 C.F.R. § 170.3(e).

[52]32 C.F.R. § 170.3(e)(1).

[53]32 C.F.R. § 170.3(e)(2).

[54]32 C.F.R. § 170.3(e)(3).

[55]32 C.F.R. § 170.3(e)(4).

[56]90 Fed. Reg. 43560, 43566 (Sept. 10, 2025).

[57]Am. Justice Sols., Inc., dba CorrectiveSolutions, B-417171.2, Aug. 16, 2019, 2019 CPD ¶ 291, 2019 WL 3889528.

[58]Am. Fuel Cell & Coated Fabrics Co., B-420551, B-420551.2, June 2, 2022, 2022 CPD ¶ 139, 2022 WL 2116235 (holding that noncompliance with DFARS 252.204-7019 and DFARS 252.204-7020 is disqualifying, but dismissing the protest for lack of standing because protester did not show it would be in line for award).

[59]88 Fed. Reg, 17336 (Mar. 22, 2023).

[60]DFARS 252.204-7024(b), (d).

[61]SMS Data Prods. Grp. Inc., B-423197, B-432197.4, Mar. 4, 2025, 2025 CPD ¶ 64, 2025 WL 831119 (sustaining protest where agency failed to assess risks in violation of DFARS 252.204-7024).

[62]Pitney Bowes, Inc., B-422528, May 23, 2024, 2024 CPD ¶ 123, 2024 WL 2801536.

[63]31 U.S.C.A. § 3729 et seq.

[64]31 U.S.C.A. § 3729(a)(1)(A).

[65]31 U.S.C.A. § 3730(b).

[66]See United States ex rel. Polansky v. Exec. Health Res., Inc., 599 U.S. 419, 449 (2023), 65 GC ¶ 181 (Thomas, J. dissenting) ("[t]here are substantial arguments that the qui tam device is inconsistent with Article II and that private relators may not represent the interests of the United States in litigation"); United States ex rel. Montcrief v. Peripheral Vascular Assocs., P.A., 133 F.4th 395, 410 (5th Cir. 2025) (questioning constitutionality of FCA's qui tam provisions) (Duncan, J. concurring); United States ex rel. Zafirov v. Fla. Med. Assocs., LLC, 751 F. Supp. 3d 1293 (M.D. Fla. 2024), 66 GC ¶ 273 (holding qui tam provisions unconstitutional), appeal pending, Docket No. 24-13581 (11th Cir.).

[67]31 U.S.C.A. § 3733.

[68]DOJ Press Release, Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative (Oct. 6, 2021), https://www.justice.gov/archives/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative.

[69]Id.

[70]See, e.g., DOJ Press Release, Raytheon Companies and Nightwing Group To Pay $8.4M To Resolve False Claims Act Allegations Relating to Non-Compliance With Cybersecurity Requirements in Federal Contracts (May 1, 2025), https://www.justice.gov/opa/pr/raytheon-companies-and-nightwing-group-pay-84m-resolve-false-claims-act-allegations-relating.

[71]See, e.g., Arcade Travel, Inc. d/b/a Boersma Travel Servs., ASBCA No, 62009, 20-1 BCA ¶ 37,641, 2020 WL 4379241.

[72]90 Fed. Reg. 43560, 43573 (Sept. 10, 2025).

[73]DOJ Press Release, Raytheon Companies and

Nightwing Group To Pay $8.4M To Resolve False Claims Act Allegations Relating to Non-Compliance With Cybersecurity Requirements in Federal Contracts (May 1, 2025), https://www.justice.gov/opa/pr/raytheon-companies-and-nightwing-group-pay-84m-resolve-false-claims-act-allegations-relating.

[74]90 Fed. Reg. at 43566.

[75]90 Fed. Reg. at 43566.

# NOTES:

# BRIEFING PAPERS