COVINGTON

Cybersecurity Maturity Model Certification ("CMMC") Program Final Rule Announced

October 23, 2024

Government Contracts, Data Privacy & Cybersecurity

On October 15, 2024, the U.S. Department of Defense ("DoD") released the final Cybersecurity Maturity Model Certification ("CMMC") Program Rule ("the Rule"). The Rule formally establishes the CMMC Program for DoD and will solidify CMMC as the governing program for imposing and enforcing safeguarding requirements on DoD contractors for Federal Contract Information ("FCI") and Controlled Unclassified Information ("CUI"). It is one of two complementary sets of regulations that, in combination, will govern operation of the Program and will impose new assessment and affirmation processes for all contractors to be eligible for certain contracts with DoD. The Rule will become effective December 16, 2024, sixty days after publication. Once the related Defense Federal Acquisition Regulation Supplement ("DFARS") rule is implemented, the CMMC Program will likely have a significant impact on defense contractors and subcontractors storing, processing, or transmitting FCI or CUI.

The Rule has been a long time in the making. We have been advising clients on DoD safeguarding rules since 2013 and specifically about CMMC since it was introduced by DoD in 2019. For background on CMMC leading up to the issuance of the Rule, you can reference our first blog post on CMMC in July 2019 and our updates, including for Version 0.4, Version 0.6, Version 0.7, and Version 1.0. For specific background on Version 2.0, you can reference our initial blog post when it was announced and subsequent updates (here and here).

This client alert 1) provides an overview of the Rule, 2) background on the history of the Rule, 3) a walkthrough of the CMMC Program, 4) an overview of the Rule's phased implementation, and 5) a discussion on key takeaways for the Rule. A table summarizing the CMMC Program is also included at the end of this client alert.

Overview of the Final CMMC Program Rule and the Proposed CMMC DFARS Rule

The CMMC Program applies only to DoD contracts that include the appropriate DFARS clause (currently DFARS 252.204–7021)[1] and under which either FCI and/or CUI is processed, stored,

[1] DFARS clause 252.204–7021 provides for the insertion of the CMMC Requirements.

or transmitted on contractor information systems.[2] The Rule will provide DoD with a means to validate that contractor-owned information systems achieve and maintain compliance with security measures necessary to safeguard FCI and CUI and will also impose stricter requirements around implementation of required security controls.

The Rule authorizes DoD to confirm that a defense contractor or subcontractor has implemented and maintains security requirements for a specified CMMC level (Level 1, Level 2, or Level 3) and assessment type (self-assessment, third party assessment, or government assessment) throughout the contract period of performance. The CMMC level required is based on the type of information that will need to be safeguarded during contract performance, and security requirements are specified for each level based on FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems, as well as National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-171 Rev. 2 and NIST SP 800-172.

- CMMC Level 1 requires contractors safeguarding FCI to self-assess and certify compliance.
- CMMC Level 2 applies to contractors safeguarding CUI and requires either a third-party or self-assessment to validate compliance.
- CMMC Level 3 applies to some CUI and requires a Defense Contract Management Agency ("DCMA") Defense Industrial Base Cybersecurity Assessment Center ("DIBCAC")-led assessment.[3]

All contractors must provide affirmation of compliance to help monitor and enforce accountability.

The Rule also outlines limited contractor and subcontractor use of plans of action and milestones ("POA&Ms"), prohibiting POA&Ms for CMMC Level 1 and allowing businesses to obtain conditional certification for 180 days for some controls while working to meet NIST standards for CMMC Levels 2 and 3. The Rule outlines a four-phase implementation over the course of four years.

The Rule reflects updates since publication of the proposed rule on December 26, 2023. Key updates are described in the Program Walkthrough section below.

Separate from this rulemaking, on August 15, 2024, DoD published a proposed procurement rule that complements the Rule. In contrast to the Rule, the proposed procurement rule would

---

[2] FCI is defined under 48 CFR 4.1901 as information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government. CUI is defined in 32 CFR 2002.4(h) as information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls (but does not include classified information).

[3] The DCMA DIBCAC assesses Defense Industrial Base companies to ensure they are meeting contractually required cybersecurity standards and to ensure contractors have the ability to protect CUI for government contracts they are awarded.

outline contract requirements around CMMC and would implement CMMC in the DFARS. When finalized, the procurement rule will require DoD to impose a specific CMMC level in a solicitation or contract. When CMMC requirements are applied to a solicitation through this procurement rule, contracting officers will not make award, exercise an option, or extend the period of performance on a contract if the offeror or contractor does not have the passing results of a current certification assessment or self-assessment for the required CMMC level, and an affirmation of continuous compliance with the security requirements in DoD's Supplier Performance Risk System ("SPRS") for all information systems that process, store, or transmit FCI or CUI during contract performance. DoD can impose CMMC requirements on contracts awarded before the proposed procurement rule is finalized, but that would be done on a contract-by-contract basis. We addressed this proposed procurement rule in a prior blog.

More details on key areas of the Rule are outlined below.

Background on the Final CMMC Program Rule

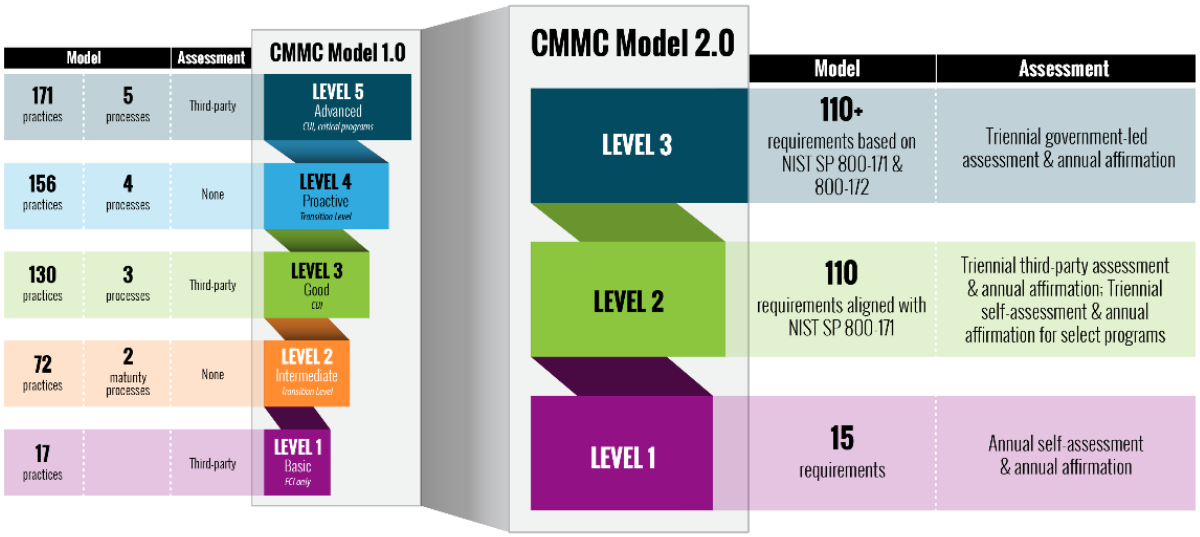
In 2016, DoD amended the DFARS to add a clause, DFARS 252.204-7012, requiring DoD contractors to report cyber incidents and to safeguard certain DoD CUI (though under the DFARS clause, CUI that requires safeguarding is referred to as covered defense information or CDI) in accordance with the 110 security controls identified in NIST SP 800-171. Four years later, DoD announced CMMC 1.0 and issued an interim rule that addressed the initial vision for CMMC. This initial rule envisioned a five-year phase in period and included five levels of safeguarding requirements. DoD received approximately 750 comments on this rule and as a result DoD conducted an internal review of CMMC. Comments focused on concerns related to the cost of CMMC Third Party Assessment Organization ("C3PAO")[4] certification requirements, the cost and challenges of implementing required process maturity and 20 additional cybersecurity practices, and the impact of the rule on small businesses.

In November 2021, DoD announced CMMC 2.0, which is reflected in the Rule, outlining an updated program structure and requirements. We previously wrote about CMMC 2.0 here and here. According to DoD, key features and major improvements from the first version of the proposed rule, reflected in the Rule include:

1. Three tiers or assessment levels (down from five levels) to simplify the process for small- and medium-sized businesses;
2. The use of NIST cybersecurity standards to align with widely accepted standards;
3. Ability of all contractors at Level 1 and a subset of contractors at Level 2 to demonstrate compliance through self-assessments to reduce costs;
4. Increased oversight of third-party assessors to improve accountability;
5. Additional guidelines for, and allowing for use of, POA&Ms in limited circumstances to promote collaboration; and

[4] A C3PAO is a contracted organization authorized by the CMMC Accreditation Body to conduct assessments under the CMMC Program.

6. Flexibility for the government to waive inclusion of CMMC requirements under limited circumstances.



This graphic is from the DoD CIO website, outlining key features of the Rule and updates from the earlier version 1.0 of the CMMC rule.

In December 2023, DoD published a proposed rule to amend 32 CFR part 170, implementing the revised CMMC Program with a comment period that ended on February 26, 2024. After some additional updates to the proposed CMMC Program rule, DoD published the revised final Rule October 15, 2024. As discussed above, the CMMC requirements in the Rule will be implemented in the DFARS through the proposed procurement rule once it becomes final. Prior to the proposed procurement rule being finalized, DoD could add CMMC requirements on a contract-by-contract basis.

Program Walkthrough

Once the CMMC Program is implemented, a DoD solicitation will specify the minimum CMMC status required for a contractor to be eligible for the award. The program manager will identify the status applied to a procurement based on a variety of factors, including criticality of the associated mission capability, type of acquisition program or technology, threat of loss of the information, and impacts from exploitation of information security deficiencies. In some very limited instances, a DoD Service Acquisition Executive or a Component Acquisition Executive may choose to waive inclusion of CMMC Program requirements.

To be eligible for an award, a contractor must adhere to the appropriate requirements and obtain certification for the minimum CMMC level in accordance with the solicitation. The Rule requires contractors to identify the information systems that will process, store, or transmit FCI and/or CUI and other relevant assets that may be in scope for CMMC assessment requirements. This includes information systems provided by External Service Providers

("ESPs") and Cloud Service Providers ("CSPs").[5] The Rule categorizes the assets into the following categories to determine systems and assets in scope and the corresponding CMMC requirements for each contractor:

1. Assets[6] that process, store, or transmit FCI and/or CUI;
2. Contractor Risk Managed Assets (i.e., assets that can but are not intended to process, store, or transmit CUI), which may, for example, include a laptop or email system that can be used to access an environment where CUI is stored but is restricted;
3. Security Protection Assets (i.e., assets that provide security functions or capabilities), which may include, for example, intrusion detection systems and vulnerability scanners; and
4. Specialized Assets (i.e., assets that can process, store, or transmit CUI but cannot be fully secured), which may include Internet of Things devices, Industrial Internet of Things devices, Government Furnished Equipment, Operational Technology, Restricted Information Systems, and Test Equipment.

Other scoping considerations apply for ESPs and CSPs, discussed further below. See our prior alert on DoD issuing the proposed rule implementing CMMC, § 170.19 of the Rule, supporting guidance documents for additional details on CMMC Scoping, and CMMC Program FAQs for further information regarding ESPs and CSPs and their relationships to contractors.

Level 1 (Self): Level 1 involves the securing of FCI processed, stored, or transmitted during the course of performing a contract. Contractors must comply with 17 requirements in NIST SP 800-171 Rev. 2 (which map to 15 controls required by FAR 52.204-21), with no exceptions or POA&Ms permitted. Contractors must verify through an annual self-assessment that all requirements have been fully implemented and submit an affirmation in SPRS attesting that they have implemented and will maintain implementation of all applicable CMMC security requirements in their CMMC level for all information systems within the relevant CMMC assessment scope ("affirmation of continuous compliance"). DoD clarified the Level 1 Scoping Guide to state that there are no explicit documentation requirements for a CMMC Level 1 self-assessment. Nonetheless, contractors may be well served to document their actions that demonstrate compliance given the need to enter compliance status into SPRS and maintain the

[5] The CMMC Program Rule defines ESPs as external people, technology, or facilities that an organization utilizes for provision and management of IT and/or cybersecurity services on behalf of the organization. In the CMMC Program, CUI or Security Protection Data (e.g., log data, configuration data), must be processed, stored, or transmitted on the ESP assets to be considered an ESP. CSPs, also addressed in the Rule, are external companies that provide cloud services based on cloud computing. Different requirements apply for ESPs that are CSPs and ESPs that are not CSPs, discussed further below.
[6] The Final CMMC Program Rule defines an "Asset" as an item of value to stakeholders, which may include physical items such as hardware, firmware, computing platform, network device, or other technology component, or intangibles such as data, information, software, services, or intellectual property.

status thereafter. All assessments under the Rule must adhere to the Scoring Methodology outlined in § 170.24.

Level 2 (Self or C3PAO): CMMC Level 2 requirements apply to contracts involving the securing of CUI processed, stored, or transmitted on the contractor system or a third party cloud system (relevant Security Protection Assets, Contractor Risk Managed Assets, and Specialized Assets may also be in scope, and the presence of any CUI (CDI under the DFARS 7012 rule) on an information system would trigger the requirement for that system to meet the Level 2 assessment/certification requirements). Contractors must meet the 110 security controls in NIST SP 800-171. For some contracts, a self-assessment is sufficient; other contracts will require an assessment by an authorized or accredited C3PAO. Contractors can retain a C3PAO listed on the CMMC Accreditation Body ("AB")[7] Marketplace.

Although DoD requires contractors to have "MET" all the security controls, both scenarios permit some controls that are not fully implemented, which the Rule defines as "NOT MET" requirements, to be subject to POA&Ms. If the contractor achieves the minimum score of 80% on the assessment (as set forth in the CMMC Scoring Methodology) and meets the five critical security controls that cannot be included on a POA&M (AC.L.2-3.1.20, AC.L2–3.1.22; CA.L2–3.12.4; PE.L2–3.10.3; PE.L2–3.10.4; PE.L2–3.10.5), then the contractor is rated at CMMC Conditional Level 2 Status, so long as all the NOT MET requirements are included on a POA&M. The contractor must remedy NOT MET requirements listed on the POA&M within 180 days to achieve compliance. If the contractor has Conditional CMMC Status, the contractor or C3PAO, as applicable, must conduct a second assessment to verify all NOT MET requirements have been fully remediated by the end of 180 days for the contractor to achieve final CMMC Level 2 Status, or the contractor will be considered in breach of the current contract.

After achieving conditional or final compliance, the contractor must submit an affirmation of continuing compliance in SPRS. Contractors must reaffirm continuing compliance with Level 2 Status annually, but only need to conduct a new assessment every three years. Contractors will need to consider what they need to do short of a full assessment to permit that affirmation of continuing compliance.

Contractors with Level 2 Status are also eligible for contracts subject to Level 1 Status.

The Rule also clarifies requirements for contractor use of ESPs (both for ESPs that are CSPs and those that are not ESPs) to achieve compliance with Level 2 Status.

- CSPs: Contractors may use a CSP to process, store, or transmit CUI in performance of a contract with a CMMC Level 2 Status requirement if the product/service is FedRAMP

[7] The CMMC AB is the one organization DoD contracts with to authorize and accredit organizations assessing and certifying contractor compliance (C3PAO) with CMMC requirements.

Authorized at the FedRAMP Moderate or higher baseline or meets equivalent security requirements.[8]

- ESPs that are not CSPs: A contractor may use a CSP to process, store, or transmit CUI in performance of a contract with a CMMC Level 2 Status requirement if information about the ESP is properly documented in accordance with §§ 170.16, 170.17 and the ESP services used to meet contractor requirements (i.e., in scope) are included in the contractor's Level 2 assessment.

Above is a summary of requirements; see additional details at §§ 170.16, 170.17, 170.19.

Level 3 (DIBCAC): Level 3 also involves the securing of CUI processed, stored, or transmitted in the course of performing on a contract, on the contractor's information system, or on third party cloud systems, but under Level 3 Status, DoD program offices consider the information to be especially sensitive and requiring heightened protections against advanced persistent threats (relevant Security Protection Assets and Specialized Assets may also be in scope). The DIBCAC conducts CMMC Level 3 assessments. Contractors must obtain a CMMC Level 2 Final Certification Assessment for information systems within the Level 3 CMMC Assessment Scope as a prerequisite for a CMMC Level 3 Certification Assessment. In addition to the Level 2 requirements, contractors must meet 24 additional security requirements from NIST SP 800-172 "Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST SP 800-171, Rev. 2." If contractors are able to implement 80% of 24 requirements and the seven critical requirements are met (IR.L3–3.6.1e; IR.L3–3.6.2e; RA.L3–3.11.1e; RA.L3–3.11.6e; RA.L3–3.11.7e; RA.L3–3.11.4e; SI.L3–3.14.3e), contractors will obtain a CMMC Status of Conditional Level 3 (DIBCAC). All NOT MET requirements must be noted on the POA&M and remedied within 180 days to achieve final CMMC Level 3 Status. Although DIBCAC will focus on the 24 requirements, it may also perform limited checks on the 110 requirements from NIST SP 800-171. DIBCAC's assessment will take precedence over other assessment determinations for CMMC Level 2 requirements.

DIBCAC submits assessment results into the Enterprise Mission Assurance Support Service ("eMASS") for CMMC, which then provides automated transmission to SPRS. Contractors must submit an affirmation of continuing compliance into SPRS after achieving Conditional and Final Level 3 Status. To maintain Level 3 Status, contractors must also obtain Level 2 and Level 3 Certification Assessments every three years.

Contractors with Level 3 Status are also eligible for contracts subject to Level 1 and Level 2 Statuses.

[8] FedRAMP, or Federal Risk and Authorization Management Program, is a government program that promotes the adaptation of secure cloud services across the federal government through standardized approaches for executive agency cloud deployments and service models at low, moderate, and high-risk impact levels.

The Rule also clarifies requirements for contractor use of ESPs (both for ESPs that are CSPs and those that are not ESPs) for Level 3 Status.

- CSPs: Contractors may use a CSP to process, store, or transmit CUI in performance of a contract with a CMMC Level 3 Status requirement if the product/service is FedRAMP Authorized at the FedRAMP Moderate or higher baseline or meets equivalent security requirements. Even with use of a CSP, the 24 requirements still apply to all in-scope assets. Additional specifications are outlined at § 170.18.
- ESPs that are not CSPs: A contractor may use an ESP that is not a CSP to process, store, or transmit CUI in performance of a contract with a CMMC Level 3 Status requirement if information about the ESP is properly documented in accordance with § 170.18, and the ESP services used to meet contractor requirements (i.e., in scope) are included in the contractor's Level 2 and Level 3 assessment.

Above is a summary of requirements; see additional details on requirements at §§ 170.18, 170.19.

Flow Down to Subcontractors

CMMC Level requirements apply to subcontractors throughout the contractor's supply chain if they process, store, or transmit FCI or CUI on their contractor information systems in the performance of a government subcontract. Prime contractors are responsible for flowing down CMMC compliance requirements to subcontractors in accordance with the solicitation and resulting contract based on the sensitivity of the information flowed down to each subcontractor. DoD clarified that prime contractors will not be granted access to subcontractor accreditation information in SPRS and must confirm status with prospective subcontractors "early and often"; thus, the onus is on the contractor to follow flow down requirements outlined in § 170.23. (DFARS clause 252.204-7012 also requires defense contractors to include flow down requirements in relevant subcontracts.)

Most Recent Updates to the Final Rule

While the Rule did not change significantly since DoD published the proposed rule in December 2023, DoD made several key updates in response to some of the 361 public submissions received during the comment period between December 2023 and February 2024. Examples include:

1. Extending the implementation timeline (i.e., adding six months to Phase 1, with appropriate adjustments to later phases);
2. Expanding rules for contracting organizations that provide oversight and assessments under the CMMC Program to mitigate conflicts of interest and require reporting of adverse information;
3. Reducing assessment requirements for ESPs;
4. Narrowing the definition of a CSP and aligning it with NIST SP 800-145 Sept. 2011;
5. Reducing assessment requirements for certain types of information assets (i.e., Security Protection Assets and Security Protection Data); and

6. Clarifying the responsibility of DIBCAC in assessing contractor compliance, including clarifying that DIBCAC can perform limited checks on Level 2 requirements.

The Rule includes a full list of changes here. In addition, we have provided a detailed chart of the CMMC Program below.

Phased Implementation

DoD will implement the CMMC Program in four phases. Over a four-year period, CMMC level requirements will be incrementally added to solicitations, ending with full implementation of requirements in Phase 4. According to DoD, the phased implementation will help minimize financial impacts on contractors, allow contractors time to understand and implement CMMC requirements, provide time to train assessors, and limit disruptions on the supply chain. Information on each phase is provided in the table below. Additional details for each phase are addressed in § 170.3(e).

Phase	Requirement	Effective Date
1	▪ Solicitations and contracts include Level 1 or Level 2 self-assessment requirements as condition of contract award ▪ DoD may include Level 2 third party assessments (C3PAO) in place of the Level 2 self-assessments (Self) for applicable DoD solicitations and contracts and as a condition to exercise an option period on a contract awarded before the effective date ▪ DoD may include the requirement for Level 2 (C3PAO) in place of Level 2 (Self) for applicable DoD solicitations and contracts	Effective date of Final Procurement Rule (48 CFR Part 204 Acquisition Final Rule)[9]
2	▪ Solicitations and contracts include Level 2 (C3PAO) as a condition of contract award ▪ DoD may delay inclusion of requirement for Level 2 (C3PAO) to an option period instead of as a condition of contract award ▪ DoD may include requirement for Level 3 (DIBCAC) for applicable solicitations and contracts	One calendar year after start of Phase 1

[9] The final procurement rule implementing the Rule is forthcoming, so the date is unknown. However, prior to the effective date, DoD may, at its discretion, include the requirement for CMMC Status of Level 1 or Level 2 (Self) for applicable DoD solicitations and contracts as a condition to exercise an option period on a contract awarded before the effective date.

3	▪ Solicitations and contracts include the requirement for Level 2 (C3PAO) as a condition of contract award and as a condition to exercise an option period on a contract awarded after the effective date ▪ All applicable DoD solicitations and contracts include the requirement for Level 3 (DIBCAC) as a condition of contract award ▪ DoD may delay the inclusion of requirement for Level 3 (DIBCAC) to an option period instead of as a condition of contract award	One calendar year after start of Phase 2
4	▪ DoD will include CMMC requirements in all applicable DoD solicitations and contracts (including option periods in contracts awarded prior to Phase 4)	One calendar year after start of Phase 3

Key Takeaways and Impact

The CMMC Program will likely have a significant impact on defense contractors and subcontractors once implemented where their performance requires them to store, process, or transmit FCI or CUI. Although CMMC Program requirements track closely with existing NIST standards and existing FAR and DFARS requirements, the CMMC Program, once fully implemented, will impose new assessment and affirmation processes for all contractors to be eligible for certain DoD contracts. For example, DoD estimates 8,350 medium and large entities will be required to meet CMMC Level 2 C3PAO assessment requirements as a condition of contract award. DoD further estimates that 4,452 C3PAO Certification Assessments will be completed in year four.

The level of effort to become compliant could be significant depending on the scale of a contractor's covered systems and the maturity of its cybersecurity program and capabilities. If not already underway, contractors should consider inventorying their covered systems relative to the CMMC Program to define their in-scope assets, assessing any internal and external services on which they currently rely, assessing their cybersecurity program for gaps with current requirements, identifying reasonable timeframes for addressing those gaps, and budgeting to become and maintain compliance with the desired CMMC Level. Additionally, DoD contractors should begin to closely assess their supply chains given that some subcontractors or service providers may be unable or unwilling to meet these requirements.

* * *

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Government Contracts and Data Privacy & Cybersecurity practices:

Ryan Burnette	+1 202 662 5746	rburnette@cov.com
Susan Cassidy	+1 202 662 5348	scassidy@cov.com
Krissy Chapman	+1 202 662 5764	kchapman@cov.com
Moriah Daugherty	+1 202 662 5718	mdaugherty@cov.com
Ashden Fein	+1 202 662 5116	afein@cov.com
Bob Huffman	+1 202 662 5645	rhuffman@cov.com
Micaela McMurrough	+1 212 841 1242	mmcmurrough@cov.com
Darby Rourick	+1 202 662 5455	drourick@cov.com
Caleb Skeath	+1 202 662 5119	cskeath@cov.com

Summary of the CMMC Program Final Rule

The table below includes a summary of the Rule based on the requirements at each CMMC Level. Changes based on an increase in CMMC Level or type of assessment within a CMMC Level are noted in blue.

CMMC Level	Scope	Summary of Requirements	Assessment Requirement	POA&M	Affirmation Requirements
1 – Self	Processing, storing, or transmitting of FCI	17 requirements in NIST SP 800-171 R2 (which map to 15 required by FAR 52.204-21)	Self-assessment annually Results entered into SPRS (or successor)	None permitted	After each assessment Entered into SPRS (or successor)
2 – Self	Processing, storing, or transmitting of CUI (and as relevant Security Protection Assets, Contractor Risk Managed Assets, Specialized Assets) Other scoping considerations apply for ESPs *DoD determines the assessment type (i.e., Level 2 (Self) or Level 2 (C3PAO) based on the type and sensitivity of information and safeguarding needed*	110 NIST SP 800-171 R2 required by DFARS 252.204-7012	Self-assessment every 3 years Results entered into SPRS (or successor) CMMC Status valid for 3 years	Permitted as defined in § 170.21(a)(2) Closed out within 180 days of initial assessment Final status valid for 3 years from Conditional Status Date	After each assessment and annually thereafter; failure to affirm annually results in lapse Entered into SPRS (or successor)

2 – C3PAO	Processing, storing, or transmitting of CUI (and as relevant Security Protection Assets, Contractor Risk Managed Assets, Specialized Assets) Other scoping considerations apply for ESPs *DoD determines the assessment type (i.e., Level 2 (Self) or Level 2 (C3PAO) based on the type and sensitivity of information and safeguarding needed*	110 NIST SP 800-171 R2 required by DFARS 252.204-7012	Conducted by C3PAO every 3 years Results entered into eMASS (or successor) CMMC Status valid for 3 years	Permitted as defined in § 170.21(a)(2) Closed out within 180 days of initial assessment Final status valid for 3 years from Conditional Status Date	After each assessment and annually thereafter; failure to affirm annually results in lapse Entered into SPRS (or successor)
3 – DIBCAC	Processing, storing, or transmitting of CUI (and as relevant Security Protection Assets and Specialized Assets) Other scoping considerations apply for ESPs	110 NIST SP 800-171 R2 required by DFARS 252.204-7012 24 controls selected from NIST SP 800-172 Feb2021	Pre-requisite CMMC Status of Level 2 (C3PAO) for the same CMMC Assessment Scope, for each Level 3 certification assessment Conducted by DIBCAC every 3 years Results entered into eMASS (or successor) CMMC Status valid for 3 years	Permitted as defined in § 170.21(a)(3) Closed out within 180 days of initial assessment Final status valid for 3 years from Conditional Status Date	After each assessment and annually thereafter; failure to affirm annually results in lapse Level 2 (C3PAO) affirmation must also continue to be completed annually Entered into SPRS (or successor)

[See also Table 1—CMMC Level and Assessment Requirements in the Rule.]