# Contents

## 1. Service Providers

Comment 1: Multiple commenters asked about applicability of the CMMC Program to a variety of service providers. One commenter requested clarification regarding how CUI controls apply to Internet Service Providers and their globally sourced service support because of the prohibition of foreign dissemination for CUI. Two commenters suggested that common carrier telecommunications (often termed as Plain-Old-Telephone-Services (POTS)) and similar commercial services (cloud services, external service providers) should be treated as commercial off-the-shelf (COTS), and so excluded from CMMC certification requirements. One commenter expressed concerns about the impact of the rule on the telecom industry. One commenter recommended that, to limit the burden of CMMC implementation, contractors providing commercial services to support COTS items, such as technical support for software, should receive the same exceptions as other COTS contracts.

***Response:*** The CMMC Program will result in cybersecurity protection and assessment requirements for defense contractors and subcontractors. CMMC Level requirements will apply only if a defense contractor or subcontractor handles FCI or CUI on its own contractor information systems. If so, then under CMMC, the contractor or subcontractor will be required to comply with the cybersecurity protection and assessment requirements associated with the appropriate Level. As such, CMMC Level requirements will not apply to Internet Service Providers or other telecommunications service providers (i.e., common carriers), unless those entities themselves are or intend to become defense contractors or subcontractors. In addition, there is no general prohibition of foreign dissemination for CUI, although certain CUI may be subject to export restrictions. Commercial item determinations per 48 CFR 15, to include those relating to common carrier telecommunications or cloud services, are not defined by CMMC. With respect to the CMMC Assessment Scope, although they provide connectivity for contractor systems, and the common carrier link is within the boundary of the contractor's system, the common carrier's information system is not within the contractor's CMMC Assessment Scope as long as CUI is encrypted during transport across the common carrier's information system.

## 2. Joint Ventures

Comment 2: Multiple commenters asked for clarification on how to handle joint ventures with respect to DFARS clause 252.204-7021.

***Response*:** The CMMC Program requirements proposed in this rule will be implemented in the DFARS, as needed, which may result in changes to current DoD solicitation provisions and contract clauses, including DFARS clause 252.204-7021. As such, DoD cannot address applicability of current DFARS clause 252.204-7021 at this time. With respect to joint ventures, CMMC Program requirements will apply to information systems associated with the contract efforts that process, store, or transmit FCI or CUI, and to any information system that provides security protections for such systems, or information systems not logically or physically isolated from all such systems.

## 3. Internet of Things /Operational Technology

Comment 3: Multiple commenters noted the applicability of the CMMC requirements to Internet of Things (IoT) and Operational Technology (OT) systems were unclear. Several commenters expressed concerns about the impact of the rule on factories and OT.

***Response**:* CMMC security requirements apply to information systems associated with the contract efforts that process, store, or transmit FCI or CUI, and to any information system that provides security protections for such systems; or are not logically or physically isolated from all such systems. In accordance with § 170.19, an OSA's IoT or OT systems located within its Level 1 or Level 2 CMMC Assessment Scope are not assessed; however, for CMMC Level 2 they are required to be documented in the System Security Plan (SSP). When a CMMC Level 2 Certification Assessment is performed as a precursor to a CMMC Level 3 Certification Assessment, the IOT and OT (and all other Specialized Assets) should be assessed against all CMMC Level 2 security requirements as described in § 170.18(a)(1). For CMMC Level 3, an OSC's IoT or OT located within its CMMC Assessment Scope are assessed against all CMMC security requirements unless they are physically or logically isolated. However, for IoT and OT (and all other Specialized Assets), it is permissible to use intermediary devices to provide the capability for the specialized asset to meet CMMC Level 3 security requirements.

## 4. Government Furnished Equipment:

Comment 4: One commenter questioned how the interim rule applies to Government Furnished Equipment (GFE) in a 'test' versus a 'production environment.'

***Response:*** As described in § 170.3, CMMC security requirements will apply to any information system associated with the contract efforts that process, store, or transmit FCI or CUI, and to any information system that provides security protections for such systems; or information systems not logically or physically isolated from all such systems. This includes when a 'Test environment' processes, stores, or transmits FCI or CUI; provides security protections for such systems; or is not logically or physically isolated from such systems. See §170.19 and the response to public comment under the heading 3. Internet of Things /Operational Technology in the Discussion of Comments and Changes section of this preamble for additional details on defining the scope of CMMC assessments.
If GFE cannot be configured to meet all the NIST SP 800-171 Rev 2 requirements or must be maintained in a specified configuration which does not comply with NIST SP 800-171 Rev 2, additional protections such as physical or logical isolation may be used for risk mitigation in accordance with the treatment of Specialized Assets as defined in table 1 to § 170.19(c)(1) CMMC Level 2 Scoping.

## 5. Fundamental Research:

Comment 5: Multiple commenters requested that DoD clarify the application of CMMC requirements to fundamental research. Commenters described adverse consequences of not explicitly exempting fundamental research from the CMMC requirements, noting that institutions of higher education will have to pull out of research agreements with the Department, may no longer accept DoD funds because the resource burden would be cost prohibitive to both the institution and its partners, and the burdens imposed by even CMMC Level 1 requirements would hinder the progress of fundamental research. These commenters also noted that restrictions on posting of public information would inhibit open collaboration and the exchange of ideas that is critical to the advancement of scientific discovery. Commenters also requested that the Department clarify that subcontracts scoped as fundamental research also be exempt from CMMC requirements.

***Response:*** CMMC Program requirements are designed to provide increased assurance to the Department that defense contractors can adequately protect FCI and CUI, in accordance with already applicable regulations and standards. Fundamental research is defined by National Security Defense Directive (NSDD)-189[17] as 'basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons.' CMMC Program requirements apply only to defense contractors and subcontractors who handle FCI and CUI on an information system associated with a contract effort or any information system that provides security protections for such systems, or information systems not logically or physically isolated from all such systems. Fundamental research that is 'shared broadly within the scientific community' is not, by definition, FCI or CUI; however, other research-related information that is provided to or handled by contractors as part of contract performance may be FCI or CUI, thus may trigger application of CMMC Level requirements. If DoD determines the information handled by contractors pursuant to the fundamental research contract activities is or will become FCI or CUI, the information would be required to be processed, stored, or transmitted on an information system compliant with the appropriate CMMC Level.

## 6. International- Foreign DIB Partners / Non-U.S. Contractors

Comment 6: Multiple commenters asked if international subcontractors of a U.S. prime will require CMMC certification. Commenters also asked if there is a strategy for legally implementing CMMC requirements beyond the U.S. DIB, and if an enterprise-level resolution has been developed to address foreign DIB sovereignty. One commenter suggested that some foreign governments have issued guidance to their local companies directing them not to accept CMMC flow down requirements.
One commenter expressed concern regarding the impact of CMMC to existing bilateral/multilateral security agreements. Another commenter asked if the foreign DIB will be

authorized to evaluate U.S. DIB and vice versa. One non-U.S. commenter suggested using the existing Facility Security Clearance process to ensure a company is compliant with CMMC in accordance with national legislation.

***Response***: Contractors are required to comply with all terms and conditions of the contract, to include terms and conditions relating to cybersecurity protections and assessments. In addition, offerors will be required to comply with the pre-award CMMC requirement. This holds true when a contract clause is flowed down to subcontractors. The Facility Security Clearance process does not apply to unclassified information systems owned by, or operated on behalf of, a non-federal entity (e.g., contractors), and, therefore, does not apply to systems/networks that will be subject to CMMC requirements. This rule makes no distinction about which C3PAOs may assess which companies seeking certification. For more details on C3PAO requirements, see § 170.9.

## 7. CUI and FCI

### a. Marking and identifying CUI

Comment 7: Multiple commenters asked for clarification regarding definition, marking, and identification of CUI as related to CMMC requirements and DFARS clause 252.204-7021. One commenter asked if the definition of DoD CUI applies to the CUI required to be safeguarded under the CMMC clause. Another asked if DFARS clause 252.204-7021 includes information that requires protection under DFARS clause 252.204-7012.
One commenter requested that the Department confirm that, under CMMC, contractors will only be responsible for protecting CUI that is clearly marked upon receipt from the Department and created by contractors.

***Response:*** If the contract includes a CMMC Level requirement, contractors will be required to protect FCI and CUI, as applicable, through fulfillment of the designated CMMC Level security requirements. CMMC does not in any way change the DoD requirements regarding the definition, marking, and protection of CUI.
If DFARS clause 252.204-7012 applies, contractors are required to safeguard covered defense information in accordance with the terms and conditions of the clause and contract, which includes information developed in support of the contract. CMMC does not change these requirements.

### b. Relationship of FCI and CUI to the CMMC requirements

Comment 8: One commenter suggested that the inclusion of FCI in CMMC needs significant clarification. Others asked if FCI references within the CMMC Model [1.0] and nonpublic DoD information references in Department of Defense Instruction (DoDI) 8582.01[18] are the same type of information, and if DoDI 8582.01 is the definitive DoD policy for FCI and DoD standards regarding the requirements under FAR clause 52.204-21.

***Response:*** The CMMC Program requirements for Level 1 will apply when the contract effort requires contractors to process, store, or transmit FCI on its unclassified information system. If CUI is processed, stored, or transmitted on a contractor information system, a higher level of CMMC compliance or certification is required. The CMMC Level required to protect CUI (i.e., CMMC Level 2 Self-Assessment as described in § 170.16, CMMC Level 2 Certification Assessment as described in § 170.17, or CMMC Level 3 Certification Assessment as described in § 170.18) is determined by the Department based upon the sensitivity of the CUI and will be identified in the solicitation.
The CMMC Program uses the definitions of FCI from FAR 4.1901 and CUI from 32 CFR 2002, which are the definitive sources for these definitions. DoDI 8582.01, published on December 9, 2019, points to FAR clause 52.204-21 and DFARS clause 252.204-7012, both of which preceded it, to address the safeguarding requirements for FCI and CUI. CMMC builds from those requirements by requiring that defense contractors and subcontractors provide assurance, either with Self-Assessments, Third-Party Assessments, or Level 3 Assessments, as required, that they have implemented the required information protection requirements.

## 8. Small Business/Entities

### a. Assistance/Support for Small Business

Comment 9: Several commenters suggested that in order to successfully implement cybersecurity requirements, contractors require support from the Department. One commenter suggested DoD should perform an analysis of each requirement and ensure that necessary support structures are in place and fully functioning prior to implementing this rule, and that access to tech support/solutions should be provided. Multiple commenters suggested that more support and guidance is needed for small businesses trying to comply with CMMC. One commenter suggested that DoD should relax affiliation rules (in conjunction with the Small Business Association (SBA)) to allow small companies to work together to meet CMMC requirements while spreading the cost over a larger base and expand mentor-protégé agreements for larger businesses to help smaller companies with CMMC appraisals.
One commenter expressed concern for non-traditional, innovative companies that are coming in through the Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) process and asked what DoD is doing to help them become compliant. Another noted that if CMMC Level 1 will be the minimum requirement for SBIRs and STTRs, regardless of whether they include FCI, it may significantly limit the number of universities that can partner with small businesses under these awards.

***Response:*** DoD's Office of Small Business and Technology Partnerships (OSBTP) is working to provide SBIR/STTR programs with support for CMMC implementation through the use of Technical and Business Assistance. The SBA's affiliation rules are codified at 13 CFR 121.103, available at https://www.ecfr.gov/current/title-13/chapter-I/part-121. Any change to the SBA's affiliation rules is outside the scope of this rulemaking.
The CMMC Program is designed to increase assurance that defense contractors do in fact, comply with information protection requirements to adequately protect FCI and CUI. Additional

information to assist contractors regarding DoD's current information security protection requirements may be found in Frequently Asked Questions (FAQs) Regarding the Implementation of DFARS subpart 204.73, published at https://DoDprocurementtoolbox.com/.

## b. Impact of Cost

Comment 10: Multiple commenters commented on the cost impact of CMMC to small businesses, suggesting that the cost to become and remain compliant is too high. Several commenters added that small businesses limited by finances won't be able to compete, which could be detrimental to the supply chain and efforts to meet national defense goals, and that the rule fails to provide any consideration for the future loss of technology acquisition should small businesses be inadvertently precluded from participation. Other commenters suggested that the impact of CMMC will be a profound and significant obstacle to businesses due to their lack of resources as compared to their large business competitors, adding that the requirement to have the same measures in place for any company, regardless of size, incurs a higher percentage of indirect cost for small businesses. Multiple commenters remarked on the limited or lack of options for a small business to recover costs.

***Response:*** The estimated costs attributed to this rule do not include the costs associated with compliance with existing cybersecurity requirements under FAR clause 52.204-21 or associated with implementing NIST SP 800–171 requirements in accordance with DFARS clause 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*. To the extent that defense contractors or subcontractors have already been awarded DoD contracts or subcontracts that include these clauses, and process, store, or transmit FCI or CUI in support of the performance of those contracts, costs for implementing those cybersecurity requirements should have already been incurred and are not attributed to this rule. Those costs are distinct from costs associated with undergoing a CMMC assessment to verify implementation of those security requirements. The CMMC Program does not levy additional information security protection requirements for CMMC Levels 1 and 2. The value of DoD's sensitive information (and impact of its loss to the Department) does not diminish when it moves to contractors – prime or sub, large or small.
A Regulatory Flexibility Analysis was conducted. In comparison to CMMC 1.0, DoD has now eliminated the requirement for organizations to hire a third-party assessment organization to comply with CMMC Level 1. The CMMC Program requirements further address cost concerns by permitting self-assessment at Level 1 and at Level 2 for some contracts that are not designated to require the added assurance of C3PAO assessment.
In addition, resources available through the DoD Office of Small Business Programs (OSBP) may help defray cybersecurity costs by helping companies stay up to date with the latest cybersecurity policies and best practices. The OSBP also partners with the NIST and its Manufacturing Extension Partnership (MEP) programs (https://www.nist.gov/mep), which operate across the U.S. to provide resource and funding assistance options.
The Department currently has no plans for separate reimbursement of costs to acquire cybersecurity capabilities or a required cybersecurity certification that may be incurred by an

offeror on a DoD contract. Costs may be recouped via competitively set prices, as companies see fit.

### c. Alternative Implementation

Comment 11: Multiple commenters requested that the government give small businesses time for CMMC compliance post-contract award. One commenter recommended that DoD consider only requiring government assessment of NIST SP 800-171 compliance (vice private third party) for small businesses, even at lower CMMC assessment levels, thus offsetting a higher burden level to small businesses. Several commenters commented on the need to include exemptions for small businesses that do not possess CUI and have never been contracted by the government. One added that DoD should identify portions of contracts which won't require CMMC so that small businesses are afforded maximum practicable opportunity regardless of their CMMC status.

***Response:*** The DoD has determined that the assessment of the ability of a prospective contactor to adequately protect FCI and CUI that will be processed, stored, or transmitted on information systems during contract performance is a requirement prior to award of any prime contract or subcontract. Failure to assess a prospective contractor's ability to comply with applicable information security protection requirements, such as NIST SP 800-171 Rev 2, risks significant performance delays if information cannot be shared immediately at contract award due to lack of compliance. As applicable, the awardee must be capable of processing, storing, and transmitting FCI and CUI at the start of the performance period, regardless of the business size of the awardee. The CMMC Program has simplified requirements for Level 1 and 2 assessments in some contracts. Specifically, although contractors must still implement and maintain the security requirements set forth in FAR 52.204-21 to protect FCI and set forth in the NIST SP 800-171 Rev 2 to protect CUI, the requirement to hire a third-party assessment organization for CMMC Level 1 was eliminated, and for some contracts, contractors may be permitted to self-assess compliance with CMMC Level 2. Annual affirmations are also required for CMMC Level 1 and 2.

Prospective contractors must make a business decision regarding the type of DoD business they wish to pursue and understand the implications for doing so. If an offeror or current DoD contractor or subcontractor has self-assessed then later decides to pursue a contract or subcontract requiring a certification at CMMC Level 2 or 3, it will need to factor in the time and investment necessary to hire a third-party assessment organization and achieve certification as a condition of contract award.

Public comments received illustrate that some small businesses may be unaware of how to propose cybersecurity-related costs for cost-type contracts. This rule does not change existing contract cost principles or procedures. For firm-fixed priced efforts, market supply and demand dictates profitability and bid prices, and underlying costs are not itemized.

## 9. Disputes regarding CMMC Assessments

Comment 12: Multiple commenters asked about the CMMC assessment dispute resolution process, with regard to which standards would be followed, how much time would be available to appeal findings, the types of complaints that could be raised, any limits to the costs or schedule required for dispute resolution, and roles and responsibilities of the DoD, C3PAOs, and the Accreditation Body. Commenters also wanted to know whether a tiered recourse process would be available to resolve contractor objections to the initial resolution. Two commenters expressed concerns regarding potential impacts of C3PAO assessment errors. Two commenters requested clarification regarding whether the CMMC Level required by the DoD or a prime contractor could be contested.

***Response**:* The CMMC assessment appeal process (formerly referred to as dispute resolution) described in the DFARS Case 2019–D041 Supplementary Information has changed and is described in § 170.9(b)(20) and § 170.8(b)(16). The appeals process is derived from and consistent with ISO/IEC 17020:2012 and ISO/IEC 17011:2017. Each C3PAO is required to have a time-bound, internal appeals process to address disputes related to perceived assessor errors, malfeasance, and unethical conduct. Requests for appeals will be reviewed and approved by individual(s) within the C3PAO not involved in the original assessment activities in question. OSCs can request a copy of the process from their C3PAO. If a dispute regarding assessment findings cannot be resolved by the C3PAO, it will be escalated to the Accreditation Body. The decision by the Accreditation Body will be final.
A request for an appeal about an assessor's professional conduct that is not resolved with the C3PAO will be escalated and resolved by the Accreditation Body. The issue of C3PAO liability is between an OSC and the C3PAO with which it contracts to do the assessment.
Any questions about the CMMC Level required by the solicitation should be directed to the contracting officer for the affected contractor.

## 10. Acceptance of Alternate Standards

### a. NIST SP 800-171 Rev 2 DoD Assessments and CMMC Assessments

Comment 13: Multiple commenters asked for clarification on reciprocity between NIST SP 800-171 Rev 2 DoD Assessments and CMMC assessments.

***Response**:* As stated in § 170.20(a), DoD intends to allow qualified standards acceptance of High confidence assessment using NIST SP 800-171 Rev 2 for CMMC Level 2. However, the CMMC Program requirements proposed in this rule will be implemented in the DFARS, as needed, which may result in changes to current DoD solicitation provisions and contract clauses relating to cybersecurity assessments.

### b. Cloud Standards

Comment 14: Many commenters expressed concerns regarding CMMC recognition of Federal Risk and Authorization Management Program (FedRAMP) and requested guidance on which FedRAMP baselines, if any, would be granted standards acceptance at each CMMC Level. A few commenters sought assurance that DoD Cloud Computing Security Requirements Guide (SRG) Impact Levels 4 and 5 would not be applied to CMMC Level 3.

***Response**:* CMMC does not offer comprehensive acceptance of FedRAMP. The CMMC Program allows the acceptance of FedRAMP environments in some cases to meet CMMC requirements in connection with use of a Cloud Service Provider (CSP). If an OSC uses an external CSP to process, store, or transmit CUI or to provide security protection for any such component, the OSC must ensure the CSP's product or service offering either (1) is authorized as FedRAMP Moderate or High on the FedRAMP Marketplace; or (2) meets the security requirements equivalent to those established by the Department for the FedRAMP Moderate or High baseline. The CSP will provide evidence that its product or service offering meets the security requirements equivalent to FedRAMP Moderate or High by providing a body of evidence (BOE) that attests to and describes how the CSP's product or service offering meets the FedRAMP baseline security requirements. Note that for any portion of the on-premises (internal) network that interacts with the cloud service offering and is within the CMMC Assessment Scope, the OSC is required to meet all applicable CMMC requirements to achieve certification. *The DoD Cloud Computing* SRG applies to DoD-provided cloud services and those provided by a contractor on behalf of the department, i.e., a commercial cloud service provider or integrator. Cloud Computing SRG does not apply to CMMC.

### c. Other Standards

Comment 15: Numerous commenters asked whether CMMC could leverage the results of other assessments, such as ISO/IEC 27001/27002, NIST SP 800-53, NIST SP 800-172, HITRUST, DoE Cybersecurity Capability Maturity Model, NIAP Common Criteria Testing Laboratory Services (CCEVS), Committee on National Security Systems (CNSS) Instruction No. 12533 (CNSSI 12533), ISA/IEC-62443, DoD's Security Technical Implementation Guides (STIG), NIST Cyber Security Framework (CSF), NIST Risk Management Framework (RMF), the American Institute of CPAs Service and Organizational Controls, Service and Organization Controls (SOC) Trust Services Criteria (SOC 2), ISA/IEC-62443, ITAR, Criminal Justice Information Services (CJIS) security standards, and non-ISO/IEC standards used by foreign partners such as the Australian Cybersecurity Centre Essential Eight Maturity Model.

***Response***: The CMMC Program standards acceptance is defined in § 170.20 of this rule.

## 11. CMMC Assessment Scope

Comment 16: Multiple commenters requested details on assessment boundaries and what systems are in-scope for a CMMC assessment. Questions included how assessment boundaries

are defined, how networks composed of federal components (including systems operated on behalf of the government) and non-federal components are addressed, how centralized security services are treated, and how "enduring exceptions" are handled.

***Response***: § 170.19 states that prior to a CMMC assessment, the OSA must define the CMMC Assessment Scope for the assessment, representing the boundary with which the CMMC assessment will be associated. This section includes detailed guidance on how to define the CMMC Assessment Scope, how different categories of equipment are defined to be in- or out of scope for an assessment, how the security of specialized equipment is expected to be managed, External Service Providers considerations, and the incorporation of people, technology, and facilities into the boundary.
GFE, IoT, OT, and, as defined, Restricted Information Systems and Test Equipment are categorized as "Specialized Assets" in § 170.19. NIST SP 800-171 Rev 2 uses the term "enduring exceptions" to describe how to handle exceptions for Specialized Assets.

## 12. Applicability of Multiple CMMC Levels

Comment 17: Two commenters sought confirmation that it is acceptable for contractors with multiple business segments to have one or more CMMC assessments (e.g., one segment at Level 1, another at Level 2). Commenters also wanted to know if systems within the scope of an assessment require multiple assessments if the systems are used to support tasks under multiple contracts. Another asked, if a company has multiple Commercial and Government Entity (CAGE) codes, whether a single assessment can cover all CAGE codes.

***Response***: Yes, it is possible to have different business segments or different enclaves assessed or certified at different CMMC Levels. A CMMC assessment can be restricted to a particular segment or enclave based on the defined CMMC Assessment Scope, and an OSA can define multiple CMMC Assessment Scopes. Thus, a business segment that only supports Level 1 (FCI) efforts can identify a boundary that is assessed against Level 1 requirements, and another segment that supports Level 2 (CUI) efforts can identify a different boundary that is assessed against Level 2. Offerors will be required to attain CMMC certification, when applicable, at or above the level required by the solicitation, by the time of award (or option period exercise) and must maintain their CMMC status throughout the life of the contract, task order, or delivery order.

## 13. CMMC Implementation Timeline and Pilot Program

### a. CMMC Schedule

Comment 18: There were many comments requesting clarification or justification regarding the general roll-out schedule for DFARS clause 252.204-7021. Some commenters requested program acceleration and others advocated for delays. Two commenters were confused by statements in the Federal Register Notice that the timeline for implementation across the DoD

contractor population would be seven years, but that all contracts would include the CMMC clause in five years, at the end of the roll-out.

***Response***: The DoD is implementing a phased implementation for the CMMC Program and intends to introduce CMMC requirements in solicitations over a three-year period to provide appropriate ramp-up time. The Department anticipates it will take two years for companies with existing contracts to become CMMC certified.
In response to public comment, assessment requirements in CMMC have been simplified to three tiers, and DoD is developing policy to guide Program Managers through a time-phased introduction of CMMC requirements. From the effective date of the DFARS rule that will implement CMMC requirements, DoD will include CMMC self-assessment requirements in solicitations when warranted by the FCI and CUI categories associated with the planned effort. A similar requirement for CUI has been in place since publication of the September 2020 rule that implemented DFARS provision 252.204-7019, which requires offerors to submit NIST SP 800-171 Rev 2 self-assessment results in the SPRS as a condition of award. DoD intends to include CMMC requirements for Levels 1, 2, and 3 in all solicitations issued on or after October 1, 2026, when warranted by any FCI or CUI information protection requirements for the contract effort. In the intervening period, DoD Program Managers will have discretion to include CMMC requirements in accordance with DoD policies.

### b. CMMC Pilot Program

Comment 19: Multiple commenters wanted more information about the roll-out of the CMMC pilot program, including transparency about which acquisition programs are being considered for inclusion prior to the release of a solicitation. Commenters requested details on the "provisional period," whether there would be a break between the pilot program and the official launch of the CMMC Program, whether there would be an assessment on the effectiveness of the pilot, and if lessons learned from the pilot would be shared across the community.

***Response****:* CMMC 1.0 did include a CMMC Pilot program; however, CMMC 2.0 does not include pilots. Instead, upon the effective date of the associated CMMC DFARS rule, the Department intends to begin including CMMC self-assessment requirements when applicable, for protection of FCI and CUI.

### c. Communicating CMMC Requirements

Comment 20: Two commenters requested that, during the phased rollout of CMMC, defense contractors be forewarned of DoD plans to include a CMMC requirement in an upcoming solicitation. They asked for transparency with respect to which contracts were being considered for CMMC requirements.

***Response****:* Offerors and contractors will be informed of CMMC requirements in solicitations through (1) the specification of a required CMMC Level, and (2) inclusion of the appropriate DFARS provisions or clauses. There is no plan to advertise a list of solicitations that will or may

include CMMC requirements. The implementation plan described in § 170.3(e) addresses phase in of CMMC requirements.

### d. Market Capacity for Assessments

Comment 21: Multiple commenters wanted details about assessor availability and were concerned that a lack of assessors would impact the schedule for including CMMC requirements in solicitations and contractor planning to attain CMMC certification to meet those requirements.

***Response**:* The phased implementation plan described in § 170.3(e) is intended to address ramp-up issues, provide time to train the necessary number of assessors, and allow companies the time needed to understand and implement CMMC requirements. An extension of the implementation period or other solutions may be considered in the future to mitigate any C3PAO capacity issues, but the Department has no such plans at this time. If changes to the implementation plan occur, DoD policies that govern requirements definition in the acquisition process will be modified.

### e. Certification Sustainment during Validity Period

Comment 22: Three commenters asked about sustainment of CMMC certification during the three-year certificate validity period. They wanted to know how sustainment will be monitored and whether demonstrating continuous monitoring capabilities would be considered in lieu of a strict three-year recertification period. There were also questions about what the criteria or triggers would be that would lead to a loss of accreditation during this period, including what happens when a company with a certification is acquired by another company, and whether contractors are required to notify the DoD if systems fall out of compliance with CMMC requirements.

***Response***: The validity period is one (1) year for CMMC Level 1 and three (3) years for CMMC Levels 2 and 3. Contractors must continue to meet CMMC requirements during the period of performance of the contract. Under CMMC, contractors must submit affirmations into SPRS for each assessment, attesting that they have met the CMMC requirements and will maintain the applicable information systems at the required CMMC level as specified in § 170.22. Monitoring contractor compliance with the terms of the contract is the responsibility of the contractor, with the government contracting officer. DoD is not utilizing a continuous monitoring capability in lieu of compliance requirements. DoD understands that information systems operating in a CMMC Assessment Scope will require upgrades and maintenance. For systems certified at CMMC Level 2 or above, a plan for addressing deficiencies is defined in § 170.21.
It is possible for an organization to need a new assessment during the validity period. CMMC self-assessments and certifications are valid for a defined CMMC Assessment Scope. If the CMMC Assessment Scope changes due to infrastructure modifications or expansion of the CMMC Assessment Scope due to new acquisition, a new assessment may be required. The original CMMC certification remains valid for the original CMMC Assessment Scope. The information system(s) in the new CMMC Assessment Scope may not be used to process, store, or transmit CUI for any contract until it is validated via a new CMMC assessment. The same

applies to the annual affirmations. During the annual affirmation process, a senior organization official affirms that the organization is satisfying and will maintain the requirements of the specified CMMC level (e.g., CMMC Level 2 Self-Assessment). The affirmation applies to the CMMC Assessment Scope. At the time of a new self-assessment or certification, a new affirmation is submitted into SPRS affirming that the organization meets the CMMC requirements and will maintain the applicable information system (within the CMMC Assessment Scope) at the required CMMC level. For CMMC Levels 2 and 3, an affirmation is required to be submitted in SPRS annually for the duration of the triennial validity period and at the conclusion of any POA&M closeout assessments. Affirmation requirements are set forth in § 170.22.

## 14. CMMC Assessment Timeline

Comment 23: Several comments requested details about CMMC assessment timelines, including how long an assessment would take, how long after an assessment was completed would the assessment report be ready, and when SPRS content would be updated. One commenter wanted to know how soon after a failed assessment a subsequent assessment could be scheduled. One commenter wanted details about the remediation period.

***Response***: The actual length of time it takes for an OSA to prepare for, and assessors to conduct an assessment and prepare the assessment report depends on many factors, including the number of systems and networks in the CMMC Assessment Scope, the level of assessment being conducted, staff preparedness for assessor questions, and the number of assessors conducting the assessment.
For CMMC assessments, C3PAOs will upload the results of the assessment and the signed CMMC certificate into the CMMC instantiation of eMASS. Certification is automatically posted to SPRS. There is no minimum time to wait after a failed assessment before scheduling another assessment.
A NOT MET requirement may be re-evaluated during the course of the assessment and for 10 business days following the active assessment period under certain conditions, as set forth in § 170.17(c)(2) and § 170.18(c)(2). A Level 2 or Level 3 conditional assessment and associated POA&M must be closed out within 180 days.

## 15. Assessment Delays and Award Impact

Comment 24: Several commenters expressed concerns about the impact that delays in the assessment process would have on contract award. For example, if an assessment is held up, by no fault of the contractor, such that the results will not be available until after the award date, will the contractor be ineligible to receive the award or is there a process for delaying the award? Would the answer be the same for a reassessment of a contractor whose three-year assessment or certificate is expiring? On a related issue, one comment asked about the timing of reassessment/recertification and whether work on an existing contract can continue after an assessment/certificate has expired if the reassessment is scheduled but delayed.

***Response**:* The CMMC Program rule does not provide mitigations for assessment delays that may impact timeliness of certification or recertification with regard to the closing date of a particular solicitation. Offerors will be required to attain CMMC certification, when applicable, at or above the level in the solicitation, by the time of award (or option period exercise) and must maintain their CMMC status throughout the life of the contract, task order, or delivery order. The three-year validity period should provide adequate time to prepare for and schedule subsequent assessments for certification. Timelines for meeting CMMC requirements for Level 1 or 2 self-assessment are within the control of the contractor.

## 16. Defense Contractor and Subcontractor Engagement

Comment 25: Several commenters suggested that defense contractors and subcontractors should be more engaged in the formulation of the rule and better informed in how the rule will be applied. They indicated that guidance is unclear, ad hoc, and inconsistent, and requested an authoritative source of information, such as FAQs, that are kept up to date and provide reliable responses to questions. They also expressed a desire for more transparency in how ambiguities are being resolved in early assessments.

***Response:*** In September 2019, the CMMC PMO released the first draft publication of the CMMC Model v 0.4. The CMMC PMO received over 2,000 comments from individuals and industry associations. These comments informed changes included in CMMC Model 1.0 released in January 2020. In addition, DFARS Case 2019-D041 generated over 750 additional public comments that informed changes to the rule text and influenced the transition to CMMC 2.0. The Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) held over 100 industry listening sessions in 2020 and 2021, engaged with the DIB through briefings and discussions with defense industry trade associations, academia, and government-based organizations with industry members (e.g., National Industrial Security Program Policy Advisory Committee). Many sessions were recorded and shared with the public on the Internet in social media, news releases, and the CMMC PMO website (https://DoDcio.defense.gov/CMMC/), which was completely updated in 2021 and contains new information, FAQs, and allows the public direct contact with the CMMC PMO. As always, FAQs are to clarify content only, and do not interpret, define, or otherwise change the meaning of the regulatory text. The CMMC PMO continues to communicate with defense contractors and subcontractors, to include small businesses, and other members of the public.
The official website of the DoD CMMC Program is https://DoDcio.defense.gov/CMMC/.
This website contains links to CMMC documents including, but not limited to, the CMMC Model Overview, CMMC Scoping Guidance (by level), CMMC Level 1 Self-Assessment Guide, CMMC Level 2 Assessment Guide, and the CMMC Glossary.

## 17. C3PAO Consistency

Comment 26: One commenter expressed concerns that C3PAOs would not conduct CMMC assessments in a uniform manner, leading to inconsistent results.

***Response***: C3PAOs use only certified CMMC assessors to perform CMMC assessments. To ensure assessments are conducted in a uniform manner, assessors are trained by certified instructors and required to pass CMMC assessor tests before becoming certified. The accredited CAICO manages and oversee the training, testing, authorizing, and certifying of candidate assessors and instructors. A CAICO must meet the DoD requirements set forth in § 170.10 and achieve compliance with ISO/IEC 17024:2012, Conformity Assessment – General Requirements for Bodies Operating Certification of Persons Conformity Assessment.

## 18. CMMC Cost Impacts

### a. CMMC Cost Assumptions and Estimates

Comment 27: Several commenters questioned or refuted the cost estimates and/or the assumptions and mathematical approach upon which the cost estimates were based. Several commenters requested clarification around the cited difference in both cost and hours between the CMMC certification process and the DoD Assessment process, the accounting for completion of NIST SP 800-171 Rev 2 requirements, and cost distinction between enterprise and enclave assessments. Two commenters stated that the estimated number of subcontractors was low, and one commenter suggested that the $5 million threshold for small businesses excluded a large number of small businesses from the calculations. One commenter asked whether duplication of assessments was considered for small businesses who support many prime contractors. Additional commenters believed costs were absent from the calculations, to include the cost of completing POA&M, management costs for small companies to achieve maturity, and costs for international suppliers. A number of comments requested additional estimates based on adjustments to labor rates for benefits and taxes, each of the assessment levels, and small, medium, and large companies. One commenter asked for clarification on the calculations used to estimate public savings. One commenter questioned why North American Industry Classification System (NAICS) code 54715 pertaining to sensitive CUI was not included in the calculations.

***Response****:* The cost estimates and assumptions referenced by the commenters pertain to CMMC 1.0 and are not reflective of the changes in CMMC, though public comment feedback has been incorporated into the cost estimation process for the CMMC Program where appropriate. The Department limited estimates for CMMC to those costs associated with preparing for, attaining, and publishing results of: (a) CMMC compliance via self-assessment for CMMC Levels 1 and 2, and (b) certification at CMMC Level 2 through a C3PAO and Level 3 through the DoD. Costs for companies to implement information security protections to comply with the existing FAR subpart 4.19 to achieve CMMC Level 1, and DFARS subpart 204.73 to achieve CMMC Level 2, are distinct from costs associated with CMMC assessment processes to verify and attest to the

corresponding implementation of existing rules. Cost estimates were developed for companies to implement security requirements for CMMC Level 3. CMMC Level 3 security requirements are defined in table 1 to § 170.14(c)(4) CMMC Level 3 Requirements.
For the vast majority of the DIB, CMMC does not levy additional information security protection requirements but is designed to provide increased assurance that defense contractors are contract compliant and can adequately protect FCI and CUI at a level commensurate with risk, accounting for information flow down to its subcontractors in a multi-tier supply chain. There is no recognized duplication of assessments for small companies that support many primes, because once assessed, an organization need only provide evidence of compliance or certification to prospective primes in order to satisfy the CMMC requirement in a solicitation. When information system or network boundaries differ, an additional assessment may apply.

### b. CMMC Cost Burden

Comment 28: Several commenters suggested that costs were underestimated, particularly for small businesses who were perceived to be at risk of decreased participation in the marketplace due to the cost prohibitive nature of the CMMC requirement. Multiple commenters requested additional strategies to mitigate costs, including the promotion of new technologies.

***Response**:* CMMC Levels 1 and 2, which represent the majority of the anticipated requirements, does not levy any additional information security protection requirements. To address assessment cost concerns, CMMC eliminates the third-party assessment requirement at CMMC Level 1 and permits self-assessment for certain contracts containing a CMMC Level 2 requirement. The DoD Office of Small Business Programs, available at https://business.defense.gov/, has informational resources that may help defray cybersecurity implementation costs by helping organizations stay up-to-date with the latest cybersecurity compliance and policy best practices.

### c. CMMC Cost Effectiveness and Alternatives

Comment 29: Two commenters requested that the DoD measure the impact of implementing the additional security requirements. One commenter suggested an alternative strategy to protect CUI when generated.

***Response**:* CMMC does not require implementation of any additional security protection requirements beyond those identified in current FAR clause 52.204-21 and in NIST SP 800-171 Rev 2 for CMMC Levels 1 and Level 2, respectively. CMMC Level 3 requirements are new and based upon NIST SP 800-172.

## 19. CMMC Model

### a. CMMC Level Requirement Selection

Comment 30: Multiple commenters requested clarification about who selects the CMMC Level that is specified in a solicitation and the criteria used. Commenters also wanted to know if the

contractor's CMMC Level flows-down directly to subcontracts and if so, whether that level carries down to lower tier subcontracts. Numerous questions asked if the government or a contractor is responsible for determining the appropriate CMMC Level to include in a subcontract and, if it is the contractor's responsibility, what criteria is used to identify the appropriate level to flow-down. To that end, commenters requested guidance for identifying CUI and information sensitivity. One commenter asked for clarification on whether different CMMC Level requirements could be identified within a single Statement of Work (SOW).

***Response***: The solicitation will specify the required CMMC Level, and the level itself will be identified by the requiring activity. The requiring activity knows the type and sensitivity of information that will be shared with or developed by the awarded contractor and selects the CMMC Level required to protect the information according to DoD guidance. Contractors must have achieved this level, or higher, to be awarded the resultant contract. For subcontracts, the prime contractor will identify for its subcontractor the required CMMC Level in accordance with § 170.23 if it is not already defined in the solicitation. If a prime contractor is uncertain about the appropriate CMMC Level to assign when creating a subcontract solicitation, it should consult with the government program office to determine what type of certification or assessment will be required given the information that will flow down. Policies for identification and clear marking of CUI materials are provided in CUI program materials and 32 CFR part 2002, when applicable. A solicitation may contain requirements for multiple CMMC Levels if, in support of the contract, different enclaves are expected to process, store, or transmit information that needs different levels of security.

### b. Model Standard, CMMC Levels, and Model Updates

Comment 31: One commenter stated that the CMMC Model is not a configuration-controlled standard managed by a recognized standards body.

***Response***: This rule codifies the CMMC Program, elements of which are reflected in the CMMC Model. All CMMC Model requirements are derived from FAR 52.204-21, NIST SP 800-171 Rev 2, and NIST SP 800-172, which are configuration-controlled guidelines managed by NIST. As a result of the alignment of CMMC to NIST guidelines, the Department's requirements will continue to evolve as changes are made to the underlying NIST SP 800-171 Rev 2 and NIST SP 800-172 security requirements. Additional rulemaking may be necessary in the future to conform CMMC requirements described in this rule to any changes to the underlying information protection requirements defined in the foundational NIST guidelines.

Comment 32: Many comments were received requesting changes to CMMC Model 1.0. Several commenters requested changes to CMMC Level requirements and others had questions about the content and handling of CMMC Model updates. A few commenters made suggestions for restricting the current implementation, such as using only NIST SP 800-171 Rev 2 for the CMMC 1.0 implementation of Level 1-3 requirements and supplementing with additional requirements only in Levels 4 and 5. Similar comments recommended using NIST SP 800-171 Rev 2 for the initial CMMC rollout and later expanding to include additional CMMC

requirements. A number of comments questioned the purpose and use of the CMMC 1.0 implementation of CMMC Level 2. Other comments requested information on updating CMMC requirements as new technology and threats emerge and new versions of NIST SP 800-171 Rev 2 and NIST SP 800-53 are released. Multiple comments were received on CMMC 1.0 Levels 4 and 5. Several commenters believed there to be a significant disconnect between NIST SP 800-171B/172 and CMMC 1.0 Levels 4 and 5, and issues with implementation of these levels. Many comments requested that Levels 4 and 5 be updated to allow for flexibility in implementation rather than require all the requirements as written. Reasons cited for allowing flexibility include reducing cost and assessment complexity as well as allowing for the ability to adapt based on architectural environments and dynamic threat models.

***Response***: Changes were made in this rule to requirements in the former CMMC model based in part upon receipt of informal public comment. The CMMC Model was streamlined to three-tiers, which align to the protection requirements set forth in FAR 52.204-21, NIST SP 800-171 Rev 2, and NIST SP 800-172, and all CMMC-unique requirements and process maturity elements have been removed.
The CMMC Model and program requirements will be evaluated as new technology and threats emerge and revised as appropriate.

Comment 33: One comment included a request to identify instances where contractors would be better off using a classified environment, rather than CMMC version 1.0 Level 4 or 5, to protect the information.

***Response****:* The CMMC Program is designed to enforce protection of unclassified information, to include FCI and CUI, not intended for public release that is shared by the Department with its contractors and subcontractors. The program provides the Department increased assurance that contractors and subcontractors are meeting the cybersecurity requirements that apply to acquisition programs and systems that process federal contract information and controlled unclassified information. Any discussion regarding the use of classified networks is outside of the scope of the CMMC Program.

## 20. CMMC Requirements

Comment 34: There were multiple comments suggesting additions, deletions, or changes to model requirements. One commenter noted multiple instances of CMMC requirements with the term ‘information system’ rather than ‘system’ used in NIST SP 800-171 Rev 2, asking if CMMC meant to change the intent by inserting ‘information’ in these requirements. Multiple commenters questioned the intent, clarity, or interpretation of several CMMC requirements/NIST SP 800-171 Rev 2 requirements, recommending clarification regarding vulnerability management, protection of mobile devices, review of audit logs, disabling of identifiers, FIPS validated encryption, and malicious code scans. One comment suggested that CMMC 1.0 requirements RM.2.141 and RM.3.144 are redundant and recommended incorporating RM 3.146 into CA.2.159, justifying that a plan of action is essentially a risk management plan. Two

commenters noted that two CMMC 1.0 requirements (RE.2.137 and RE.3.139) are unclear as they do not specify what data requires backup, or the meaning of resilient backup. One commenter said that CMMC 1.0 requirement MA.2.114 removed the qualifier of "maintenance" when describing personnel requiring supervision of maintenance activities, asking if this is an insignificant change to the NIST SP 800-171 Rev 2 security requirement, or whether there is some rationale or message that the CMMC specification is trying to adjust by deviating from the NIST SP 800-171 Rev 2. Two commenters stated that CMMC 1.0 requirement MP.1.1.18 requires only FCI be sanitized, but, for CMMC 1.0 Level 3 (CMMC Level 2 under CMMC 2.0) assessments, there is no requirement to sanitize CUI. One commenter wanted to know which CMMC requirement requires a medium assurance certificate for reporting cyber incidents.

***Response***: In CMMC 1.0, there was no intent to change the meaning of NIST requirements except those referenced as "modified." These minor discrepancies are now resolved as all FCI requirements use the exact FAR language and all CUI requirements use the exact language from the relevant NIST guidelines. The requirements in CMMC Level 3 are derived from NIST SP 800-172 with DoD-approved parameters. Commenters requesting revisions to NIST guidelines should respond to the NIST public comment periods. There is no CMMC-specific cyber incident reporting requirement or need for associated medium assurance certificate.

Comment 35: Several comments sought clarification on the alignment and relative authority or precedence of the CMMC requirements to Federal, Legislative, Statutory, Regulatory, or DoD Organizational policy, DoD instructions, and FAQs.

***Response***: The CMMC Program requirements will be required once implemented in the DFARS and will have the same relative authority of any other DoD contract requirement. The CMMC Program relates to and incorporates elements of the following authorities: Executive Order No. 13556, Controlled Unclassified Information, 75 FR 68675 (November 4, 2010), which establishes "an open and uniform program for managing [unclassified] information that requires safeguarding or dissemination controls;" 32 CFR part 2002, which describes the executive branch's Controlled Unclassified Information Program and establishes policy for designating, handling, safeguarding, and decontrolling information that qualifies as CUI when processed, stored, or transmitted on a federal or non-federal information system; FAR clause 52.204-21, Basic Safeguarding of Covered Contractor Information Systems, which, as applicable, requires contractors to apply certain basic safeguarding procedures on covered contractor information systems that process, store, or transmit FCI; and DFARS clause 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*, which, as applicable, requires defense contractors to implement NIST SP 800-171 Rev 2 requirements on unclassified covered contractor information systems that process, store, or transmit covered defense information. Additional DoD instructions and manuals address DoD information security policy, including DoDI 5200.48 CUI which establishes policy, assigns responsibilities, and prescribes procedures for CUI throughout the DoD for federal and on non-federal information systems to include the implementation of NIST SP 800-171 Rev 2. A requirement for CMMC assessments provides DoD assurance that contractors have implemented required cybersecurity protections. The

requirements of this rule will be implemented in an associated 48 CFR acquisition rule regarding CMMC.

## 21. CMMC Assessment

Comment 36: Multiple commenters pointed out that the rule does not specify an authoritative source for obtaining a CMMC certificate, leaving the pedigree of certificates in question. Two comments inquired about the security of record [data] collection and retention and whether the assessors' platforms would need to be CMMC Level 3 compliant to protect sensitive data used for the assessment/certification process.

***Response***: The processes for achieving compliance with a CMMC level are described in §170.15 through § 170.18. CMMC Level 2 Certification Assessments are conducted by C3PAOs authorized by the CMMC Accreditation Body. C3PAOs grant CMMC Level 2 certificates of assessment. The DoD conducts CMMC Level 3 Certification Assessments and grants Level 3 certificates of assessment. A C3PAO's IT infrastructure must achieve at least a CMMC Level 2 Certification Assessment. Certified CMMC Assessors working at their place of business or from home must use their C3PAO's IT infrastructure. Assessment data and results are securely uploaded by the C3PAO into the CMMC instantiation of eMASS. The CMMC instantiation of eMASS automatically feeds compliance data into SPRS. Both eMASS and SPRS are Department owned and operated systems.

Comment 37: A few commenters requested resources for understanding CMMC requirements. There were also many comments related to the purpose, status, schedule, or content of the CMMC Assessment Guides. Additional comments requested clarification on the evaluation criteria and evidence described in the current Assessment Guides.

***Response*****:** CMMC Assessment Guides are optional resources to aid in understanding CMMC requirements and are largely derived from NIST documentation, to include NIST SP 800-171 Rev 2 and NIST SP 800-172. The CMMC assessment process is defined in § 170.15 through §170.18, and the CMMC Scoring Methodology is defined in § 170.24. The evaluation criteria (i.e., assessment procedures) and evidence (i.e., potential assessment methods and objects) required are taken directly from the NIST documentation, and revisions to NIST documentation are outside the scope of this rule. The CMMC Assessment Guides provide supplementary information, further discussion, examples, and references for assessors and contractors preparing for assessments. The guides do not identify specific solutions or baselines. These documents are available at: https://DoDcio.defense.gov/CMMC/. Updated CMMC Assessment Guides and associated CMMC documents were posted on the OUSD(A&S) CMMC website after the public comment period for DFARS Case 2019-D041 closed on November 30, 2020. These documents reflected changes based on review of public comments. Future updates to CMMC guidance documentation will be made as needed.

Comment 38: One comment suggested that audit standards be determined for CMMC assessments. Two comments asked for clarification regarding references provided in the model, whether all references must be reviewed, and if the requirements within the references must also be achieved.

***Response***: The Department has reviewed definitions of audit and assessments and determined "assessment" best meets the goals of the CMMC Program. The cybersecurity standard requirements for the different CMMC Levels are set forth in § 170.14 and clarify references for the security requirements.

Comment 39: Many commenters were concerned about the lack of waivers or POA&Ms. Several commenters commented that not allowing waivers is impractical and will impact the ability of businesses to qualify for contract award. Commenters asked for clarification on the differences between POA&M that are not allowed by CMMC and the plans of action as required in the CMMC Level 3 control (now CMMC Level 2 under CMMC 2.0), CA.2.159 (now CA.L2-3.12.2 under CMMC 2.0). Many noted that POA&Ms are necessary when managing activities like system upgrades, vendor changes, and company acquisitions to avoid temporarily falling out of compliance.

***Response***: Under certain circumstances, the CMMC Program does permit contract award to organizations that have an approved and time limited POA&M. See § 170.21 for additional information on POA&Ms. There is no process for organizations to request waiver of CMMC solicitation requirements. DoD internal policies, procedures, and approval requirements will govern the process for DoD to waive inclusion of the CMMC requirement in the solicitation.

## 22. The Accreditation Body and C3PAOs

Comment 40: Many commenters had questions and concerns about the management of the Accreditation Body and C3PAOs. A few commenters suggested using a government entity instead of the Accreditation Body construct to manage assessments. Commenters asked about the governance, resourcing, and oversight of the Accreditation Body with respect to CMMC training and assessments. Commenters expressed concerns such as who would make final decisions about CMMC issues, the lack of clearly defined roles and responsibilities for CMMC governance, and the long-term effectiveness of the Accreditation Body staffed by an all-volunteer workforce. One comment asked how the Accreditation Body can legally license training when CMMC Program information is available for free.

***Response***: The decision to use a non-governmental Accreditation Body was made because the DoD determined that there was insufficient capacity within the DoD to manage assessor training and assessments for all defense contractors who need to comply with CUI protection policies. The DoD CMMC PMO provides oversight of the Accreditation Body and is also responsible for developing, updating, maintaining, and publishing the CMMC Model, CMMC Assessment Guides, and policies for implementation of the CMMC Program.

Roles and responsibilities of the CMMC PMO, the Accreditation Body, and its organizations are described in SUBPART C of this rule. The Accreditation Body accredits C3PAOs and the CAICO. The Accreditation Body authorizes the CAICO to certify CMMC assessors and instructors and the C3PAOs to conduct assessments using CAICO-certified assessors.

Comment 41: Many commenters expressed concerns about how to ensure the necessary independence, quality assurance, integrity, and rigor of, and protection against potential conflicts of interest within the Accreditation Body and C3PAOs. Numerous commenters recommended the use of ISO/IEC standards to address these issues. Additionally, one commenter was concerned about high costs for assessments that could result if there is a lack of oversight for charging fees.

***Response***: The Accreditation Body is required to become compliant with the ISO/IEC 17011:2017 standard (the international benchmark used in demonstrating an accreditation body's impartiality, technical competency, and resources) and the requirements set forth in § 170.8. Additionally, the C3PAOs and CAICO must comply with requirements as specified in § 170.9 and § 170.10, respectively, including the specified ISO/IEC standards.

Comment 42: To address a perceived shortage of CMMC C3PAO assessors, two commenters suggested authorizing the use of other ISO/IEC-compliant accreditation bodies to increase the numbers of assessors. Another commenter wanted to know how a company could become an accreditation body.

***Response***: Consistency in training is imperative due to the unique qualifications needed to understand requirements. Additionally, ISO/IEC 17024:2012 Conformity Assessment requirements are levied against the CAICO and may not be required by other entities. The number and level of assessors needed is relative to the number of companies seeking CMMC assessment. The demand level is influenced, but not solely determined by, the number of solicitations that include CMMC requirements, the CMMC Levels specified, and the estimated number of subcontractors that will also need to meet CMMC requirements, when flowed down by the prime contractor. To facilitate a smooth and orderly transition to CMMC, the Department will issue policy guidance to government Program Managers to govern the rate at which CMMC requirements are levied in new solicitations. The implementation phases are described in §170.3(e). The CMMC PMO has visibility into the Accreditation Body's assessor training activities, tracks the anticipated number of trained assessors, and will use this information to inform policies that guide government Program Managers in identifying CMMC requirements in new solicitations.

## 23. Relationship to Existing Regulations

Comment 43: Several commenters asked about the implications of having DFARS clauses 252.204-7012 and 252.204-7021 coexist in contracts and wanted to know if all the 252.204-7012 requirements, including the requirements for "adequate security," incident reporting, and

flowdown, apply in the presence of 252.204-7021. Others were concerned about a perceived conflict on the protection of CUI between NIST SP 800-171 Rev 2, which specifies the minimum requirements to provide "adequate security" for CUI on nonfederal systems and DFARS clause 252.204-7021 based on the CMMC Program. Multiple commenters wanted to know if the 252.204-7021 clause and the CMMC requirements override contractor responsibility to comply with other applicable clauses of the contract, or other applicable U.S. Government statutory or regulatory requirements. Others were concerned about a continued proliferation of security requirements.

***Response***: CMMC Program requirements proposed in this rule will be implemented in the DFARS, as needed, which may result in changes to current DoD solicitation provisions and contract, including DFARS clause 252.204-7021. As such, DoD cannot address applicability of or changes to current DFARS clause 252.204-7021 or other current DFARS cybersecurity provisions or clauses at this time.
DoD does not intend to impose duplicative cybersecurity protection or assessment requirements. There is no conflict between the CMMC cybersecurity protection requirements described in this rule and DoD's current information safeguarding requirements, including those set forth in DFARS clause 252.204-7012. This CMMC rule adds new requirements for the assessment of contractor implementation of underlying information security standards and guidelines, as applicable, such as those set forth in FAR clause 52.204-21 and in the NIST SP 800-171 Rev 2. This rule also prescribes additional information security protection and assessment requirements for CMMC Level 3, derived from NIST SP 800-172, for certain limited scenarios.
As new cyber threats emerge, security requirements will continue to evolve to support efforts to protect information important to U.S. national security. However, alternate standards will continue to be reviewed, as described in § 170.20, to minimize the burden of new requirements.

## 24. Phase-out of Existing Cybersecurity Requirements

Comment 44: Several commenters asked whether DFARS clause 252.204-7012, DFARS provision 252.204-7019 and 252.204-7020 will be phased out since DFARS clause 252.204-7021 is now a requirement.

***Response***: The CMMC Program requirements proposed in this rule will be implemented in the DFARS, as needed, which may result in changes to current DoD solicitation provisions and contract clauses, including DFARS clause 252.204-7021. As such, DoD cannot address applicability of or changes to current DFARS clause 252.204-7021 or other current DFARS cybersecurity provisions or clauses at this time.
The information safeguarding requirements and cyber incident reporting requirements set forth in DFARS clause 252.204-7012 will not be phased out as a result of this rule. CMMC Program requirements provide DoD with verification, through self or third-party assessment, that defense contractors have, in fact, implemented DoD's cybersecurity protection requirements. In addition, the requirements of this rule will not be fully implemented (and will not appear in all DoD contracts) until 2026 or later. As such, DoD will continue to require the current cybersecurity

protections as reflected in the identified DFARS provisions and clauses for contracts that do not include CMMC requirements.