DEPARTMENT OF DEFENSE

Defense Acquisition Regulations System

48 CFR Parts 204, 212, 217, and 252

[Docket DARS–2020–0034]

RIN 0750–AJ81

Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019–D041)

AGENCY: Defense Acquisition Regulations System, Department of Defense (DoD).

ACTION: Interim rule.

SUMMARY: DoD is issuing an interim rule to amend the Defense Federal Acquisition Regulation Supplement (DFARS) to implement a DoD Assessment Methodology and Cybersecurity Maturity Model Certification framework in order to assess contractor implementation of cybersecurity requirements and enhance the protection of unclassified information within the DoD supply chain.

DATES: Effective November 30, 2020.

Comments on the interim rule should be submitted in writing to the address shown below on or before November 30, 2020, to be considered in the formation of a final rule.

ADDRESSES: Submit comments identified by DFARS Case 2019–D041, using any of the following methods:

- *Federal eRulemaking Portal: http://www.regulations.gov.* Search for ''DFARS Case 2019–D041''. Select ''Comment Now'' and follow the instructions provided to submit a comment. Please include ''DFARS Case 2019–D041'' on any attached documents.
- *Email: osd.dfars@mail.mil.* Include DFARS Case 2019–D041 in the subject line of the message.

Comments received generally will be posted without change to *http://www.regulations.gov,* including any personal information provided. To confirm receipt of your comment(s), please check *www.regulations.gov,* approximately two to three days after submission to verify posting.

FOR FURTHER INFORMATION CONTACT: Ms. Heather Kitchens, telephone 571–372–6104.

SUPPLEMENTARY INFORMATION:

I. Background

The theft of intellectual property and sensitive information from all U.S. industrial sectors due to malicious cyber activity threatens economic security and national security. The Council of Economic Advisors estimates that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016. Over a ten-year period, that burden would equate to an estimated $570 billion to $1.09 trillion dollars in costs. As part of multiple lines of effort focused on the security and resiliency of the Defense Industrial Base (DIB) sector, the Department is working with industry to enhance the protection of unclassified information within the supply chain. Toward this end, DoD has developed the following assessment methodology and framework to assess contractor implementation of cybersecurity requirements, both of which are being implemented by this rule: the National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171 DoD Assessment Methodology and the Cybersecurity Maturity Model Certification (CMMC) Framework. The NIST SP 800–171 DoD Assessment and CMMC assessments will not duplicate efforts from each assessment, or any other DoD assessment, except for rare circumstances when a re-assessment may be necessary, such as, but not limited to, when cybersecurity risks, threats, or awareness have changed, requiring a re-assessment to ensure current compliance.

A. NIST SP 800–171 DoD Assessment Methodology

DFARS clause 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, is included in all solicitations and contracts, including those using Federal Acquisition Regulation (FAR) part 12 commercial item procedures, except for acquisitions solely for commercially available off-the-shelf (COTS) items. The clause requires contractors to apply the security requirements of NIST SP 800–171 to ''covered contractor information systems,'' as defined in the clause, that are not part of an IT service or system operated on behalf of the Government. The NIST SP 800–171 DoD Assessment Methodology provides for the assessment of a contractor's implementation of NIST SP 800-171 security requirements, as required by DFARS clause 252.204–7012. More information on the NIST SP 800–171 DoD Assessment Methodology is available at *https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html.*

The Assessment uses a standard scoring methodology, which reflects the net effect of NIST SP 800–171 security requirements not yet implemented by a contractor, and three assessment levels (Basic, Medium, and High), which reflect the depth of the assessment performed and the associated level of confidence in the score resulting from the assessment. A Basic Assessment is a self-assessment completed by the contractor, while Medium or High Assessments are completed by the Government. The Assessments are completed for each covered contractor information system that is relevant to the offer, contract, task order, or delivery order.

The results of Assessments are documented in the Supplier Performance Risk System (SPRS) at *https://www.sprs.csd.disa.mil/* to provide DoD Components with visibility into the scores of Assessments already completed; and verify that an offeror has a current (*i.e.,* not more than three years old, unless a lesser time is specified in the solicitation) Assessment, at any level, on record prior to contract award.

B. Cybersecurity Maturity Model Certification Framework

Building upon the NIST SP 800–171 DoD Assessment Methodology, the CMMC framework adds a comprehensive and scalable certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level. CMMC is designed to provide increased assurance to the Department that a DIB contractor can adequately protect sensitive unclassified information such as Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) at a level commensurate with the risk, accounting for information flow down to its subcontractors in a multi-tier supply chain. A DIB contractor can achieve a specific CMMC level for its entire enterprise network or particular segment(s) or enclave(s), depending upon where the information to be protected is processed, stored, or transmitted.

The CMMC model consists of maturity processes and cybersecurity best practices from multiple cybersecurity standards, frameworks, and other references, as well as inputs from the broader community. The CMMC levels and the associated sets of processes and practices are cumulative. The CMMC model encompasses the basic safeguarding requirements for FCI specified in FAR clause 52.204–21, Basic Safeguarding of Covered

Contractor Information Systems, and the security requirements for CUI specified in NIST SP 800–171 per DFARS clause 252.204–7012. Furthermore, the CMMC model includes an additional five processes and 61 practices across Levels 2–5 that demonstrate a progression of cybersecurity maturity.

Level	Description
1	Consists of the 15 basic safeguarding requirements from FAR clause 52.204–21.
2	Consists of 65 security requirements from NIST SP 800–171 implemented via DFARS clause 252.204–7012, 7 CMMC practices, and 2 CMMC processes. Intended as an optional intermediary step for contractors as part of their progression to Level 3.
3	Consists of all 110 security requirements from NIST SP 800–171, 20 CMMC practices, and 3 CMMC processes.
4	Consists of all 110 security requirements from NIST SP 800–171, 46 CMMC practices, and 4 CMMC processes.
5	Consists of all 110 security requirements from NIST SP 800–171, 61 CMMC practices, and 5 CMMC processes.

In order to achieve a specific CMMC level, a DIB company must demonstrate both process institutionalization or maturity and the implementation of practices commensurate with that level. CMMC assessments will be conducted by accredited CMMC Third Party Assessment Organizations (C3PAOs). Upon completion of a CMMC assessment, a company is awarded a certification by an independent CMMC Accreditation Body (AB) at the appropriate CMMC level (as described in the CMMC model). The certification level is documented in SPRS to enable the verification of an offeror's certification level and currency (*i.e.* not more than three years old) prior to contract award. Additional information on CMMC and a copy of the CMMC model can be found at *https://www.acq.osd.mil/cmmc/index.html.*

DoD is implementing a phased rollout of CMMC. Until September 30, 2025, the clause at 252.204–7021, Cybersecurity Maturity Model Certification Requirements, is prescribed for use in solicitations and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial items, excluding acquisitions exclusively for COTS items, if the requirement document or statement of work requires a contractor to have a specific CMMC level. In order to implement the phased rollout of CMMC, inclusion of a CMMC requirement in a solicitation during this time period must be approved by the Office of the Under Secretary of Defense for Acquisition and Sustainment.

CMMC will apply to all DoD solicitations and contracts, including those for the acquisition of commercial items (except those exclusively COTS items) valued at greater than the micro-purchase threshold, starting on or after October 1, 2025. Contracting officers will not make award, or exercise an option on a contract, if the offeror or contractor does not have current (*i.e.* not older than three years) certification for the required CMMC level. Furthermore, CMMC certification requirements are required to be flowed down to subcontractors at all tiers, based on the sensitivity of the unclassified information flowed down to each subcontractor.

II. Discussion and Analysis

A. NIST SP 800–171 DoD Assessment Methodology

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

The new DFARS provision 252.204–7019 advises offerors required to implement the NIST SP 800–171 standards of the requirement to have a current (not older than three years) NIST SP 800–171 DoD Assessment on record in order to be considered for award. The provision requires offerors to ensure the results of any applicable current Assessments are posted in SPRS and provides offerors with additional information on conducting and submitting an Assessment when a current one is not posted in SPRS.

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

B. Cybersecurity Maturity Model Certification

This rule adds a new DFARS subpart, Subpart 204.75, Cybersecurity Maturity Model Certification (CMMC), to specify the policy and procedures for awarding a contract, or exercising an option on a contract, that includes the requirement for a CMMC certification. Specifically, this subpart directs contracting officers to verify in SPRS that the apparently successful offeror's or contractor's CMMC certification is current and meets the required level prior to making the award.

A new DFARS clause 252.204–7021, Cybersecurity Maturity Model Certification Requirements, is prescribed for use in all solicitations and contracts or task orders or delivery orders, excluding those exclusively for the acquisition of COTS items. This DFARS clause requires a contractor to: Maintain the requisite CMMC level for the duration of the contract; ensure that its subcontractors also have the appropriate CMMC level prior to awarding a subcontract or other contractual instruments; and include the requirements of the clause in all subcontracts or other contractual instruments.

The Department took into consideration the timing of the requirement to achieve a CMMC level certification in the development of this rule, weighing the benefits and risks associated with requiring CMMC level certification: (1) At time of proposal or offer submission; (2) at time of award;

or (3) after contract award. The Department ultimately adopted alternative 2 to require certification at the time of award. The drawback of alternative 1 (at time of proposal or offer submission) is the increased risk for contractors since they may not have sufficient time to achieve the required CMMC certification after the release of the Request for Information (RFI). The drawback of alternative 3 (after contract award) is the increased risk to the Department with respect to the schedule and uncertainty with respect to the case where the contractor is unable to achieve the required CMMC level in a reasonable amount of time given their current cybersecurity posture. This potential delay would apply to the entire supply chain and prevent the appropriate flow of CUI and FCI. The Department seeks public comment on the timing of contract award, to include the effect of requiring certification at time of award on small businesses.

C. Conforming Changes

This rule also amends the following DFARS sections to make conforming changes:

- Amends the list in DFARS section 212.301 of solicitation provisions and contract clauses that are applicable for the acquisition of commercial items to include the provisions and clauses included in this rule.
- Amends DFARS 217.207, Exercise of Options, to advise contracting officers that an option may only be exercised after verifying the contractor's CMMC level, when CMMC is required in the contract.

III. Applicability to Contracts at or Below the Simplified Acquisition Threshold and for Commercial Items, Including Commercially Available Off-the-Shelf Items

This rule creates the following new solicitation provision and contract clauses:

- DFARS 252.204–7019, Notice of NIST SP 800–171 DoD Assessment Requirements;
- DFARS clause 252.204–7020, NIST SP 800–171 DoD Assessment Requirements; and
- DFARS clause 252.204–7021, Cybersecurity Maturity Model Certification Requirements.

The objective of this rule is provide the Department with: (1) The ability to assess contractor implementation of NIST SP 800–171 security requirements, as required by DFARS clause 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting; and (2) assurances that DIB contractors can adequately protect sensitive unclassified information at a level commensurate with the risk, accounting for information flowed down to subcontractors in a multi-tier supply chain. Flowdown of the requirements is necessary to respond to threats that reach even the lowest tiers in the supply chain. Therefore, to achieve the desired policy outcome, DoD intends to apply the new provision and clauses to contracts and subcontracts for the acquisition of commercial items and to acquisitions valued at or below the simplified acquisition threshold, but greater than the micro-purchase threshold. The provision and clauses will not be applicable to contracts or subcontracts exclusively for the acquisition of commercially available off-the-shelf items.

IV. Expected Cost Impact and Benefits

A. Benefits

The theft of intellectual property and sensitive information from all U.S. industrial sectors due to malicious cyber activity threatens U.S. economic and national security. The aggregate loss of intellectual property and certain unclassified information from the DoD supply chain can undercut U.S. technical advantages and innovation, as well as significantly increase risk to national security. This rule is expected to enhance the protection of FCI and CUI within the DIB sector.

B. Costs

A Regulatory Impact Analysis (RIA) that includes a detailed discussion and explanation about the assumptions and methodology used to estimate the cost of this regulatory action is available at *www.regulations.gov* (search for ''DFARS Case 2019–D041'' click ''Open Docket,'' and view ''Supporting Documents''). The total estimated public and Government costs (in millions) associated with this rule, calculated in perpetuity in 2016 dollars at a 7 percent discount rate, is provided as follows:

Total cost (in millions)	Public	Govt	Total
Annualized Costs	$6,500.5	$0.3	$6,500.7
Present Value Costs	92,863.6	3.7	92,867.3

The following is a breakdown of the public and Government costs and savings associated with each component of the rule:

1. NIST SP 800–171 DoD Assessments

The following is a summary of the estimated public and Government costs (in millions) associated with the NIST SP DoD Assessments, calculated in perpetuity in 2016 dollars at a 7 percent discount rate:

DoD assessments	Public	Government	Total
Annualized Costs	$6.7	$9.5	$16.3
Present Value Costs	96.1	136.2	232.3

2. CMMC Requirements

The following is a summary of the estimated public and Government costs (in millions) associated with the CMMC requirements, calculated in perpetuity in 2016 dollars at a 7 percent discount rate:

CMMC requirements	Public	Government	Total
Annualized Costs	$6,525.0	$8.9	$6,533.9
Present Value Costs	93,213.6	127.3	93,340.9

3. Elimination of Duplicate Assessments

The following is a summary of the estimated public and Government savings (in millions) associated with the elimination of duplicate assessments, calculated in perpetuity in 2016 dollars at a 7 percent discount rate:

Eliminate duplication	Public	Government	Total
Annualized Savings	-$31.2	-$18.2	-$49.4
Present Value Savings	-446.1	-259.8	-705.9

V. Executive Orders 12866 and 13563

Executive Orders (E.O.s) 12866 and 13563 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). E.O. 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This is an economically significant regulatory action and, therefore, was subject to review under section 6(b) of E.O. 12866, Regulatory Planning and Review, dated September 30, 1993. This rule is a major rule under 5 U.S.C. 804.

VI. Executive Order 13771

The rule is not subject to the requirements if E.O. 13771, because this rule is being issued with respect to a national security function of the United States.

VII. Regulatory Flexibility Act

DoD expects this rule to have a significant economic impact on a substantial number of small entities within the meaning of the Regulatory Flexibility Act, 5 U.S.C. 601, *et seq.* Therefore, an initial regulatory flexibility analysis has been performed and is summarized as follows:

A. Reasons for the Action

This rule is necessary to address threats to the U.S. economy and national security from ongoing malicious cyber activities, which includes the theft of hundreds of billions of dollars of U.S. intellectual property. Currently, the FAR and DFARS prescribe contract clauses intended to protect FCI and CUI within the DoD supply chain. Specifically, the clause at FAR 52.204–21, Basic Safeguarding of Covered Contractor Information Systems, is prescribed at FAR 4.1903 for use in Government solicitations and contracts and requires contractors and subcontractors to apply basic safeguarding requirements when processing, storing, or transmitting FCI in or from covered contractor information systems. The clause focuses on ensuring a basic level of cybersecurity hygiene and is reflective of actions that a prudent business person would employ.

In addition, DFARS clause 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, requires defense contractors and subcontractors to provide ''adequate security'' to store, process, or transmit CUI on information systems or networks, and to report cyber incidents that affect these systems or networks. The clause states that to provide adequate security, the Contractor shall implement, at a minimum, the security requirements in ''National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171, Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations.'' Contractors are also required to flow down DFARS Clause 252.204–7012 to all subcontracts, which involve CUI.

However, neither the FAR clause, nor the DFARS clause, provide for DoD verification of a contractor's implementation of basic safeguarding requirements or the security requirements specified in NIST SP 800–171 prior to contract award.

Under DFARS clause 252.204–7012, DIB companies self-attest that they will implement the requirements in NIST SP 800–171 upon submission of their offer. A contractor can document implementation of the security requirements in NIST SP 800–171 by having a system security plan in place to describe how the security requirements are implemented, in addition to associated plans of action to describe how and when any unimplemented security requirements will be met. As a result, the current regulation enables contractors and subcontractors to process, store, or transmit CUI without having implemented all of the 110 security requirements and without establishing enforceable timelines for addressing shortfalls and gaps.

Findings from DoD Inspector General report (DODIG–2019–105 ''Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems'') indicate that DoD contractors did not consistently implement mandated system security requirements for safeguarding CUI and recommended that DoD take steps to assess a contractor's ability to protect this information. The report emphasizes that malicious actors can exploit the vulnerabilities of contractors' networks and systems and exfiltrate information related to some of the Nation's most valuable advanced defense technologies.

Although DoD contractors must include DFARS clause 252.204–7012 in subcontracts for which subcontract performance will involve covered defense information (DoD CUI), this does not provide the Department with sufficient insights with respect to the cybersecurity posture of DIB companies throughout the multi-tier supply chain for any given program or technology development effort.

Furthermore, given the size and scale of the DIB sector, the Department cannot scale its organic cybersecurity assessment capability to conduct on-site assessments of approximately 220,000 DoD contractors every three years. As a result, the Department's organic assessment capability is best suited for conducting targeted assessments for a subset of DoD contractors.

Finally, the current security requirements specified in NIST SP 800–171 per DFARS clause 252.204–7012, do not sufficiently address additional threats to include Advanced Persistent Threats (APTs).

Because of these issues and shortcomings and the associated risks to national security, the Department determined that the status quo was not acceptable and developed a two-pronged approach to assess and verify the DIB's ability to protect the FCI and CUI on its information systems or networks, which is being implemented by this rule:

- *The National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171 DoD Assessment Methodology.* A standard methodology to assess contractor implementation of the cybersecurity requirements in NIST SP 800–171,

''Protecting Controlled Unclassified Information (CUI) In Nonfederal Systems and Organizations.''

• *The Cybersecurity Maturity Model Certification (CMMC) Framework.* A DoD certification process that measures a company's institutionalization of processes and implementation of cybersecurity practices.

B. Objectives of, and Legal Basis for, the Rule

This rule establishes a requirement for contractors to have a current NIST SP 800–171 DoD Assessment and the appropriate CMMC level certification prior to contract award and during contract performance. The objective of the rule is to provide the Department with: (1) The ability to assess at a corporate-level a contractor's implementation of NIST SP 800–171 security requirements, as required by DFARS clause 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting; and (2) assurances that a DIB contractor can adequately protect sensitive unclassified information at a level commensurate with the risk, accounting for information flow down to its subcontractors in a multi-tier supply chain.

1. NIST SP 800–171 DoD Assessment Methodology

In February 2019, the Under Secretary of Defense for Acquisition and Sustainment directed the Defense Contract Management Agency (DCMA) to develop a standard methodology to assess contractor implementation of the cybersecurity requirements in NIST SP 800–171 at the corporate or entity level. The DCMA Defense Industrial Base Cybersecurity Assessment Center's NIST SP 800–171 DoD Assessment Methodology is the Department's initial strategic DoD/corporate-wide assessment of contractor implementation of the mandatory cybersecurity requirements established in the contracting regulations. Results of a NIST SP 800–171 DoD Assessment reflect the net effect of NIST SP 800–171 security requirements not yet implemented by a contractor, and may be conducted at one of three assessment levels. The DoD Assessment Methodology provides the following benefits:

• *Enables Strategic Assessments at the Entity-level.* The NIST SP 800–171 DoD Assessment Methodology enables DoD to strategically assess a contractor's implementation of NIST SP 800–171 on existing contracts that include DFARS clause 252.204–7012, and to provide an objective assessment of a contractor's NIST SP 800–171 implementation status.

• *Reduces Duplicative or Repetitive Assessments of our Industry Partners.* Assessment results will be posted in the Supplier Performance Risk System (SPRS), DoD's authoritative source for supplier and product performance information. This will provide DoD Components with visibility to summary level scores, rather than addressing implementation of NIST SP 800–171 on a contract-by-contract approach. Conducting such assessments at a corporate- or entity-level, significantly reduces the need to conduct assessments at the program or contract level, thereby reducing the cost to both DoD and industry.

• *Provides a Standard Methodology for Contractors to Self-assess Their Implementation of NIST SP 800–171.* The Basic Assessment provides a consistent means for contractors to review their system security plans prior to and in preparation for either a DoD or CMMC assessment.

The NIST SP 800–171 DoD Assessment Methodology provides a means for the Department to assess contractor implementation of these requirements as the Department transitions to full implementation of the CMMC, and a means for companies to self-assess their implementation of the NIST SP 800–171 requirements prior to either a DoD or CMMC assessment.

2. The CMMC Framework

Section 1648 of the National Defense Authorization Act for Fiscal Year (FY) 2020 (Pub. L. 116–92) directs the Secretary of Defense to develop a risk-based cybersecurity framework for the DIB sector, such as CMMC, as the basis for a mandatory DoD standard. Building upon the NIST SP 800–171 DoD Assessment Methodology, the CMMC framework adds a comprehensive and scalable certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level. CMMC is designed to provide increased assurance to the Department that a DIB contractor can adequately protect sensitive unclassified information (*i.e.* FCI and CUI) at a level commensurate with the risk, accounting for information flow down to its subcontractors in a multi-tier supply chain. Implementation of the CMMC Framework is intended to solve the following policy problems:

• *Verification of a contractor's cybersecurity posture.* DFARS clause 252.204–7012 does not provide for the DoD verification of a DIB contractor's implementation of the security requirements specified in NIST SP 800–171 prior to contract award. DIB companies self-attest that they will implement the requirements in NIST SP 800–171 upon submission of their offer. Findings from DoD Inspector General report (DODIG–2019–105 ''Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems'') indicate that DoD contractors did not consistently implement mandated system security requirements for safeguarding CUI and recommended that DoD take steps to assess a contractor's ability to protect this information. CMMC adds the element of verification of a DIB contractor's cybersecurity posture through the use of accredited C3PAOs. The company must achieve the CMMC level certification required as a condition of contract award.

• *Comprehensive implementation of cybersecurity requirements.* Under DFARS clause 252.204–7012, a contractor can document implementation of the security requirements in NIST SP 800–171 by having a system security plan in place to describe how the security requirements are implemented, in addition to associated plans of action to describe how and when any unimplemented security requirements will be met. The CMMC framework does not allow a DoD contractor or subcontractor to achieve compliance status through the use of plans of action. In general, CMMC takes a risk-based approach to addressing cyber threats. Based on the type and sensitivity of the information to be protected, a DIB company must achieve the appropriate CMMC level and demonstrate implementation of the requisite set of processes and practices. Although the security requirements in NIST SP 800–171 addresses a range of threats, additional requirements are needed to further reduce the risk of Advanced Persistent Threats (APTs). An APT is an adversary that possesses sophisticated levels of expertise and significant resources, which allow it to create opportunities to achieve its objectives by using multiple attack vectors (*e.g.* cyber, physical, and deception). The CMMC model includes additional processes and practices in Levels 4 and 5 that are focused on further reducing the risk of APT threats. The CMMC implementation will provide the Department with an ability to illuminate the supply chain, for the first time, at scale across the entire DIB sector. The CMMC framework requires contractors to flow down the appropriate CMMC

certification requirement to subcontractors throughout the entire supply chain. DIB companies that do not process, store, or transmit CUI, must obtain a CMMC level 1 certification. DIB companies that process, store, or transmit CUI must achieve a CMMC level 3 or higher, depending on the sensitivity of the information associated with a program or technology being developed.

• *Scale and Depth.* DoD contractors must include DFARS clause 252.204–7012 in subcontracts for which subcontract performance will involve covered defense information (DoD CUI), but this does not provide the Department with sufficient insights with respect to the cybersecurity posture of DIB companies throughout the multi-tier supply chain for any given program or technology development effort. Given the size and scale of the DIB sector, the Department cannot scale its organic cybersecurity assessment capability to conduct on-site assessments of approximately 220,000 DoD contractors every three years. As a result, the Department's organic assessment capability is best suited for conducting targeted assessments for a subset of DoD contractors that support prioritized programs and/or technology development efforts. CMMC addresses the challenges of the Department scaling its organic assessment capability by partnering with an independent, non-profit CMMC–AB that will accredit and oversee multiple third party assessment organizations (C3PAOs) which in turn, will conduct on-site assessments of DoD contractors throughout the multi-tier supply chain. DIB companies will be able to directly schedule assessments with an accredited C3PAO for a specific CMMC level. The cost of these CMMC assessments will be driven by multiple factors including market forces, the size and complexity of the network or enclaves under assessment, and the CMMC level.

• *Reduces Duplicate or Repetitive Assessments of our Industry Partners.* Assessment results will be posted in the Supplier Performance Risk System (SPRS), DoD's authoritative source for supplier and product performance information. This will provide DoD Components with visibility to CMMC certifications for DIB contractor networks and an alternative to addressing implementation of NIST SP 800–171 on a contract-by-contract approach—significantly reducing the need to conduct assessments at the program level, thereby reducing the cost to both DoD and industry.

C. Description of and Estimate of the Number of Small Entities to Which the Rule Will Apply

This rule will impact all small businesses that do business with Department of Defense, except those competing on contracts or orders that are exclusively for COTS items or receiving contracts or orders valued at or below the micro-purchase threshold.

1. The NIST SP 800–171 DoD Assessment Methodology

According to data available in the Electronic Data Access system for fiscal years (FYs) 2016, 2017, and 2018, on an annual basis DoD awards on average 485,859 contracts and orders that contain DFARS clause 252.204–7012 to 39,204 unique awardees, of which 262,509 awards (54 percent) are made to 26,468 small entities (68 percent). While there may be some entities that have contracts that contain the clause at 252.204–7012, but never process CUI and, therefore, do not have to implement NIST SP 800–171, it is not possible for DoD to estimate what fraction of unique entities fall into this category. Assuming all of these small entities have covered contractor information systems that are required to be in compliance with NIST SP 800–171, then all of these entities would be required to have, at minimum, a Basic Assessment in order to be considered for award.

The requirement for the Basic Assessment would be imposed through incorporation of the new solicitation provision and contract clause in new contracts and orders. As such, the requirement to have completed a Basic Assessment is expected to phase-in over a three-year period, thus impacting an estimated 8,823 small entities each year. It is expected that the Medium and High Assessments, on the other hand, will be conducted on a finite number of awardees each year based on the capacity of the Government to conduct these assessments. DoD estimates that 200 unique entities will undergo a Medium Assessment each year, of which 148 are expected to be small entities. High Assessments are expected to be conducted on approximately 110 unique entities each year, of which 81 are expected to be small entities. DoD Assessments are valid for three years, so small entities will be required to renew, at minimum, their basic assessment every three years in order to continue to receive DoD awards or to continue performance on contracts and orders with options. The following is a summary of the number of small entities that will be required to undergo NIST SP 800–171 DoD Assessments over a three-year period:

Assessment	Year 1	Year 2	Year 3
Basic	8,823	8,823	8,823
Medium	148	148	148
High	81	81	81

The top five NAICS code industries expected to be impacted by this rule are as follows: 541712, Research and Development in the Physical, Engineering, and Life Sciences (Except Biotechnology); 541330, Engineering Services; 236220, Commercial and Institutional Building Construction; 541519, Other Computer Related Services; and 561210, Facilities Support Services. These NAICS codes were selected based on a review of NAICS codes associated with awards that include the clause at DFARS 252.204–7012.

2. The CMMC Framework

Given the enterprise-wide implementation of CMMC, the Department developed a five-year phased rollout strategy. The rollout is intended to minimize the financial impacts to the industrial base, especially small entities, and disruption to the existing DoD supply chain. The Office of the Secretary of Defense staff is coordinating with the Military Services and Department Agencies to identify candidate contracts during the first five years of implementation that will include the CMMC requirement in the statement of work.

Prior to October 1, 2025, this rule impacts certain large and small businesses that are competing on acquisitions that specify a requirement for CMMC in the statement of work. These businesses will be required to have the stated CMMC certification level at the time of contract award. Inclusion of a CMMC requirement in a

solicitation during this time period must be approved by the USD(A&S). It is estimated that 129,810 unique entities will pursue their initial CMMC certification during the initial five-year period. By October 1, 2025, all entities receiving DoD contracts and orders, other than contracts or orders exclusively for commercially available off-the-shelf items or those valued at or below the micro-purchase threshold, will be required to have the CMMC Level identified in the solicitation, but which at minimum will be a CMMC Level 1 certification. CMMC certifications are valid for three years; therefore, large and small businesses will be required to renew their certification every three years.

Based on information from the Federal Procurement Data System (FPDS), the number of unique prime contractors is 212,657 and the number of known unique subcontractors is 8,309. Therefore, the total number of known unique prime contractors and subcontractors is 220,966, of which approximately 163,391 (74 percent) are estimated to be unique small businesses. According to FPDS, the average number of new contracts for unique contractors is 47,905 for any given year. The timeline required to implement CMMC across the DoD contractor population will be approximately 7 years. The phased rollout plan for years 1–7 for small entities is detailed below with the total number of unique DoD contractors and subcontractors specified. The rollout assumes that for every unique prime contractor there are approximately 100 unique subcontractors. Each small business represented in the table would be required to pursue recertification every three years in order to continue to do business with DoD.

Year	Level 1	Level 2	Level 3	Level 4	Level 5	Total
1	665	110	335	0	0	1,110
2	3,323	555	1,661	2	2	5,543
3	11,086	1,848	5,543	4	4	18,485
4	21,248	3,542	10,624	6	6	35,426
5	21,245	3,541	10,623	7	7	35,423
6	21,245	3,541	10,623	7	7	35,423
7	19,180	3,197	9,590	7	7	31,981
1–7	97,992	16,334	48,999	33	33	163,391

The top five NAICS code industries expected to be impacted by this rule are as follows: 541712, Research and Development in the Physical, Engineering, and Life Sciences (Except Biotechnology); 541330, Engineering Services; 236220, Commercial and Institutional Building Construction; 541519, Other Computer Related Services; and 561210, Facilities Support Services. These NAICS codes are the same as the DoD Assessment NAICS codes and were selected based on a review of NAICS codes associated with awards that include the clause at FAR 52.204–21 or DFARS 252.204–7012.

D. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements of the Rule

Details on the compliance requirements and associated costs, savings, and benefits of this rule are provided in the Regulatory Impact Analysis referenced in section IV of this preamble. The following is a summary of the compliance requirements and the estimated costs for small entities to undergo a DoD NIST SP 800–171 Assessment or obtain a CMMC certification. For both the DoD Assessment Methodology and the CMMC Framework, the estimated public costs are based on the cost for an entity to pursue each type of assessment: The Basic, Medium, or High Assessment under the DoD Assessment Methodology; or the CMMC Level 1, 2, 3, 4, or 5 certifications. The estimated costs attributed to this rule do not include the costs associated with compliance with the existing cybersecurity requirements under the clause at FAR 52.204–21 or associated with implementing NIST SP 800–171 in accordance with the clause at DFARS 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. Contractors who have been awarded a DoD contract that include these existing contract clauses should have already implemented these cybersecurity requirements and incurred the associated costs; therefore, those costs are not attributed to this rule.

1. DoD Assessment Methodology

To comply with NIST SP 800–171 a company must (1) implement 110 security requirements on their covered contractor information systems; or (2) document in a ''system security plan'' and ''plans of action'' those requirements that are not yet implemented and when the requirements will be implemented. All offerors that are required to implement NIST SP 800–171 on covered contractor information systems pursuant to DFARS clause 252.204–7012, will be required to complete a Basic Assessment and upload the resulting score to the Supplier Risk Management System (SPRS), DoD's authoritative source for supplier and product performance information. The Basic Assessment is a self-assessment done by the contractor using a specific scoring methodology that tells the Department how many security requirements have not yet been implemented and is valid for three years. A company that has fully implemented all 110 NIST SP 800–171 security requirements, would have a score of 110 to report in SPRS for their Basic Assessment. A company that has unimplemented requirements will use the scoring methodology to assign a value to each unimplemented requirement, add up those values, and subcontract the total value from 110 to determine their score.

In accordance with NIST SP 800–171, a contractor should already be aware of the security requirements they have not yet implemented and have documented plans of action for those requirements; therefore, the burden associated with conducting a self-assessment is the time burden associated with calculating the score. DoD estimates that the burden to calculate the Basic Assessment score is thirty minutes per entity at a journeyman-level-2 rate of pay (0.50 hour * $99.08/hour = $49.54/assessment)).

To submit the Basic Assessment, the contractor is required to complete 6 fields: System security plan name (if more than one system is involved); CAGE code associated with the plan; a brief description of the plan architecture; date of the assessment; total score; and the date a score of 110 will be achieved. All of this data is available from the Basic Assessment itself, the existing system security plan, and the plans of action. The contractor selects the date when the last plan of

action will be complete as the date when a score of 110 will be achieved. The burden to submit a Basic Assessment for posting in SPRS is estimated to be 15 minutes per entity at a journeyman-level-2 rate of pay (0.25 hour * $99.08/hour = $24.77/assessment)). Therefore, the total cost per assessment per entity is approximately $74.31 ($49.54 + $24.77).

The estimate for the rate of pay for both preparation and submission of the Basic Assessment is journeyman-level-2, which is an employee who has the equivalent skills, responsibilities, and experience as a General Schedule (GS) 13 Federal Government employee. While these are rather simple tasks that can reasonably be completed by a GS–11 equivalent employee, or even a GS–9 clerk, the GS–13 (or perhaps GS–11) is the most likely grade for several reasons. First, in a small company, the number of IT personnel are very limited. The employee that is available to complete this task would also have significant responsibilities for operation and maintenance of the IT system and, therefore, be at a higher grade than would otherwise be required if the only job was to prepare and submit the assessment. Second, while the calculation of the assessment is simple, the personnel who would typically have access to and understand the system security plan and plans of action in order to complete the Basic Assessment would be at the higher grade. Third, while the actual submission is a simple task, the person who would complete the assessment and submit the data in SPRS would be the person with SPRS access/responsibilities, and therefore at the higher grade. Fourth, given that proper calculation of the score and its submission may well determine whether or not the company is awarded the contract, the persons preparing and submitting the report are likely to be at a higher grade than is actually required to ensure this is done properly.

After a contract is awarded, DoD may choose to conduct a Medium or High Assessment of an offer based on the criticality of the program or the sensitivity of information being handled by the contractor. Under both the Medium and High Assessment DoD assessors will be reviewing the contractor's system security plan description of how each NIST SP 800–171 requirement is met and will identify any descriptions that may not properly address the security requirements. The contractor provides DoD access to its facilities and personnel, if necessary, and prepares for/participates in the assessment conducted by the DoD. Under a High Assessment a contractor will be asked to demonstrate their system security plan. DoD will post the results in SPRS.

For the Medium Assessment, DoD estimates that the burden for a small entity to make the system security plan and supporting documentation available for review by the DoD assessor is one hour per entity at a journeyman-level-2 rate of pay, a cost of $99.08/assessment (1 hour * $99.08/hour). It is estimated that the burden for a small entity to participate in the review and discussion of the system security plan and supporting documents with the DoD assessor is three hours, with one journeyman-level-2 and one senior-level-2 contractor employee participating in the assessment, a cost of $710.40/assessment ((3 hours * $99.08/hour = $297.24) + (3 hours * $137.72/hour = $413.16)). Assuming issues are identified by the DoD Assessor, DoD estimates that the burden for a small entity to determine and provide to DoD the date by which the issues will be resolved is one hour per entity at a journeyman-level rate of pay, a cost of $99.08/assessment (1 hour * $99.08/hour). Therefore, total estimated cost for a small entity that undergoes a Medium Assessment is $908.56/assessment ($99.08 + $710.40 + $99.08).

For the High Assessment, DoD estimates that the burden for a small entity to participate in the review and discussion of the system security plan and supporting documents to the DoD assessors is 116 hours per entity at a cost of $14,542.24/assessment. The cost estimate is based on 2 senior-level-2 employees dedicating 32 hours each, 8 senior-level-1 employees dedicating 4 hours each, and 10 journeyman-level employees dedicating 2 hours each ((2 * 32 hours * $137.72/hour = $8,814.08) + (8 * 4 hours * 117.08/hour = $3,746.56) + (10 * 2 hours * $99.08/hour = 1,981.60)). It is estimated that the burden to make the system security plan and supporting documentation available for review by the DoD assessors, prepare for demonstration of requirements implementation, and to conduct post review activities is 304 hours per entity, at a cost of $36,133.76/assessment. The cost estimate is based on 2 senior-level-2 employees dedicating 48 hours each, 8 senior-level-1 employees dedicating 16 hours each, and 10 journeyman-level employees dedicating 8 hours each ((2 * 48 hours * $137.72/hour = $13,221.12) + (8 * 16 hours * 117.08/hour = $14,986.24) + (10 * 8 hours * $99.08/hour = $7,926.40)). Therefore, total estimated cost for a small entity that undergoes a High Assessment is $50,676/assessment ($14,542.24 + $36,133.76). DoD considers this to be the upper estimate of the cost, as it assumes a very robust information technology workforce. For many smaller companies, which may not have a complex information system to manage, the information system staff will be a much more limited, and labor that can be devoted (or is necessary) to prepare for and participate in the assessment is likely to be significantly less than estimated.

The following table provides the estimated annual costs for small entities to comply with the DoD Assessment requirements of this rule. Since assessments are valid for three years, the cost per assessment has been divided by three to estimate the annual cost per entity:

Assessment	Cost/ assessment	Annual cost/entity	Total unique entities	Annual cost all entities
Basic	$75	$25	26,469	$655,637
Medium	909	303	444	134,467
High	50,676	16,892	243	4,104,756
Total	.....	.....	27,156	4,894,860

The following table presents the average annual cost per small entity for each DoD Assessment as a percentage of the annual revenue for a small entity for four of the top five NAICS codes. The low-end of the range of annual revenues presented in the table includes the average annual revenue for smaller sized firms. The high-end of the range includes the maximum annual revenue allowed by the Small Business Administration (SBA) for a small

business, per the SBA's small business size standards published at 13 CFR 121.201. NAICS code 541712 is excluded, because it is no longer an active NAICS code and the prior size standard was based on number of employees.

NAICS code	Range of annual revenues for small businesses (in millions)	Basic assessment annual cost as % of annual revenue	Medium assessment annual cost as % of annual revenue	High assessment annual cost as % of annual revenue
541330	$5–16.5	0.0005–0.0002	0.0061–0.0018	0.3378–0.1024
236220	$10–$39.5	0.0002–0.0001	0.0030–0.0008	0.1689–0.0428
541519	$10–$30.0	0.0002–0.0001	0.0030–0.0010	0.1689–0.0563
561210	$10–$41.5	0.0002–0.0001	0.0030–0.0007	0.1689–0.0407

2. CMMC Framework

This rule adds DFARS clause 252.204–7021, Cybersecurity Maturity Model Certification Requirement, which requires the contractor to have the CMMC certification at the level required in the solicitation by contract award and maintain the required CMMC level for the duration of the contract. In order to achieve a specific CMMC level, a DIB company must demonstrate both process institutionalization or maturity and the implementation of practices commensurate with that level. A DIB contractor can achieve a specific CMMC level for its entire enterprise network or particular segment(s) or enclave(s), depending upon where the information to be protected is processed, stored, or transmitted.

The following table provides a high-level description of the processes and practices evaluated during a CMMC assessment at each level; however, more specific information on the processes and practices associated with each CMMC Level is available at *https://www.acq.osd.mil/cmmc/index.html.*

Level	Description
1	Consists of the 15 basic safeguarding requirements from FAR clause 52.204–21.
2	Consists of 65 security requirements from NIST SP 800–171 implemented via DFARS clause 252.204–7012, 7 CMMC practices, and 2 CMMC processes. Intended as an optional intermediary step for contractors as part of their progression to Level 3.
3	Consists of all 110 security requirements from NIST SP 800–171, 20 CMMC practices, and 3 CMMC processes.
4	Consists of all 110 security requirements from NIST SP 800–171, 46 CMMC practices, and 4 CMMC processes.
5	Consists of all 110 security requirements from NIST SP 800–171, 61 CMMC practices, and 5 CMMC processes.

CMMC Assessments will be conducted by C3PAOs, which are accredited by the CMMC–AB. C3PAOs will provide CMMC Assessment reports to the CMMC–AB who will then maintain and store these reports in appropriate database(s). The CMMC–AB will issue CMMC certificates upon the resolution of any disputes or anomalies during the conduct of the assessment. These CMMC certificates will be distributed to the DIB contractor and the requisite information will be posted in SPRS.

If a contractor disputes the outcome of a C3PAO assessment, the contractor may submit a dispute adjudication request to the CMMC–AB along with supporting information related to claimed errors, malfeasance, or ethical lapses by the C3PAO. The CMMC–AB will follow a formal process to review the adjudication request and provide a preliminary evaluation to the contractor and C3PAO. If the contractor does not accept the CMMC–AB preliminary finding, the contractor may request an additional assessment by the CMMC–AB staff.

The costs associated with the preparation and the conduct of CMMC Assessments assumes that a small DIB company, in general, possesses a less complex and less expansive IT and cybersecurity infrastructure and operations relative to a larger DIB company. In estimating the cost for a small DIB company to obtain a CMMC certification, DoD took into account non-recurring engineering costs, recurring engineering costs, the cost to participate in the assessment, and re-certification costs:

- Nonrecurring engineering costs consist of hardware, software, and the associated labor. The costs are incurred only in the year of the initial assessment.
- Recurring engineering costs consist of any recurring fees and associated labor for technology refresh. The recurring engineering costs associated with technology refresh have been spread uniformly over a 5-year period (*i.e.,* 20% each year as recurring engineering costs).
- Assessment costs consist of contractor support for pre-assessment preparations, the actual assessment, and any post-assessment work. These costs also include an estimate of the potential C3PAO costs for conducting CMMC Assessment, which are comprised of labor for supporting pre-assessment preparations, actual assessment, and post-assessment work, plus travel cost.
- Re-certification costs are the same as the initial certification cost.

The following is a summary of the estimated costs for a small entity to achieve certification at each CMMC Level.

i. Level 1 Certification

Contractors pursuing a Level 1 Certification should have already implemented the 15 existing basic safeguarding requirements under FAR clause 52.204–21. Therefore, there are no estimated nonrecurring or recurring engineering costs associated with CMMC Level 1.

DoD estimates that the cost for a small entity to support a CMMC Level 1 Assessment or recertification is $2,999.56:

- *Contractor Support.* It is estimated that one journeyman-level-1 employee will dedicate 14 hours to support the assessment (8 hours for pre- and post-assessment support + 6 hours for the assessment). The estimated cost is $1,166.48 (1 journeyman * $83.32/hour * 14 hours).
- *C3PAO Assessment.* It is estimated that one journeyman-level-1 employee will dedicate 19 hours to conduct the assessment (8 hours for pre- and post-assessment support + 6 hours for the assessment + 5 hours for travel). Each employee is estimated to have 1 day of per diem for travel. The estimated cost

is $1,833.08 ((1 journeyman * $83.32/hour * 19 hours = $1,583.08) + (1 employees * 1 day * $250/day = $250 travel costs)).

ii. Level 2 Certification

Contractors pursuing a Level 2 Certification should have already implemented the 65 existing NIST SP 800–171 security requirements. Therefore, the estimated engineering costs per small entity is associated with implementation of 9 new requirements (7 CMMC practices and 2 CMMC processes). The estimated nonrecurring engineering cost per entity per assessment/recertification is $8,135. The estimated recurring engineering cost per entity per year is $20,154.

DoD estimates that the cost for a small entity to support a CMMC Level 2 Assessment or recertification is $22,466.88.

- *Contractor Support.* It is estimated that two senior-level-1 employees will dedicate 48 hours each to support the assessment (24 hours for pre- and post-assessment support + 24 hours for the assessment). The estimated cost is $11,239.68 (2 senior * $117.08/hour * 48 hours).
- *C3PAO Assessment.* It is estimated that one journeyman-level-2 employee and one senior-level-1 employee will dedicate 45 hours each to conduct the assessment (16 hours for pre- and post-assessment support + 24 hours for the assessment + 5 hours for travel). Each employee is estimated to have 3 days of per diem for travel. The estimated cost is $11,227.20 ((1 senior * $117.08/hour * 45 hours = $5,268.60) + (1 journeyman * $99.08/hour * 45 hours = $4,458.60) + (2 employees * 3 days * $250/day = $1,500 travel costs)).

iii. Level 3 Certification

Contractors pursuing a Level 3 Certification should have already implemented the 110 existing NIST SP 800–171 security requirements. Therefore, the estimated engineering costs per small entity is associated with implementation 23 new requirements (20 CMMC practices and 3 CMMC processes). The estimated nonrecurring engineering cost per entity per assessment/recertification is $26,214. The estimated recurring engineering cost per entity per year is $41,666.

DoD estimates that the cost for a small entity to support a CMMC Level 3 assessment or recertification is $51,095.60.

- *Contractor Support.* It is estimated that three senior-level-1 employees will dedicate 64 hours each to support the assessment (32 hours for pre- and post-assessment support + 32 hours for the assessment). The estimated cost is $22,479.36 (3 seniors * $117.08/hour * 64 hours).
- *C3PAO Assessment.* It is estimated that one senior-level-1 employee and three journeyman-level-2 employees will dedicate 57 hours each to conduct the assessment (24 hours for pre- and post-assessment support + 32 hours for the assessment + 5 hours for travel). Each employee is estimated to have 5 days of per diem for travel. The estimated cost is $28,616.24 ((1 senior * $117.08/hour * 57 hours = $6,673.56) + (3 journeyman * $99.08/hour * 57 hours = $16,942.68) + (4 employees * 5 days * $250/day = $5,000 travel costs)).

iv. Level 4 Certification

Contractors pursuing a Level 4 Certification should have already implemented the 110 existing NIST SP 800–171 security requirements. Therefore, the estimated engineering costs per small entity is associated with implementation 50 new requirements (46 CMMC practices and 4 CMMC processes). The estimated nonrecurring engineering cost per entity per assessment/recertification is $938,336. The estimated recurring engineering cost per entity per year is $301,514.

DoD estimates that the cost for a small entity to support a CMMC Level 4 Assessment or recertification is $70,065.04.

- *Contractor Support.* It is estimated that three senior-level-2 employees will dedicate 80 hours each to support the assessment (40 hours for pre- and post-assessment support + 40 hours for the assessment). The estimated cost is $33,052.80 (3 seniors * $137.72/hour * 80 hours)
- *C3PAO Assessment.* It is estimated that one senior-level-2 employee and three journeyman-level-2 employees will dedicate 69 hours each to conduct the assessment (32 hours for pre- and post-assessment support + 48 hours for the assessment + 5 hours for travel). Each employee is estimated to have 5 days of per diem for travel, plus airfare. The estimated cost is $37,012.24 ((1 senior * $137.72/hour * 69 hours = $9502.68) + (3 journeyman * $99.08/hour * 69 hours = $20,509.56) + (4 employees * 5 days * $250/day = $5,000 travel costs) + (4 employees * $500 = $2,000 airfare)).

v. Level 5 Certification

Contractors pursuing a Level 5 Certification should have already implemented the 110 existing NIST SP 800–171 security requirements. Therefore, the estimated engineering costs per small entity is associated with implementation 66 new requirements (61 CMMC practices and 5 CMMC processes). The estimated nonrecurring engineering cost per entity per assessment/recertification is $1,230,214. The estimated recurring engineering cost per entity per year is $384,666.

DoD estimates that the cost for a small entity to support a CMMC Level 5 Assessment or recertification is $110,090.80.

- *Contractor Support.* It is estimated that four senior-level-2 employees will dedicate 104 hours each to support the assessment (48 hours for pre- and post-assessment support + 56 hours for the assessment). The estimated cost is $57,291.52 (4 senior * $137.72/hour * 104 hours).
- *C3PAO Assessment.* It is estimated that one senior-level-2 employee, two senior-level-1 employees, and one journeyman-level-2 employee will dedicate 93 hours each to conduct the assessment (32 hours for pre- and post-assessment support + 56 hours for the assessment + 5 hours for travel). Each employee is estimated to have 7 days of per diem for travel. The estimated cost is $52,799.28 ((1 senior * $137.72/hour * 93 hours = $12,807.96) + (2 senior * $117.08/hour * 93 hours = $21,776.88) + (1 journeyman * $99.08/hour * 93 hours = $9,214.44) + (4 employees * 7 days * $250/day = $7,000 travel costs) + (4 employees * $500 = $2,000 airfare)).

vi. Total Estimated Annual Costs

The following table provides a summary of the total estimated annual costs for an individual small entity to obtain each CMMC certification level. Nonrecurring engineering costs are spread over a 20-year period to determine the average annual cost per entity. Assessment costs have been spread over a 3-year period, since entities will participate in a reassessment every 3 years.

CMMC cert	Average nonrecurring engineering costs	Recurring engineering costs	Average assessment costs	Total annual assessment cost
Level 1	$0	$0	$1,000	$1,000

CMMC cert	Average nonrecurring engineering costs	Recurring engineering costs	Average assessment costs	Total annual assessment cost
Level 2	407	20,154	7,489	28,050
Level 3	1,311	41,666	17,032	60,009
Level 4	46,917	301,514	23,355	371,786
Level 5	61,511	384,666	36,697	482,874

The following table presents the average annual cost per small entity for CMMC certifications at levels 1 through 3 as a percentage of the annual revenue for a small entity for four of the top five NAICS codes. The low-end of the range of annual revenues presented in the table includes the average annual revenue for smaller sized firms. The high-end of the range includes the maximum annual revenue allowed by the SBA for a small business, per the SBA's small business size standards published at 13 CFR 121.201. NAICS code 541712 is excluded, because it is no longer an active NAICS code and the prior size standard was based on number of employees.

NAICS code	Range of annual revenues for small businesses (in millions)	CMMC level 1 annual cost as % of annual revenue	CMMC level 2 annual cost as % of annual revenue	CMMC level 3 annual cost as % of annual revenue
541330	$5–$16.5	0.0200–0.0061	0.5610–0.1700	1.2002–0.3637
236220	$10–$39.5	0.0100–0.0025	0.2805–0.0710	0.6001–0.1519
541519	$10–$30.0	0.0100–0.0033	0.2805–0.0935	0.6001–0.2000
561210	$10–$41.5	0.0100–0.0024	0.2805–0.0676	0.6001–0.1446

For CMMC certification at levels 4 and 5, the following table presents the annual cost per small entity for CMMC certification at levels 4 and 5 as a percentage of the low, average, and high annual revenues for entities that have represented themselves as small in the System for Award Management (SAM) for their primary NAICS code and are performing on contracts that could be subject to a CMMC level 4 or 5 certification requirements. The values of the low, average, and high annual revenues are based on an average of the annual receipt reported in SAM by such entities for FY16 through FY20.

FY16 thru FY20	Annual revenue of entities represented as small for primary NAICS	Level 4 certification cost as % of annual revenue	Level 5 certification cost as % of annual revenue
Low	$6.5 million	5.67	7.36
Average	$22.9 million	1.62	2.11
High	$85 million	0.43	0.56

The following is a summary of the estimated annual costs in millions for all 163,391 small entities to achieve their initial CMMC certifications (and recertifications every three years) over a 10-year period:

Year	Level 1	Level 2	Level 3	Level 4	Level 5
1	$1.99	$5.58	$39.86	$0.00	$0.00
2	9.97	30.39	211.58	2.62	3.45
3	33.25	107.20	742.65	5.84	7.67
4	65.73	232.90	1,595.23	9.67	12.66
5	73.69	314.23	2,105.53	12.93	16.91
6	96.98	414.64	2,746.50	15.18	19.82
7	123.26	509.08	3,342.95	17.43	22.74
8	73.69	421.22	2,669.25	10.58	13.68
9	96.98	450.27	2,867.60	10.72	13.90
10	123.26	483.07	3,091.56	10.86	14.13

E. Relevant Federal Rules, Which May Duplicate, Overlap, or Conflict With the Rule

The rule does not duplicate, overlap, or conflict with any other Federal rules. Rather this rule validates and verifies contractor compliance with the existing cybersecurity requirements in FAR clause 52.204–21 and DFARS clause 252.204–7012, and ensures that the entire DIB sector has the appropriate cybersecurity processes and practices in place to properly protect FCI and CUI during performance of DoD contracts.

F. Description of Any Significant Alternatives to the Rule Which Accomplish the Stated Objectives of Applicable Statutes and Which Minimize Any Significant Economic Impact of the Rule on Small Entities

DoD considered and adopted several alternatives during the development of

this rule that reduce the burden on small entities and still meet the objectives of the rule. These alternatives include: (1) Exempting contracts and orders exclusively for the acquisition of commercially available off-the-shelf items; and (2) implementing a phased rollout for the CMMC portion of the rule and stipulating that the inclusion a CMMC requirement in new contracts until that time be approved by the Office of the Under Secretary of Defense for Acquisition and Sustainment. Additional alternatives were considered, however, it was determined that these other alternatives did not achieve the intended policy outcome.

1. CMMC Model and Implementation

The Regulatory Impact Analysis (RIA) referenced in section IV of this preamble estimates that the total number of unique DoD contractors and subcontractors is 220,966, with approximately 163,391 or 74% being small entities. The RIA also specifies the estimates for the percentage of all contractors and subcontractors associated with each CMMC level. These estimates indicate that the vast majority of small entities (*i.e.,* 163,325 of 163,391 or 99.96%) will be required to achieve CMMC Level 1–3 certificates during the initial rollout. The Department looked at Levels 1 through 5 to determine if there were alternatives and whether these alternatives met the intended policy outcome.

For CMMC Level 1, the practices map directly to the basic safeguarding requirements specified in the clause at FAR 52.204–21. The phased rollout estimates that the majority of small entities (*i.e.,* 97,992 of the 163,325 or 60%) will be required to achieve CMMC Level 1. The planned implementation of CMMC Level 1 adds a verification component to the existing FAR clause by including an on-site assessment by a credentialed assessor from an accredited C3PAO. The on-site assessment verifies the implementation of the required cybersecurity practices and further supports the physical identification of contractors and subcontractors in the DoD supply chain. In the aggregate, the estimated cost associated with supporting this on-site assessment and approximated C3PAO fees does not represent a cost-driver with respect to CMMC costs to small entities across levels. An alternative to an on-site assessment is for contractors to provide documentation and supporting evidence of the proper implementation of the required cybersecurity practices through a secure online portal. These artifacts would then be reviewed and checked virtually by an accredited assessor prior to the CMMC–AB issuing a CMMC Level 1 certificate. The drawback of this alternative is the inability of the contractor to interact with the C3PAO assessor in person and provide evidence directly without transmitting proprietary information. Small entities will not receive as much meaningful and interactive feedback that would be part of a Level 1 on-site assessment.

For CMMC Level 2, the practices encompass only 48 of the 110 security requirements of NIST SP 800–171, as specified in DFARS clause 252.204–7012, and 7 additional cybersecurity requirements. In addition, CMMC Level 2 includes two process maturity requirements. The phased rollout estimates that approximately 10% of small entities may choose to use Level 2 as a transition step from Level 1 to Level 3. Small entities that achieve Level 1 can seek to achieve Level 3 (without first achieving a Level 2 certification) if the necessary cybersecurity practices and processes have been implemented. The Department does not anticipate releasing new contracts that require contractors to achieve CMMC Level 2. As a result, the Department did not consider alternatives with respect to CMMC Level 2.

For CMMC Level 3, the practices encompass all the 110 security requirements of NIST SP 800–171, as specified in DFARS clause 252.204–7012, as well as 13 additional cybersecurity requirements above Level 2. In addition, CMMC Level 3 includes three process maturity requirements. These additional cybersecurity practices were incorporated based upon several considerations that included public comments from September to December 2019 on draft versions of the model, inputs from the DIB Sector Coordinating Council (SCC), cybersecurity threats, the progression of cybersecurity capabilities from Level 3 to Levels 4, and other factors. The CMMC phased rollout estimates that 48,999 of the 163,325 small entities or 30% will be required to achieve CMMC Level 3. The alternatives considered include removing a subset or all of the 20 additional practices at Level 3 or moving a subset or all of the 20 additional practices from Level 3 to Level 4. The primary drawback of these alternatives is that the cybersecurity capability gaps associated with protecting CUI will not be addressed until Level 4, which will apply to a relatively small percentage of non-small and small entities. Furthermore, the progression of cybersecurity capabilities from Level 3 to Level 4 becomes more abrupt.

For CMMC Level 4, the practices encompass the 110 security requirements of NIST SP 800–171 as specified in DFARS clause 252.204–7012 and 46 additional cybersecurity requirements. More specifically, CMMC Level 4 adds 26 enhanced security requirements above CMMC Level 3, of which 13 are derived from Draft NIST SP 800–171B. In addition, CMMC Level 4 includes four process maturity requirements. The DIB SCC and the public contributed to the specification of the other 13 enhanced security requirements. For CMMC Level 4, an alternative considered is to define a threshold for contractors to meet 15 out of the 26 enhanced security requirements. In addition, contractors will be required to meet 6 out of the 11 remaining non-threshold enhanced security requirements. This alternative implies that a contractor will have to implement 21 of the 26 enhanced security requirements as well as the associated maturity processes. A drawback of this alternative is that contractors implement a different subset of the 11 non-threshold requirements which in turn, leads to a non-uniform set of cybersecurity capabilities across those certified at Level 4.

For CMMC Level 5, the practices encompass the 110 security requirements of NIST SP 800–171 as specified in DFARS clause 252.204–7012 and 61 additional cybersecurity requirements. More specifically, CMMC Level 5 adds 15 enhanced security requirements above CMMC Level 4, of which 4 are derived from Draft NIST SP 800–171B. In addition, CMMC Level 5 includes five process maturity requirements. The DIB SCC and the public contributed to the specification of the other 11 enhanced security requirements. For CMMC Level 5, the alternative considered is to define a threshold for contractors to meet 6 out of the 15 enhanced security requirements. In addition, contractors will be required to meet 5 out of the 9 remaining non-threshold enhanced security requirements. This alternative implies that a contractor will have implemented 11 of the 15 enhanced security requirements as well as the associated maturity processes. A drawback of this alternative is that contractors implement a different subset of the 9 non-threshold requirements which in turn, leads to a non-uniform set of cybersecurity capabilities across those certified at Level 5.

2. Timing of CMMC Level Certification Requirement

In addition to evaluating the make-up of the CMMC levels, the Department

took into consideration the timing of the requirement to achieve a CMMC level certification: (1) At time of proposal or offer submission, (2) in order to receive award, or (3) post contract award. The Department ultimately adopted alternative 2 to require certification at the time of award. The drawback of alternative 1 (at time of proposal or offer submission) is the increased risk for contractors since they may not have sufficient time to achieve the required CMMC certification after the release of the Request for Information (RFI). The drawback of alternative 3 (after contract award) is the increased risk to the Department with respect to the schedule and uncertainty with respect to the case where the contractor is unable to achieve the required CMMC level in a reasonable amount of time given their current cybersecurity posture. This potential delay would apply to the entire supply chain and prevent the appropriate flow of CUI and FCI. The Department seeks public comment on the timing of contract award, to include the effect of requiring certification at time of award on small businesses.

DoD invites comments from small business concerns and other interested parties on the expected impact of this rule on small entities. DoD will also consider comments from small entities concerning the existing regulations in subparts affected by this rule in accordance with 5 U.S.C. 610. Interested parties must submit such comments separately and should cite 5 U.S.C. 610 (DFARS Case 2019–D041), in correspondence.

VIII. Paperwork Reduction Act

The Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*) (PRA) provides that an agency generally cannot conduct or sponsor a collection of information, and no person is required to respond to nor be subject to a penalty for failure to comply with a collection of information, unless that collection has obtained OMB approval and displays a currently valid OMB Control Number.

DoD requested, and OMB authorized, emergency processing of the collection of information tied to this rule, as OMB Control Number 0750–0004, *Assessing Contractor Implementation of Cybersecurity Requirements,* consistent with 5 CFR 1320.13.

DoD has determined the following conditions have been met:

a. The collection of information is needed prior to the expiration of time periods normally associated with a routine submission for review under the provisions of the PRA, to enable the Department to immediately begin assessing the current status of contractor implementation of NIST SP 800–171 on their information systems that process CUI.

b. The collection of information is essential to DoD's mission. The collection of information is essential to DoD's mission. The National Defense Strategy (NDS) and DoD Cyber Strategy highlight the importance of protecting the Defense Industrial Base (DIB) to maintain national and economic security. To this end, DoD requires defense contractors and subcontractors to implement the NIST SP 800–171 security requirements on information systems that handle CUI, pursuant to DFARS clause 252.204–7012. This DoD Assessment Methodology enables the Department to assess strategically, at a corporate-level, contractor implementation of the NIST SP 800–171 security requirements. Results of a NIST SP 800–171 DoD Assessment reflect the net effect of NIST SP 800–171 security requirements not yet implemented by a contractor.

c. Moreover, DoD cannot comply with the normal clearance procedures, because public harm is reasonably likely to result if current clearance procedures are followed. Authorizing collection of this information on the effective date will motivate defense contractors and subcontractors who have not yet implemented existing NIST SP 800–171 security requirements, to take action to implement the security requirements on covered information systems that process CUI, in order to protect our national and economic security interests. The aggregate loss of sensitive controlled unclassified information and intellectual property from the DIB sector could undermine U.S. technological advantages and increase risk to DoD missions.

Upon publication of this rule, DoD intends to provide a separate 60-day notice in the **Federal Register** requesting public comment for OMB Control Number 0750–0004, *Assessing Contractor Implementation of Cybersecurity Requirements.*

DOD estimates the annual public reporting burden for the information collection as follows:

a. Basic Assessment

Respondents: 13,068.
Responses per respondent: 1.
Total annual responses: 13,068.
Hours per response: .75.
Total burden hours: 9,801.

b. Medium Assessment

Respondents: 200.
Responses per respondent: 1.
Total annual responses: 200.
Hours per response: 8.
Total burden hours: 1,600.

c. High Assessment

Respondents: 110.
Responses per respondent: 1.
Total annual responses: 110.
Hours per response: 420.
Total burden hours: 46,200.

d. Total Public Burden (All Entities)

Respondents: 13,068.
Total annual responses: 13,378.
Total burden hours: 57,601.

e. Total Public Burden (Small Entities)

Respondents: 8,823.
Total annual responses: 9,023.
Total burden hours: 41,821.

The requirement to collect information from offerors and contractors regarding the status of their implementation of NIST SP 800–171 on their information systems that process CUI, is being imposed via a new solicitation provision and contract clause. Per the new provision, if an offeror is required to have implemented the NIST SP 800–171 security requirements on their information systems pursuant to DFARS clause 252.204–7012, then the offeror must have, at minimum, a current self-assessment (or Basic Assessment) uploaded to DoD's Supplier Performance Risk System, in order to be considered for award. Depending on the criticality of the acquisition program, after contract award, certain contractors may be required to participate in a Medium or High assessment to be conducted by DoD assessor. During these post-award assessments, contractors will be required to demonstrate their implementation of NIST SP 800–171 security requirements. Results of a NIST SP 800–171 DoD Assessment reflect the net effect of NIST SP 800–171 security requirements not yet implemented by a contractor.

IX. Determination To Issue an Interim Rule

A determination has been made under the authority of the Secretary of Defense that urgent and compelling reasons exist to promulgate this interim rule without prior opportunity for public comment pursuant to 41 U.S.C. 1707(d) and FAR 1.501–3(b).

Malicious cyber actors have targeted, and continue to target, the DIB sector, which consists of over 200,000 small-to-large sized entities that support the warfighter. In particular, actors ranging from cyber criminals to nation-states continue to attack companies and organizations that comprise the Department's multi-tier supply chain including smaller entities at the lower

tiers. These actors seek to steal DoD's intellectual property to undercut the United States' strategic and technological advantage and to benefit their own military and economic development.

The Department has been focused on improving the cyber resiliency and security of the DIB sector for over a decade as evidenced by the development of minimum cybersecurity standards and the implementation of those standards in the National Institute of Standards and Technology (NIST) Special Publications (SP) and implementation of those standards in the FAR and DFARS. In 2013, DoD issued a final DFARS rule (78 FR 69273) that required contractors to implement a select number of security measures from NIST SP 800–53, Recommended Security Controls for Federal Information Systems and Organizations, to facilitate safeguarding unclassified DoD information within contractor information systems from unauthorized access and disclosure. In 2015, DoD issued an interim DFARS rule (80 FR 81472) requiring contractors that handle Controlled Unclassified Information (CUI) on their information systems to transition by December 31, 2017, from NIST SP 800–53 to NIST SP 800–171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations. NIST SP 800–171 was not only easier to use, but also provided security requirements that greatly increases the protections of Government information in contractor information systems once implemented. And, in 2016, the FAR Council mandated the use of FAR clause 52.204–21, Basic Safeguarding of Covered Contractor Information Systems, to require all Government contractors to implement, at minimum, some basic policies and practices to safeguard Federal Contract Information (FCI) within their information systems. Since then, the Department has been engaging with industry on improving their compliance with these exiting cybersecurity requirements and developing a framework to institutionalize cybersecurity process and practices throughout the DIB sector.

Notwithstanding the fact that these minimum cybersecurity standards have been in effect on DoD contracts since as early as 2013, several surveys and questionnaires by defense industrial associations have highlighted the DIB sector's continued challenges in achieving broad implementation of these security requirements. In a 2017 questionnaire, contractors and subcontractors that responded acknowledged implementation rates of 38% to 54% for at least 10 of the 110 security requirements of NIST SP 800–171.[1] In a separate 2018 survey, 36% of contractors who responded indicated a lack of awareness of DFARS clause 252.204–7012 and 45% of contractors acknowledged not having read NIST SP 800–171.[2] In a 2019 survey, contractors that responded rated their level of preparedness for a Defense Contract Management Agency standard assessment of contractor implementation of NIST SP 800–171 at 56%.[3] Furthermore, for the High Assessments conducted on-site by DoD to date, only 36% of contractors demonstrated implementation of all 110 of the NIST SP 800–171 security requirements.

Although these industry surveys represent a small sample of the DIB sector, the results were reinforced by the findings from DoD Inspector General report in 2019 (DODIG–2019–105 ''Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems'') indicate that DoD contractors did not consistently implement mandated system security requirements for safeguarding CUI and recommended that DoD take immediate steps to assess a contractor's ability to protect this information. The report emphasizes that malicious actors can exploit the vulnerabilities of contractors' networks and systems and exfiltrate information related to some of the Nation's most valuable advanced defense technologies.

Defense contractors must begin viewing cybersecurity as a part of doing business, in order to protect themselves and to protect national security. The various industry surveys and Government assessments conducted to date illustrate the following: Absent a requirement for defense contractors to demonstrate implementation of standard cybersecurity processes and practices, cybersecurity requirements will not be fully implemented, leaving DoD and the DIB unprotected and vulnerable to malicious cyber activity. To this end, section 1648 of the NDAA for FY 2020 (Pub. L. 116–92) directed the Secretary of Defense to develop a consistent, comprehensive framework to enhance cybersecurity for the U.S. defense industrial base no later than February 1, 2020. In the Senate Armed Services Committee Report to accompany the NDAA for FY 2020, the Committee expressed concern that DIB contractors are an inviting target for our adversaries, who have been conducting cyberattacks to steal critical military technologies.

Developing a framework to enhance the cybersecurity of the defense industrial base will serve as an important first step toward securing the supply chain. Pursuant to section 1648, DoD has developed the CMMC Framework, which gives the Department a mechanism to certify the cyber posture of its largest defense contractors to the smallest firms in our supply chain, who have become primary targets of malicious cyber activity.

This rule is an important part of the cybersecurity framework,[4] and builds on the existing FAR and DFARS clause cybersecurity requirements by (1) adding a mechanism to immediately begin assessing the current status of contractor implementation of NIST SP 800–171 on their information systems that process CUI; and (2) to require contractors and subcontractors to take steps to fully implement existing cybersecurity requirements, plus additional processes and practices, to protect FCI and CUI on their information systems in preparation for verification under the CMMC Framework. There is an urgent need for DoD to immediately begin assessing where vulnerabilities in its supply chain exist and take steps to correct such deficiencies, which can be accomplished by requiring contractors and subcontractors that handle DoD CUI on their information systems to complete a NIST SP 800–171 Basic Assessment. In fact, while this rule includes a delayed effective date, contractors and subcontractors that are required to implement NIST SP 800–171 pursuant to DFARS clause 252.204–7012, are encouraged to immediately conduct and submit a self-assessment as described in this rule to facilitate the Department's assessment.

It is equally urgent for the Department to ensure DIB contractors that have not fully implemented the basic safeguarding requirements under FAR clause 52.204–21 or the NIST SP 800–171 security requirements pursuant to DFARS 252.204–7012 begin correcting these deficiencies immediately. These are cybersecurity requirements contractors and subcontractors should have already implemented (or in the

[1] Aerospace Industries Association. ''Complying with NIST 800–171.'' Fall 2017.

[2] National Defense Industrial Association (NDIA). ''Implementing Cybersecurity in DoD Supply Chains.'' White Paper. July 2018.

[3] NDIA. ''Beyond Obfuscation: The Defense Industry's Position within Federal Cybersecurity Policy.'' A Report of the NDIA Policy Department. October 2018. Page 20 and page 24.

[4] Section 1648 of the NDAA for FY 2020 mandates the formulation of ''unified cybersecurity . . . regulations . . . to be imposed on the defense industrial base for the purpose of assessing the cybersecurity of individual contractors,''

case of implementation of NIST SP 800–171, have plans of action to correct deficiencies) on information systems that handle CUI. Under the CMMC Framework, a contractor is able to achieve CMMC Level 1 Certification if they can demonstrate implementation of the basic safeguarding requirements in the FAR clause. Similarly, a contractor is able to achieve CMMC Level 3 if they can demonstrate implementation of the NIST SP 800–171 security requirements, plus some additional processes and practices. This rule ensures contractors and subcontractors focus on full implementation of existing cybersecurity requirements on their information systems and expedites the Department's ability to secure its supply chain.

For the foregoing reasons, pursuant to 41 U.S.C. 1707(d), DoD finds that urgent and compelling circumstances make compliance with the notice and comment requirements of 41 U.S.C. 1707(a) impracticable, and invokes the exception to those requirements under 41 U.S.C. 1707(d) and FAR 1.501–3(b).[5] While a public comment process will not be completed prior to the rule's effective date, DoD has incorporated feedback solicited through extensive outreach already undertaken pursuant to section 1648(d) of the NDAA for FY 2020, including through public meetings and extensive industry outreach conducted over the past year. However, pursuant to 41 U.S.C. 1707 and FAR 1.501–3(b), DoD will consider public comments received in response to this interim rule in the formation of the final rule.

List of Subjects in 204, 212, 217, and 252

Government procurement.

Jennifer D. Johnson,

Regulatory Control Officer, Defense Acquisition Regulations System.

Therefore, 48 CFR parts 204, 212, 217, and 252 are amended as follows:

■ 1. The authority citation for 48 CFR parts 204, 212, 217, and 252 continues to read as follows:

Authority: 41 U.S.C. 1303 and 48 CFR chapter 1.

[5] FAR 1.501–3(b) states that ''[a]dvance comments need not be solicited when urgent and compelling circumstances make solicitation of comments impracticable prior to the effective date of the coverage, such as when a new statute must be implemented in a relatively short period of time. In such case, the coverage shall be issued on a temporary basis and shall provide for at least a 30 day public comment period.''

PART 204—ADMINISTRATIVE MATTERS

■ 2. Amend section 204.7302 by revising paragraph (a) to read as follows:

204.7302 Policy.

(a)(1) Contractors and subcontractors are required to provide adequate security on all covered contractor information systems.

(2) Contractors required to implement NIST SP 800–171, in accordance with the clause at 252.204–7012, Safeguarding Covered Defense Information and Cyber incident Reporting, are required at time of award to have at least a Basic NIST SP 800–171 DoD Assessment that is current (*i.e.,* not more than 3 years old unless a lesser time is specified in the solicitation) (see 252.204–7019).

(3) The NIST SP 800–171 DoD Assessment Methodology is located at *https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html.*

(4) High NIST SP 800–171 DoD Assessments will be conducted by Government personnel using NIST SP 800–171A, ''Assessing Security Requirements for Controlled Unclassified Information.''

(5) The NIST SP 800–171 DoD Assessment will not duplicate efforts from any other DoD assessment or the Cybersecurity Maturity Model Certification (CMMC) (see subpart 204.75), except for rare circumstances when a re-assessment may be necessary, such as, but not limited to, when cybersecurity risks, threats, or awareness have changed, requiring a re-assessment to ensure current compliance.

* * * * *

■ 3. Revise section 204.7303 to read as follows:

204.7303 Procedures.

(a) Follow the procedures relating to safeguarding covered defense information at PGI 204.7303.

(b) The contracting officer shall verify that the summary level score of a current NIST SP 800–171 DoD Assessment (*i.e.,* not more than 3 years old, unless a lesser time is specified in the solicitation) (see 252.204–7019) for each covered contractor information system that is relevant to an offer, contract, task order, or delivery order are posted in Supplier Performance Risk System (SPRS) (*https://www.sprs.csd.disa.mil/*), prior to—

(1) Awarding a contract, task order, or delivery order to an offeror or contractor that is required to implement NIST SP 800–171 in accordance with the clause at 252.204–7012; or

(2) Exercising an option period or extending the period of performance on a contract, task order, or delivery order with a contractor that is that is required to implement the NIST SP 800–171 in accordance with the clause at 252.204–7012.

■ 4. Amend section 204.7304 by revising the section heading and adding paragraphs (d) and (e) to read as follows:

204.7304 Solicitation provisions and contract clauses.

* * * * *

(d) Use the provision at 252.204–7019, Notice of NIST SP 800–171 DoD Assessment Requirements, in all solicitations, including solicitations using FAR part 12 procedures for the acquisition of commercial items, except for solicitations solely for the acquisition of commercially available off-the-shelf (COTS) items.

(e) Use the clause at 252.204–7020, NIST SP 800–171 DoD Assessment Requirements, in all solicitations and contracts, task orders, or delivery orders, including those using FAR part 12 procedures for the acquisition of commercial items, except for those that are solely for the acquisition of COTS items.

■ 5. Add subpart 204.75, consisting of 204.7500 through 204.7503, to read as follows:

Subpart 204.75—Cybersecurity Maturity Model Certification

Sec.

Subpart 204.75—Cybersecurity Maturity Model Certification

204.7500 Scope of subpart.

(a) This subpart prescribes policies and procedures for including the Cybersecurity Maturity Model Certification (CMMC) level requirements in DoD contracts. CMMC is a framework that measures a contractor's cybersecurity maturity to include the implementation of cybersecurity practices and institutionalization of processes (see *https://www.acq.osd.mil/cmmc/index.html*).

(b) This subpart does not abrogate any other requirements regarding contractor physical, personnel, information, technical, or general administrative security operations governing the protection of unclassified information,

nor does it affect requirements of the National Industrial Security Program.

204.7501 Policy.

(a) The contracting officer shall include in the solicitation the required CMMC level, if provided by the requiring activity. Contracting officers shall not award a contract, task order, or delivery order to an offeror that does not have a current (*i.e.,* not more than 3 years old) CMMC certificate at the level required by the solicitation.

(b) Contractors are required to achieve, at time of award, a CMMC certificate at the level specified in the solicitation. Contractors are required to maintain a current (*i.e.,* not more than 3 years old) CMMC certificate at the specified level, if required by the statement of work or requirement document, throughout the life of the contract, task order, or delivery order. Contracting officers shall not exercise an option period or extend the period of performance on a contract, task order, or delivery order, unless the contract has a current (*i.e.,* not more than 3 years old) CMMC certificate at the level required by the contract, task order, or delivery order.

(c) The CMMC Assessments shall not duplicate efforts from any other comparable DoD assessment, except for rare circumstances when a re-assessment may be necessary such as, but not limited to when there are indications of issues with cybersecurity and/or compliance with CMMC requirements.

204.7502 Procedures.

(a) When a requiring activity identifies a requirement for a contract, task order, or delivery order to include a specific CMMC level, the contracting officer shall not—

(1) Award to an offeror that does not have a CMMC certificate at the level required by the solicitation; or

(2) Exercise an option or extend any period of performance on a contract, task order, or delivery order unless the contractor has a CMMC certificate at the level required by the contract.

(b) Contracting officers shall use Supplier Performance Risk System (SPRS) (*https://www.sprs.csd.disa.mil/*) to verify an offeror or contractor's CMMC level.

204.7503 Contract clause.

Use the clause at 252.204–7021, Cybersecurity Maturity Model Certification Requirements, as follows:

(a) Until September 30, 2025, in solicitations and contracts or task orders or delivery orders, including those using FAR part 12 procedures for the acquisition of commercial items, except for solicitations and contracts or orders solely for the acquisition of commercially available off-the-shelf (COTS) items, if the requirement document or statement of work requires a contractor to have a specific CMMC level. In order to implement a phased rollout of CMMC, inclusion of a CMMC requirement in a solicitation during this time period must be approved by OUSD(A&S).

(b) On or after October 1, 2025, in all solicitations and contracts or task orders or delivery orders, including those using FAR part 12 procedures for the acquisition of commercial items, except for solicitations and contracts or orders solely for the acquisition of COTS items.

PART 212—ACQUISITION OF COMMERCIAL ITEMS

■ 6. Amend section 212.301, by adding paragraphs (f)(ii)(K), (L), and (M) to read as follows:

212.301 Solicitation provisions and contract clauses for acquisition of commercial items.

* * * * *

(f) * * *

(ii) * * *

(K) Use the provision at 252.204–7019, Notice of NIST SP 800–171 DoD Assessment Requirements, as prescribed in 204.7304(d).

(L) Use the clause at 252.204–7020, NIST SP 800–171 DoD Assessment Requirements, as prescribed in 204.7304(e).

(M) Use the clause at 252.204–7021, Cybersecurity Maturity Model Certification Requirements, as prescribed in 204.7503(a) and (b).

* * * * *

PART 217—SPECIAL CONTRACTING METHODS

■ 7. Amend section 217.207 by revising paragraph (c) to read as follows:

217.207 Exercise of options.

(c) In addition to the requirements at FAR 17.207(c), exercise an option only after:

(1) Determining that the contractor's record in the System for Award Management database is active and the contractor's Data Universal Numbering System (DUNS) number, Commercial and Government Entity (CAGE) code, name, and physical address are accurately reflected in the contract document. See PGI 217.207 for the requirement to perform cost or price analysis of spare parts prior to exercising any option for firm-fixed-price contracts containing spare parts.

(2) Verifying in the Supplier Performance Risk System (SPRS) (*https://www.sprs.csd.disa.mil/*) that—

(i) The summary level score of a current NIST SP 800–171 DoD Assessment (*i.e.,* not more than 3 years old, unless a lesser time is specified in the solicitation) for each covered contractor information system that is relevant to an offer, contract, task order, or delivery order are posted (see 204.7303).

(ii) The contractor has a CMMC certificate at the level required by the contract, and that it is current (*i.e.,* not more than 3 years old) (see 204.7502).

PART 252—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

■ 8. Add sections 252.204–7019, 252.204–7020, and 252.204–7021 to read as follows:

Sec.

* * * * *

252.204–7019 Notice of NIST SP 800–171 DoD Assessment Requirements.

252.204–7020 NIST SP 800–171 DoD Assessment Requirements.

252.204–7021 Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement.

* * * * *

252.204–7019 Notice of NIST SP 800–171 DoD Assessment Requirements.

As prescribed in 204.7304(d), use the following provision:

NOTICE OF NIST SP 800–171 DOD ASSESSMENT REQUIREMENTS (NOV 2020)

(a) *Definitions.*

Basic Assessment, Medium Assessment, and *High Assessment* have the meaning given in the clause 252.204–7020, NIST SP 800–171 DoD Assessments.

Covered contractor information system has the meaning given in the clause 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, of this solicitation.

(b) *Requirement.* In order to be considered for award, if the Offeror is required to implement NIST SP 800–171, the Offeror shall have a current assessment (*i.e.,* not more than 3 years old unless a lesser time is specified in the solicitation) (see 252.204–7020) for each covered contractor information system that is relevant to the offer, contract, task order, or delivery order. The Basic, Medium, and High NIST SP 800–171 DoD Assessments are described in the NIST SP 800–171 DoD Assessment Methodology located at *https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html.*

(c) *Procedures.* (1) The Offeror shall verify that summary level scores of a current NIST SP 800–171 DoD Assessment (*i.e.,* not more than 3 years old unless a lesser time is

specified in the solicitation) are posted in the Supplier Performance Risk System (SPRS) (*https://www.sprs.csd.disa.mil/*) for all covered contractor information systems relevant to the offer.

(2) If the Offeror does not have summary level scores of a current NIST SP 800–171 DoD Assessment (*i.e.,* not more than 3 years old unless a lesser time is specified in the solicitation) posted in SPRS, the Offeror may conduct and submit a Basic Assessment to *webptsmh@navy.mil* for posting to SPRS in the format identified in paragraph (d) of this provision.

(d) *Summary level scores.* Summary level scores for all assessments will be posted 30 days post-assessment in SPRS to provide DoD Components visibility into the summary level scores of strategic assessments.

(1) *Basic Assessments.* An Offeror may follow the procedures in paragraph (c)(2) of this provision for posting Basic Assessments to SPRS.

(i) The email shall include the following information:

(A) Cybersecurity standard assessed (*e.g.,* NIST SP 800–171 Rev 1).

(B) Organization conducting the assessment (*e.g.,* Contractor self-assessment).

(C) For each system security plan (security requirement 3.12.4) supporting the performance of a DoD contract—

(*1*) All industry Commercial and Government Entity (CAGE) code(s) associated with the information system(s) addressed by the system security plan; and

(*2*) A brief description of the system security plan architecture, if more than one plan exists.

(D) Date the assessment was completed.

(E) Summary level score (*e.g.,* 95 out of 110, NOT the individual value for each requirement).

(F) Date that all requirements are expected to be implemented (*i.e.,* a score of 110 is expected to be achieved) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800–171.

(ii) If multiple system security plans are addressed in the email described at paragraph (d)(1)(i) of this section, the Offeror shall use the following format for the report:

System security plan	CAGE codes supported by this plan	Brief description of the plan architecture	Date of assessment	Total score	Date score of 110 will achieved

(2) *Medium and High Assessments.* DoD will post the following Medium and/or High Assessment summary level scores to SPRS for each system assessed:

(i) The standard assessed (*e.g.,* NIST SP 800–171 Rev 1).

(ii) Organization conducting the assessment, *e.g.,* DCMA, or a specific organization (identified by Department of Defense Activity Address Code (DoDAAC)).

(iii) All industry CAGE code(s) associated with the information system(s) addressed by the system security plan.

(iv) A brief description of the system security plan architecture, if more than one system security plan exists.

(v) Date and level of the assessment, *i.e.,* medium or high.

(vi) Summary level score (*e.g.,* 105 out of 110, not the individual value assigned for each requirement).

(vii) Date that all requirements are expected to be implemented (*i.e.,* a score of 110 is expected to be achieved) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800–171.

(3) *Accessibility.* (i) Assessment summary level scores posted in SPRS are available to DoD personnel, and are protected, in accordance with the standards set forth in DoD Instruction 5000.79, Defense-wide Sharing and Use of Supplier and Product Performance Information (PI).

(ii) Authorized representatives of the Offeror for which the assessment was conducted may access SPRS to view their own summary level scores, in accordance with the SPRS Software User's Guide for Awardees/Contractors available at *https://www.sprs.csd.disa.mil/pdf/SPRS_Awardee.pdf.*

(iii) A High NIST SP 800–171 DoD Assessment may result in documentation in addition to that listed in this section. DoD will retain and protect any such documentation as ''Controlled Unclassified Information (CUI)'' and intended for internal DoD use only. The information will be protected against unauthorized use and release, including through the exercise of applicable exemptions under the Freedom of Information Act (*e.g.,* Exemption 4 covers trade secrets and commercial or financial information obtained from a contractor that is privileged or confidential).

(End of provision)

252.204–7020 NIST SP 800–171 DoD Assessment Requirements.

As prescribed in 204.7304(e), use the following clause:

NIST SP 800–171 DOD ASSESSMENT REQUIREMENTS (NOV 2020)

(a) *Definitions.*

Basic Assessment means a contractor's self-assessment of the contractor's implementation of NIST SP 800–171 that—

(1) Is based on the Contractor's review of their system security plan(s) associated with covered contractor information system(s);

(2) Is conducted in accordance with the NIST SP 800–171 DoD Assessment Methodology; and

(3) Results in a confidence level of ''Low'' in the resulting score, because it is a self-generated score.

Covered contractor information system has the meaning given in the clause 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, of this contract.

High Assessment means an assessment that is conducted by Government personnel using NIST SP 800–171A, Assessing Security Requirements for Controlled Unclassified Information that—

(1) Consists of—

(i) A review of a contractor's Basic Assessment;

(ii) A thorough document review;

(iii) Verification, examination, and demonstration of a Contractor's system security plan to validate that NIST SP 800–171 security requirements have been implemented as described in the contractor's system security plan; and

(iv) Discussions with the contractor to obtain additional information or clarification, as needed; and

(2) Results in a confidence level of ''High'' in the resulting score.

Medium Assessment means an assessment conducted by the Government that—

(1) Consists of—

(i) A review of a contractor's Basic Assessment;

(ii) A thorough document review; and

(iii) Discussions with the contractor to obtain additional information or clarification, as needed; and

(2) Results in a confidence level of ''Medium'' in the resulting score.

(b) *Applicability.* This clause applies to covered contractor information systems that are required to comply with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171, in accordance with Defense Federal Acquisition Regulation System (DFARS) clause at 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, of this contract.

(c) *Requirements.* The Contractor shall provide access to its facilities, systems, and personnel necessary for the Government to conduct a Medium or High NIST SP 800–171 DoD Assessment, as described in NIST SP 800–171 DoD Assessment Methodology at *https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html,* if necessary.

(d) *Procedures.* Summary level scores for all assessments will be posted in the Supplier Performance Risk System (SPRS) (*https://www.sprs.csd.disa.mil/*) to provide DoD

Components visibility into the summary level scores of strategic assessments.

(1) *Basic Assessments.* A contractor may submit, via encrypted email, summary level scores of Basic Assessments conducted in accordance with the NIST SP 800–171 DoD Assessment Methodology to *webptsmh@navy.mil* for posting to SPRS.

(i) The email shall include the following information:

(A) Version of NIST SP 800–171 against which the assessment was conducted.

(B) Organization conducting the assessment (*e.g.,* Contractor self-assessment).

(C) For each system security plan (security requirement 3.12.4) supporting the performance of a DoD contract—

(*1*) All industry Commercial and Government Entity (CAGE) code(s) associated with the information system(s) addressed by the system security plan; and

(*2*) A brief description of the system security plan architecture, if more than one plan exists.

(D) Date the assessment was completed.

(E) Summary level score (*e.g.,* 95 out of 110, NOT the individual value for each requirement).

(F) Date that all requirements are expected to be implemented (*i.e.,* a score of 110 is expected to be achieved) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800–171.

(ii) If multiple system security plans are addressed in the email described at paragraph (b)(1)(i) of this section, the Contractor shall use the following format for the report:

System security plan	CAGE codes supported by this plan	Brief description of the plan architecture	Date of assessment	Total score	Date score of 110 will achieved

(2) *Medium and High Assessments.* DoD will post the following Medium and/or High Assessment summary level scores to SPRS for each system security plan assessed:

(i) The standard assessed (*e.g.,* NIST SP 800–171 Rev 1).

(ii) Organization conducting the assessment, *e.g.,* DCMA, or a specific organization (identified by Department of Defense Activity Address Code (DoDAAC)).

(iii) All industry CAGE code(s) associated with the information system(s) addressed by the system security plan.

(iv) A brief description of the system security plan architecture, if more than one system security plan exists.

(v) Date and level of the assessment, *i.e.,* medium or high.

(vi) Summary level score (*e.g.,* 105 out of 110, not the individual value assigned for each requirement).

(vii) Date that all requirements are expected to be implemented (*i.e.,* a score of 110 is expected to be achieved) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800–171.

(e) *Rebuttals.* (1) DoD will provide Medium and High Assessment summary level scores to the Contractor and offer the opportunity for rebuttal and adjudication of assessment summary level scores prior to posting the summary level scores to SPRS (see SPRS User's Guide *https://www.sprs.csd.disa.mil/pdf/SPRS_Awardee.pdf*).

(2) Upon completion of each assessment, the contractor has 14 business days to provide additional information to demonstrate that they meet any security requirements not observed by the assessment team or to rebut the findings that may be of question.

(f) *Accessibility.* (1) Assessment summary level scores posted in SPRS are available to DoD personnel, and are protected, in accordance with the standards set forth in DoD Instruction 5000.79, Defense-wide Sharing and Use of Supplier and Product Performance Information (PI).

(2) Authorized representatives of the Contractor for which the assessment was conducted may access SPRS to view their own summary level scores, in accordance with the SPRS Software User's Guide for Awardees/Contractors available at *https://www.sprs.csd.disa.mil/pdf/SPRS_Awardee.pdf.*

(3) A High NIST SP 800–171 DoD Assessment may result in documentation in addition to that listed in this clause. DoD will retain and protect any such documentation as ''Controlled Unclassified Information (CUI)'' and intended for internal DoD use only. The information will be protected against unauthorized use and release, including through the exercise of applicable exemptions under the Freedom of Information Act (*e.g.,* Exemption 4 covers trade secrets and commercial or financial information obtained from a contractor that is privileged or confidential).

(g) *Subcontracts.* (1) The Contractor shall insert the substance of this clause, including this paragraph (g), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items (excluding COTS items).

(2) The Contractor shall not award a subcontract or other contractual instrument, that is subject to the implementation of NIST SP 800–171 security requirements, in accordance with DFARS clause 252.204–7012 of this contract, unless the subcontractor has completed, within the last 3 years, at least a Basic NIST SP 800–171 DoD Assessment, as described in *https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html,* for all covered contractor information systems relevant to its offer that are not part of an information technology service or system operated on behalf of the Government.

(3) If a subcontractor does not have summary level scores of a current NIST SP 800–171 DoD Assessment (*i.e.,* not more than 3 years old unless a lesser time is specified in the solicitation) posted in SPRS, the subcontractor may conduct and submit a Basic Assessment, in accordance with the NIST SP 800–171 DoD Assessment Methodology, to *webptsmh@navy.mil* for posting to SPRS along with the information required by paragraph (d) of this clause.

(End of clause)

252.204–7021 Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement.

As prescribed in 204.7503(a) and (b), insert the following clause:

CONTRACTOR COMPLIANCE WITH THE CYBERSECURITY MATURITY MODEL CERTIFICATION LEVEL REQUIREMENT (NOV 2020)

(a) *Scope.* The Cybersecurity Maturity Model Certification (CMMC) CMMC is a framework that measures a contractor's cybersecurity maturity to include the implementation of cybersecurity practices and institutionalization of processes (see *https://www.acq.osd.mil/cmmc/index.html*).

(b) *Requirements.* The Contractor shall have a current (*i.e.* not older than 3 years) CMMC certificate at the CMMC level required by this contract and maintain the CMMC certificate at the required level for the duration of the contract.

(c) *Subcontracts.* The Contractor shall—

(1) Insert the substance of this clause, including this paragraph (c), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items, excluding commercially available off-the-shelf items; and

(2) Prior to awarding to a subcontractor, ensure that the subcontractor has a current (*i.e.,* not older than 3 years) CMMC certificate at the CMMC level that is appropriate for the information that is being flowed down to the subcontractor.

(End of clause)

[FR Doc. 2020–21123 Filed 9–28–20; 8:45 am]

BILLING CODE 5001–06–P