CMMC: The DoD's Cybersecurity Requirements

What businesses need to know about the Cybersecurity Maturity Model Certification for Department of Defense contracting

What is CMMC: CMMC is the Department of Defense's program for verifying that contractors protect sensitive government information. CMMC requirements are being phased into DoD solicitations and contracts, and without certification at the required level it can affect your eligibility to win and perform work.

If you touch covered DoD information, CMMC is about doing the required practices and being able to prove you are doing them.

What is required?

Federal Contract Information (FCI)

FCI is information not intended for public release that is provided by or generated for the Government under a contract.

In plain terms, this can include:

- Contract performance details
- Technical specifications not publicly available
- Internal project communications related to the contract
- If you are performing DoD work and handling non-public contract information, you are likely handling FCI.

FCI drives CMMC Level 1.

Controlled Unclassified Information (CUI)

CUI is unclassified information that requires safeguarding or dissemination controls under federal law, regulation, or government wide policy.

This is more sensitive than FCI. It can include:

- Technical drawings or engineering data marked as CUI
- Export controlled data
- Data that could pose risk to national security if improperly disclosed
- CUI is typically marked and identified in the contract or by the prime contractor.

CUI drives CMMC Level 2.

Level 1 or Level 2

Level 1 (FCI)	Level 2 (CUI)
DoD contractors handling FCI	DoD contractors handling CUI
Basic safeguards implemented and evidenced	NIST SP 800-171 requirements implemented and evidenced
Focus on fundamental cyber hygiene	Focus on protecting Controlled Unclassified Information
15 security practices required	**110** security requirements required
Commonly self-attested early in rollout	Increasing third-party validation as rollout progresses

Timeline

CMMC is rolling out in phases, meaning requirements will appear in more contracts over time and validation becomes more common as the rollout progresses.

Current Market Landscape

North Carolina's Defense Industrial Base includes more than 3,600 identified defense contractors across the state, many of which could be subject to CMMC requirements if they handle Federal Contract Information or Controlled Unclassified Information on DoD work.

Nationally, well over 100,000 companies are expected to require Level 2 certification, yet only a small number have been certified to date. Industry surveys show fewer than 1 percent of organizations feel fully prepared for assessment, and less than half have completed foundational documentation.

Within North Carolina, readiness varies widely. Larger firms may have established cybersecurity programs, while many small and mid sized subcontractors are balancing compliance planning alongside production demands and workforce constraints. As CMMC requirements phase into contracts, companies that are not prepared risk losing eligibility for future DoD opportunities.

Why waiting is risky

CMMC preparation is not a single technical fix. It requires defining system scope, implementing security controls, documenting policies and procedures, training personnel, and building evidence that those controls are consistently operating. These steps take time to complete properly.

As requirements phase into more DoD solicitations, companies that are not prepared may find themselves unable to bid on or perform certain contracts. Waiting until a solicitation requires certification can compress timelines, increase costs, and create internal disruption.

Early preparation allows organizations to address gaps methodically, spread costs over time, and avoid last-minute decisions that may limit future eligibility in the defense market.

Common Misunderstandings About CMMC

"We only need this if we are a prime contractor."

CMMC requirements flow down through the supply chain. Subcontractors that handle covered information can be subject to the same level requirements as primes.

"We can wait until a contract requires certification."

Implementation, documentation, and evidence collection take time. Waiting until a solicitation includes CMMC language may compress timelines and increase internal disruption.

"We just need to buy the right cybersecurity software."

CMMC is not a product purchase. It requires defined processes, trained personnel, documented procedures, and evidence that controls are consistently operating.

"We can get a waiver if we are not ready."

Waivers are limited and approved at senior levels within the Department of Defense. They are not a routine or contractor-driven solution.

What Certification Actually Means

Certification means your organization has implemented the required security practices, documented how they operate, and can provide evidence that they are consistently followed.

For Level 2, this means aligning to NIST SP 800-171 requirements, defining system scope, closing identified gaps, and preparing for validation as required. Certification is not a one-time event. It requires ongoing discipline and maintenance..

What To Do Next:

1. **Confirm your data type**. Determine whether your DoD work involves FCI or CUI and what level may apply.
2. **Define scope early.** Identify the people, devices, systems, and vendors that handle covered information.
3. **Start structured preparation.** Complete a Level 1 checklist or a Level 2 gap assessment aligned to NIST SP 800-171.
4. **Engage local support.** The North Carolina Military Business Center works with community colleges and partner resources to connect businesses to training, guidance, and implementation support tailored to defense contractors.

Need Assistance?

The North Carolina Military Business Center (NCMBC) is an entity of the State of North Carolina that is embedded in community colleges statewide. The NCMBC provides no-fee support to businesses pursuing defense and other federal contracts.

NCMBC can help clarify applicable CMMC levels, connect you to training resources, and support structured preparation for compliance.

Learn more at www.ncmbc.us or contact Tim Malone at malonet@ncmbc.us.

CMMC Waivers: What Businesses Need to Know

CONNECTING MILITARY AND BUSINESS

In January 2025, the Department of Defense issued formal policy clarifying how CMMC assessment levels are selected and under what circumstances CMMC assessment requirements may be waived.

For contractors, the most important point is this: a waiver may apply to the CMMC assessment requirement. It does not waive the underlying cybersecurity requirements tied to the contract.

What a Waiver Is and Is Not

A waiver may apply to the requirement to complete a CMMC certification assessment for a specific procurement.

It does not remove or reduce the contractor's obligation to comply with existing cybersecurity requirements, including:

- FAR 52.204-21 for safeguarding Federal Contract Information
- DFARS 252.204-7012
- NIST SP 800-171 requirements for CUI
- NIST SP 800-172 enhanced requirements where applicable

Even if an assessment is waived, the security controls must still be implemented.

In practical terms, the certification check may be waived. The security standard is not.

Who Approves a Waiver

Waiver authority resides with the Service Acquisition Executive or Component Acquisition Executive.

Waivers must be coordinated through the Component Chief Information Officer before approval. Approved waivers are tracked and reported to senior acquisition and CIO leadership on a quarterly basis.

This is a formal, senior-level decision process. It is not routine.

CMMC Waivers: What Businesses Need to Know

CONNECTING MILITARY AND BUSINESS

When Waivers May Be Considered

The policy emphasizes that waivers are limited and risk-based.

Level 1 assessment requirements are unlikely to be waived.

Level 2 self-assessment requirements are also unlikely to be waived, given existing regulatory obligations.

In limited circumstances, a waiver of Level 2 third-party certification may be considered, such as when maintaining competition or accessing non-traditional suppliers is necessary. Even in those cases, alternative protections and risk mitigation must be evaluated.

Level 3 waivers may be considered in rare circumstances but are not appropriate where contracts require access to both classified and unclassified DoD information.

What This Means for Businesses

The memorandum reinforces that CMMC level selection must align with risk and mission impact. Where a contract requires a specific CMMC level, the expectation is that contractors will meet it unless a formal exception is approved through the defined process.

Waivers are structured, controlled, and visible within the Department. They are intended for exceptional circumstances, not as a substitute for preparation.

Businesses that delay compliance in anticipation of a waiver assume risk. The underlying cybersecurity obligations remain in force regardless of whether an assessment requirement is waived.

Practical Takeaway

If your work involves Federal Contract Information or Controlled Unclassified Information, determine the applicable CMMC level and prepare accordingly.

A waiver may remove a certification requirement in rare cases. It does not remove the requirement to protect the information.

OFFICE OF THE SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Implementing the Cybersecurity Maturity Model Certification (CMMC) Program: Guidance for Determining Appropriate CMMC Compliance Assessment Levels and Process for Waiving CMMC Assessment Requirements

The defense industrial base (DIB) is the target of recurrent and progressively sophisticated cyber attacks targeting Controlled Unclassified Information (CUI) and Federal Contract Information (FCI) processed in, stored on, or transmitted over nonfederal unclassified information systems. These attacks threaten Department of Defense (DoD or Department) mission execution, reduce warfighting capabilities, weaken American technological superiority, and exfiltrate intellectual property and national security information. The Department is undertaking multiple efforts to reduce the risk of cyber attacks to DIB businesses.

Defense contractors and subcontractors are required to safeguard unclassified nonpublic information by applying specified network security requirements, as defined in DoD Instruction 8582.01, *Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information*, which includes identified CUI and FCI that resides in or transits contractor unclassified information systems. Title 32 of the Code of Federal Regulations (CFR) § 2002 describes requirements for adequate safeguarding that, in the context of Defense contracts, are implemented through Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*. This clause applies to contracts that require the processing, storing, or transmitting of CUI on contractor-owned information systems.

To enhance the security of DoD information and reduce the risk of cyber attacks to DIB businesses, the Department established the Cybersecurity Maturity Model Certification (CMMC) Program. The final CMMC Program rule was published to the *Federal Register* on October 15, 2024 and is codified in Title 32 CFR Part 170. The CMMC Program requires pre-award assessment of covered contractor information systems against prescribed cybersecurity standards for safeguarding CUI or FCI. The CMMC Program will implement pre-award assessments of contractor compliance with the appropriate information safeguarding requirements. Title 32 CFR § 170 defines applicability of CMMC requirements and Title 48 CFR DFARS provisions and clauses will implement those requirements.

Upon publication of the final Title 48 CFR DFARS rule, 2019-D041, Program Managers and requiring activities shall include the need for CMMC assessments in procurement request and requirement documents in accordance with phase-in timelines described in Title 32 CFR § 170.3. Attachment 1 to this memorandum provides Program Managers and requiring activities guidance to apply when determining the appropriate CMMC assessment level to include in each DoD solicitation and contract. Service and Component Acquisition Executives are authorized to waive inclusion of CMMC assessment requirements in DoD solicitations. Waivers are discussed in Attachment 2.

At the conclusion of the phase-in period, Program Managers and requiring activities will designate a CMMC level for each contract, as appropriate, according to attributes of the information that will be processed, stored, or transmitted on covered contractor information systems, as described in Attachment 1. Service and Component Acquisition Executives may, after following approved procedures, waive CMMC assessment requirements, as described in Attachment 2. A waiver of CMMC assessment requirements does not affect the underlying security requirements, or current policy, that may apply (including, but not limited to, Federal Acquisition Regulation (FAR) clause 52.204-21 and DFARS clause 252.204-7012), which will remain in effect.

Finally, when a requirement is expected to result in award of a non-FAR based grant or other legal agreement, Program Managers and requiring activities are still expected to follow the CMMC Level Determination Guide (Attachment 1) to select an appropriate CMMC level requirement.

The Office of the DoD Chief Information Officer intends to incorporate the attached policies into one or more DoD Instructions, as appropriate. Additionally, the Department will revise DoD Instruction 8582.01 to provide guidance for applying the enhanced protections provided by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-172, which are carried forward in CMMC Level 3. The CMMC Program Management Office is the point of contact for this effort: osd.pentagon.dod-cio.list.cmmc-mbx@mail.mil. The Office of the Under Secretary of Defense for Research and Engineering will publish and maintain a guidebook with additional details for the application of NIST SP 800-172 at https://aaf.dau.edu/guidebook.

Heidi Shyu
Under Secretary of Defense
for Research and Engineering

JAN 15 2025

Leslie A. Beavers
Acting Chief Information Officer
of the Department of Defense

JAN 13 2025

Dr William LaPlante
Under Secretary of Defense
for Acquisition and Sustainment

Attachments:
As stated

Attachment 1
Cybersecurity Maturity Model Certification Level Determination

Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012 and Federal Acquisition Regulation (FAR) clause 52.204-21 establish the cybersecurity requirements for FAR-based contracts. Title 32 of the Code of Federal Regulations (CFR) § 170.3 (e) describes a phased implementation plan for assessment of compliance with these requirements under the CMMC Program.

Program Managers and requiring activities shall follow the CMMC Program implementation phases defined in Title 32 CFR § 170.3(e). Upon publication of the final Title 48 CFR DFARS rule, 2019-D041, all procurement requests that may result in a contract where the contractor or a subcontractor, at any tier, may have **Federal Contract Information** (FCI), as defined in FAR clause 52.204-7021, residing in or transiting through its information system shall include CMMC Level 1.

One year after publication of the DFARS rule, Program Managers and requiring activities shall also begin to require CMMC Level 2 certification assessments, when appropriate. In two years, Program Managers and requiring activities shall begin to implement CMMC Level 3 certification assessment requirements, when appropriate.

In accordance with DFARS Procedures, Guidance, and Information 204.7303-1(b)(1), the requiring activity must notify the contracting officer when an effort is expected to result in a contract, task order, or delivery order that will involve **covered defense information** (including Controlled Unclassified Information (CUI)) or operationally critical support. Covered defense information is defined in DFARS clause 252.204-7012. In order to appropriately apply information safeguarding requirements, when the effort will involve CUI, the requiring activity must also identify whether CMMC Level 2 self-assessment of certification assessment is the minimum requirement. Contacting Officers will rely on information provided by the requiring activity to communicate the applicable CMMC level requirements to offerors and contractors.

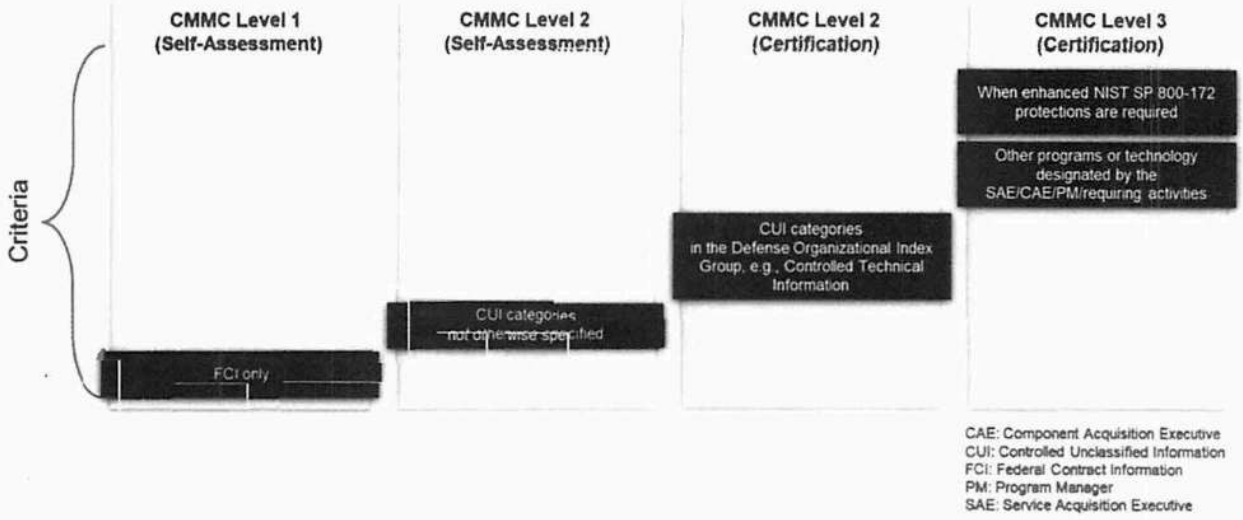
CMMC Level 3 assessments shall be required when DoD policy requires the application of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-172. The enhanced protections of NIST SP 800-172 must be applied to safeguard CUI associated with mission critical or unique technologies and programs. Program Managers and requiring activities must also carefully consider the risks associated with the security of the subcontractors' nonfederal information systems in the multi-tier supply chain and provide additional solicitation guidance regarding the extent to which CMMC Level 3 requirements must be flowed down.

The Department is updating DoDI 8582.01, *Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information*, and is developing a Defense Acquisition University guidebook, to include guidance for applying NIST SP 800-172.

DoD Program Managers and requiring activities will use the following CMMC Level Determination Guide to identify the appropriate CMMC level for a given contract. When a contract effort will result in CUI being processed, stored, or transmitted on a contractor information system that meets multiple CMMC level determination criteria, Program Managers and requiring activities shall select the highest applicable CMMC level. The guidance contained herein addresses the minimum required assessment levels and does not preclude selection of a higher CMMC level requirement when security needs dictate.

Until supplanted by a DoD Instruction, this CMMC Level Determination Guide defines the minimum CMMC level requirement. Other DoD policies, regulations, or security concerns may necessitate selection of a higher CMMC level requirement. Service and Component Acquisition Executives may issue supplementary guidance to ensure CMMC requirements are consistently applied, in particular for CMMC Level 3 Certification assessments. Flow-down requirements for all other CMMC assessment requirements are defined in Title 32 CFR § 170.23.

CMMC Level Determination Guide



CMMC Level 1 (Self-Assessment) – Assessed against the FAR clause 52.204-21:

- FAR clause 52.204-21 applies to FCI. This clause does not apply to information provided by the Government to the public, such as on public websites, or simple transactional information, such as is necessary to process payments.

- If the planned contract, task order, or delivery order may require the contractor (or subcontractors at any tier) to process, store, or transmit only FCI in its information system, the appropriate assessment requirement is CMMC Level 1 Self-Assessment.

CMMC Level 2 – Assessed against the NIST SP 800–171:

- DFARS clause 252.204-7012 applies when CUI will be processed, stored, or transmitted on contractor-owned information systems in the performance of a DoD contract and flows down to subcontracts, or similar contractual instruments, as described in DFARS clause 252.204-7012.

- If the planned contract will require the contractor (or subcontractors) to process, store, or transmit CUI on a contractor-owned information system, compliance must be assessed against NIST SP 800-171 requirements.

    - **CMMC Level 2 (Self-Assessment)** is the minimum assessment requirement for CUI. It is sufficient only for CUI outside of the National Archive's CUI Registry Defense Organizational Index Grouping. Category markings and definitions may be found on

the CUI Registry at https://www.archives.gov/cui. The Program Manager may elevate the CMMC level if there is high risk to the confidentiality, integrity, or availability of the CUI.

- **CMMC Level 2 (Certification)** is the minimum assessment requirement when the planned contract will require the contractor (or subcontractors) to process, store, or transmit CUI categorized under the National Archive's CUI Registry Defense Organizational Index Grouping. Category markings and definitions may be found on the CUI Registry at https://www.archives.gov/cui. CMMC Level 2 certification assessment is performed by third-party assessors employing the methods described in NIST SP 800-171A.

CMMC Level 3 (Certification) – Assessed by DoD officials against select controls in NIST SP 800–172:

- The enhanced protections of NIST SP 800-172 must be applied to safeguard mission critical or unique technologies and programs associated with the following factors/scenarios. Compliance with NIST SP 800-172 is a significant effort. Program Managers and requiring activities must carefully consider the need for safeguarding of the particular CUI to be shared and avoid overuse of the CMMC Level 3 requirement.
  - CUI associated with a breakthrough, unique, and/or advanced technology;
  - Significant aggregation or compilation of CUI in a single information system or IT environment; and
  - Ubiquity – when an attack on a single information system or IT environment would result in widespread vulnerability across DoD.
- The Office of the Under Secretary of Defense for Research and Engineering will publish and maintain a guidebook with additional details for the application of NIST SP 800-172 at https://aaf.dau.edu/guidebook.
- If the planned contract will require the contractor (or subcontractors) to process, store, or transmit CUI that requires enhanced protections provided by NIST SP 800-172, then the minimum assessment requirement is CMMC Level 3 (Certification).
  - DoD Program Managers and requiring activities will determine if a contract effort requires the contractor (or subcontractors) to process, store, or transmit CUI within nonfederal unclassified information systems pertaining to the essential technology elements identified for prioritized protection through application of the NIST SP 800-172 requirements described in DoD Instruction 8582.01.
  - When CMMC Level 3 is warranted, a Security Classification Guide must be provided to communicate any CUI distribution limitations or instructions and allow for the segregation of information such that information that need not be covered by CMMC Level 3 can be handled appropriately at levels below CMMC level 3 throughout the supply chain. Failure to do so may result in the CMMC Level 3 requirements being unnecessarily flowed down to all sub-tiers at significant cost to the program.

ATTACHMENT 2
CYBERSECURITY MATURITY MODEL CERTIFICATION WAIVER APPLICABILITY AND REPORTING REQUIREMENTS

Program Managers or requiring activities may request Service Acquisition Executive (SAE) or Component Acquisition Executive (CAE) approval to waive CMMC assessment requirements that would otherwise apply (including invoking lesser CMMC assessment levels), within the parameters below, or as supplemented by policies that SAEs or CAEs may issue. All CMMC waiver requests must be coordinated through the component Chief Information Officer (CIO) prior to SAE or CAE approval. For programs under Defense Acquisition Executive (DAE) oversight, Program Managers shall coordinate waiver requests through the component CIO, Program Executive Officer, CAE or SAE, and the Office of the DoD CIO at osd.pentagon.dod-cio.list.cmmc-mbx@mail.mil prior to DAE approval.

CMMC waivers may be requested and approved for an individual procurement or a class of procurements, and waivers will impact only whether CMMC assessments must be included in solicitation documents and resultant contracts. CMMC assessment waivers do not affect the underlying security requirements of Federal Acquisition Regulation (FAR) clause 52.204-21, Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, or National Institute of Standards and Technology (NIST) Special Publication (SP) 800-172, when applicable pursuant to DoD policy. All agencies are required by Title 32 of the Code of Federal Regulations (CFR) § 2002 to use NIST SP 800-171 when establishing requirements to protect Controlled Unclassified Information (CUI) on nonfederal information systems. Refer to DoD Instruction 8582.01, *Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information*, for additional guidance on security of non-DoD information systems processing unclassified DoD information.

Waiver Reporting Requirements:

SAEs and CAEs will report CMMC waiver data quarterly to the Under Secretary of Defense (USD) for Acquisition and Sustainment, the USD for Intelligence and Security, the USD for Research and Development, and the Office of the DoD CIO. Reports can me made via postings to osd.pentagon.dod-cio.list.cmmc-mbx@mail.mil. The report will enumerate all contracts awarded with CMMC assessment requirements waived, by the certification level that would otherwise have applied, and will identify common Product Service Codes or other relevant information that may explain market circumstances necessitating such assessment waivers.

Phase-In of CMMC Assessment Requirements, Including Waiver Process:

Program Managers and requiring activities should identify information security requirements for the types of information most likely to be associated with the planned contract effort. When market research indicates that including a CMMC assessment requirement may impede ability to generate robust competition or delay delivery of mission critical capabilities, the SAE, CAE, or DAE may approve requests to waive inclusion of CMMC assessment requirements. SAEs and CAEs must carefully weigh the risk of potential loss of CUI associated with mission critical capabilities before granting a waiver. SAEs and CAEs must recognize the following waiver limitations and may supplement this guidance with specific information, formatting, and coordination requirements.

1. CMMC Level 1 requirements: CMMC Level 1 is a self-assessment requirement designed to provide added insight into or assurance of the offeror's compliance with requirements defined in FAR clause 52.204-21 for the safeguarding of Federal Contract Information (FCI). This is the most basic level of cybersecurity posture. There are no circumstances likely to warrant approval of requests to waive CMMC Level 1 requirements.

2. CMMC Level 2 requirements: CMMC Level 2 can be a self-assessment requirement or an independent third-party assessment.

    a. Effective September 29, 2020, DFARS Subpart 204.73, *Safeguarding Covered Defense Information and Cyber Incident Reporting*, was amended to require the inclusion of DFARS clause 252.204-7019, *Notice of NIST SP 800-171 DoD Assessment Requirements*, in all solicitations, except those solely for the acquisition of commercial off-the-shelf items. This provision requires offerors to provide a current NIST SP 800–171 DoD Assessment on record, prior to contract award, whenever the offeror is required to implement NIST SP 800–171, pursuant to DFARS clause 252.204–7012. Due to this pre-existing minimum requirement for a Basic self-assessment under DFARS 252.204-7019 and the ability to establish corrective Plans of Action and Milestones, there are no circumstances likely to warrant approval of requests to waive CMMC Level 2 self-assessment requirements.

    b. In rare circumstances, such as when seeking competition from non-traditional DoD sources, waivers may be warranted for CMMC Level 2 third-party assessment requirements. Such waivers are not appropriate for contracts requiring performance by a cleared defense contractor. Approved waivers on a class basis must include a planned expiration date and guidance for requiring CMMC certification in subsequent solicitations. In all such cases, the solicitation must include a requirement to submit alternate protection plans for securing FCI or Controlled Unclassified Information (CUI) data. The alternate protection plans must be evaluated as part of the selection process.

3. CMMC Level 3 requirements: Level 3 requirements are intended to protect CUI associated with the Department's mission critical technologies and programs and result in an assessment performed by the Defense Contract Management Agency's Defense Industrial Base Cybersecurity Assessment Center. In rare circumstances, waivers may be warranted for CMMC Level 3 third-party assessment requirements: such waivers, however, are not appropriate for contracts or work statements requiring access to both unclassified and classified DoD information.