Summary of the concerns and clarifications regarding the Cybersecurity Maturity Model Certification (CMMC) and related DFARS requirements:

Reporting Requirement Concerns

- The term “any changes” in DFARS 252.204-7021 is too broad, potentially leading to excessive reporting.
- Routine updates, like Windows security updates, should not be reportable.
- Suggest focusing on significant changes affecting the CMMC assessment scope or major compliance posture changes.

COTS Exclusion Clarification

- Questions whether the definition applies to products sold by their company or generally in the commercial marketplace.
- Notes CMMC will apply to all DoD solicitations and contracts (except COTS items).

CMMC Self-Assessment vs. Level 2 Certification

- Clarification needed on when a contractor needs a CMMC self-assessment versus a Level 2 certification from a C3PAO.
- Asking if the contracting officer will specify this in the contract and if resources will be available for contractors to determine their certification needs before contract award.

Level 2 CMMC Certification for Consultants

- Consultants providing technical services should not require Level 2 CMMC certification if they do not handle CUI on their own systems.
- Highlighting the financial burden on independent contractors and small businesses to implement extensive IT infrastructure and obtain C3PAO assessments.

Timing of CMMC Certification

- **Early Scheduling:**
  - Contractors and subcontractors should schedule their CMMC certification well in advance to ensure it is completed by the time they submit their bids. This also allows for any necessary remediation to be addressed before the award is granted.
- **Clear Timing Expectations:**
  - It is recommended that RFP (Request for Proposal) and RFQ (Request for Quotation) documentation clearly outline the timing expectations for CMMC certification. This is particularly important for new contractors and subcontractors who will handle Controlled Unclassified Information (CUI), Covered Defense Information (CDI), and .
- **Proposed Solutions:**
  - **Self-Evaluation with Financial Incentives:** Allowing contractors to perform self-evaluations can expedite the certification process. Providing financial incentives for early completion of these evaluations can further encourage timely compliance.

- **Extended Award Times:** Extending the award times for new contractors and subcontractors can provide them with the necessary time to complete their CMMC certification without rushing, ensuring a thorough and compliant process.

Acceptable Changes During Certification

- **Clarification Needed:** Guidance is required on what changes are permissible in a CMMC certified environment during the 3-year certification period.
    - **Key Points:**
        - Annual affirmation of compliance is necessary.
        - The scope of the CMMC assessment must remain unchanged.
- **Scenarios Requiring Clarification:**
    - Replacing a cloud security protection asset.
    - Upgrading Controlled Unclassified Information (CUI) assets to Windows 11.
    - Implementing the latest Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) on CUI assets.

Definition of "Lapses in Information Security" (DFARS 252.204-7021):

- The term "lapses in information security" is not explicitly defined in DFARS 252.204-7021. However, it generally refers to any failures or weaknesses in maintaining the confidentiality, integrity, or availability of information, which could potentially lead to unauthorized access, disclosure, modification, or destruction of information.

Alignment with "Cyber Incident" (DFARS 252.204-7012(a)):

- The term "lapses in information security" can be considered broader than "cyber incident." According to DFARS 252.204-7012(a), a "cyber incident" is defined as actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein. While a cyber incident specifically involves network-based actions, lapses in information security could encompass a wider range of security failures, including physical security breaches or procedural errors.

Definitions from DFARS Clause 252.204-7012:

- **Compromise:** Disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.
- **Cyber Incident:** Actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

Replacement Suggestion:

- Replace “any lapses in information security” with “any cyber incidents” to align with the terminology and definitions provided in DFARS 252.204-7012.

Overlap with DFARS Clause 252.204-7012

- Reporting “cybersecurity lapses” to the contracting officer is impractical for tier 2+ subcontractors and may not add value since contracting officers are not cybersecurity experts. This could lead to negative performance ratings and stifle reporting.
- Suggest removing “lapses in information security” from paragraph (b)(4) and let DFARS Clause 252.204-7012 handle this requirement.