2101 WILSON BOULEVARD, SUITE 700
ARLINGTON, VA 22201-3060
(703) 522-1820 • (703) 522-1885 FAX
WWW.NDIA.ORG

January 9, 2020

Office of the Under Secretary of Defense for
Acquisition & Sustainment
Cybersecurity Maturity Model Certification

Re: Draft CMMC v0.7

To Whom It May Concern:

As an association, NDIA represents more than 1,600 corporate and over 80,000 individual members from small, medium, and large contractors; our members and their employees feel the impact of any policy change made in how the United States equips and supports its warfighters. Our comments provided via this letter and the comment matrix have come from this diverse membership and represent a broad range of perspectives across the defense industrial base.

Thank you for your work up to this point in publicly sharing drafts of the 0.4, 0.6 and 0.7 versions of the CMMC program. NDIA welcomes DOD's robust engagement with industry on this new model and looks forward to continuing the dialogue as the initial version 1.0 is released later this month. To help facilitate CMMC's ultimate success, NDIA has identified a number of implementation questions and comments, as well as proposed changes to the CMMC draft, as will be further discussed below.

NDIA is fully supportive of the CMMC vision and plan to create a "unified cybersecurity standard for DOD acquisition," including the establishment of a third-party certification process. In the interim, while CMMC is being developed, DOD components have been promulgating their own enhanced cybersecurity requirements for inclusion in solicitations and contracts. In addition, the FAR 52.204-21 and DFARS 252.204-7012 clause remains in the applicable regulations and there has been no indication that it will be removed or replaced. We would greatly appreciate hearing more about DOD's plan to avoid having multiple and different cybersecurity requirements imposed on contractors once CMMC is finalized. We urge DOD to provide industry with the opportunity to review and comment on DOD's proposed plans for the implementation and assessment of CMMC.

2101 WILSON BOULEVARD, SUITE 700
ARLINGTON, VA 22201-3060
(703) 522-1820 • (703) 522-1885 FAX
WWW.NDIA.ORG

## I. General Comments and Recommendations

1. Terminology used in the CMMC draft is inconsistent, causing significant swings in meaning that will frustrate CMMC's goals. The CMMC drafters continue to use FCI instead of CUI in Levels 1 and 2, but use CUI in Level 3. The FAR rule uses the term "FCI", but the DFARS rule uses the terms CTI and CUI. We propose that the CMMC coordinate with the FAR Council and conform to DFARS terminology so there is a common set of terms.

2. CMMC version 0.7 still lacks clarity on when Level 2 will apply. We are already aware prime contractors are facing challenges about flowing cyber requirements down their supply chain. We propose that CMMC provide explanation and clear direction about when Level 2 will and will not apply.

3. Appendixes B and C reference "**Draft** NIST SP 800-171R2." Reference to a draft is generally improper in binding contractual or compliance matters. We propose that CMMC reference only final standards.
4. CMMC Version 0.7 makes only a few isolated references to how a small number of controls would be applied in a cloud environment. In light of the fact that sensitive DOD data has been and will continue to be stored in the cloud, we recommend that DoD provide greater clarity on how the CMMC controls apply to contractor cloud environments and cloud service providers or advise if other changes are forthcoming to DFARS 252.239-7010 (Cloud Computing Services).
5. It remains unclear in CMMC Version 0.7 how the "practices" for each CMMC maturity level are supposed to interact with the "processes" for that level. Because a contractor must meet both the practices and the processes for a certain CMMC level to achieve that overall level, there is confusion about what is the "yardstick" to certify implementation (i.e., the yardstick for measuring implementation of the practice itself in accordance with the CMMC Level "Discussion and Clarification" guidance versus the yardstick for measuring "process maturity" related to that very same practice). Therefore, we recommend restating the "Maturity Level Capability" category as a "Capability" and recharacterizing the "processes" identified therein as "practices." This will allow maturity level assessment to be based solely on capabilities and practices, without the needless complexity of considering "processes" that are practically indistinguishable from practices.
6. Other areas that need clarification are as follows:
    i. Does CMMC recognize Plans of Action & Milestones (POAMs) as acceptable evidence of compliant implementation, as the DFARS regime does? The draft CMMC references the NIST SP 800-171

2101 WILSON BOULEVARD, SUITE 700
ARLINGTON, VA 22201-3060
(703) 522-1820 • (703) 522-1885 FAX
WWW.NDIA.ORG

requirement to "develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems" in the SAS domain (P1159). However, it is unclear from the draft CMMC whether having "plans of action" can demonstrate implementation of such controls as has been the stated position of DOD for over two years. In the DFARS Cybersecurity Clause context, DOD has indicated that having "plans of action" to meet certain NIST SP 800-171 controls in system security plans is sufficient to demonstrate "implementation" of such controls. (See, e.g., DPAP memorandum from Shay Assad dated 21 September 2017). Industry has relied on these statements. Please confirm whether DOD will continue to consider "plans of action" to demonstrate implementation of controls for purposes of CMMC certification.

ii. Is it DoD's intent that a minimum of a CMMC Level 3 will become the "default" maturity level for all programs or contracts where contractors process any type of data about DOD programs on their systems (such as financial records, etc.)? Without clarification from DoD, that result seems likely.

iii. How, when, and by whom will CMMC levels be determined for a multi-tiered supply chain working on separate, discrete aspects of a program? For example, will the Government determine in the RFP which CMMC levels apply to the prime contractor's supply chain? Will the prime/higher-tier contractor have an opportunity to obtain DoD approval to flow down to a lower-tier subcontractor a lower CMMC level than the CMMC level identified for the prime contract? Or will the contractor have discretion to determine the CMMC level for the next tier below? Will the subcontractor have any responsibilities for notifying the prime contractor of issues with the CMMC levels and be required to flow down to lower levels?

iv. Would CMMC would apply to Government Furnished Equipment (GFE) or classified systems?

v. Would only DOD prime contractors and subcontractors on a DOD contract be subject to the CMMC requirements? If not, who will and how will cost reimbursement be handled for those who are not prime contractors or subcontractors?

vi. If, as the OSD plan suggests, a comprehensive assessment of process maturity can "offset" the need for 100% compliance for some practices and a "methodology to handle maturity level trade-offs" is planned, how will such trade-offs work? We recommend against replacing the current self-attestation system with a check-

2101 WILSON BOULEVARD, SUITE 700
ARLINGTON, VA 22201-3060
(703) 522-1820 • (703) 522-1885 FAX
WWW.NDIA.ORG

the-box model. Contractors should have the flexibility to prioritize and engage in meaningful risk management. This is particularly true with respect to the NIST SP 800-171 controls in CMMC Level 3. For example, if a contractor has not fully implemented all NIST SP 800-171 controls in Level 3, could the contractor still be assessed and certified at CMMC Level 3 (or 4 or 5) based on its implementation of a CMMC Level 4 or 5 practice or procedure in lieu of the NIST SP 800-171 control(s) that it has not fully implemented, or on some other basis?

vii. If only lower CMMC levels will be required for small businesses, as suggested in the OSD plan, would this restrict small businesses from handling any critical CDI data? Would small businesses be categorically restricted from competing for or participating in Level 4 or 5 contracts for critical programs? This raises a concern particularly for small businesses that currently are engaged in handling critical CDI data and/or would have the capability to handle such data.

viii. Will certification levels of individual companies be public? How will companies know what CMMC level other companies (including their subcontractors) have achieved?

ix. What happens with companies that are not timely assessed? Will they be eligible for new bids? Would they lose existing business? Will contract options not be exercised?

x. In the early implementation of CMMC, if there are no suppliers for particular parts, equipment or services that have received assessments at the appropriate level, will prime contractors be able to apply for waivers so that they can successfully deliver products and services to the Government?

xi. How can a company "appeal" the result of its CMMC assessment? Likewise, does DOD anticipate that companies will be able to challenge the CMMC assessments of competitors in bid protests if a company loses an award to a competitor that the company has grounds to believe was rated too high?

xii. Will a certified contractor run the risk of de-certification during the course of performing a contract? Will there be periodic audits to determine if a contractor remains at a certification Level? What about certification at the lower tiers of the supply chain? How will this be handled?

xiii. Will DOD or certifiers advise contractors on the effect that a merger or a sale of assets will have on their certification level?

2101 WILSON BOULEVARD, SUITE 700
ARLINGTON, VA 22201-3060
(703) 522-1820 • (703) 522-1885 FAX
WWW.NDIA.ORG

xiv. What direction will third-party assessors be given regarding prioritizing which companies to assess first? Will the third-party assessors also be precluded from assessing other segments or units in their own companies and/or competitors to avoid organizational conflict of interests under the "impaired objectivity" standard?

xv. What is the scope of the contractor's internal information that will be subject to third-party assessment and certification under CMMC? Will only those systems that house or process CDI or FCI be within the scope of the third-party assessment and certification?

xvi. We are concerned that generally the contracting officer, program manager or representative will lack a calibrated way to determine the right CMMC level for an RFP and thus, to avoid any chance of criticism, they will simply designate it as Level 3 or higher by default. How can the government representative be confident and show justification in assigning a CMMC level lower than Level 3 whenever that is appropriate?

xvii. There has been an increasing use of teleworking in the government contracting and larger commercial community, yet the CMMC draft does not address how to handle the situation in which employees use their own devices to access and perform. Recommend that the CMMC address this important development as it affects both the federal and contractor/supply chain workforces and is a potential security gap as those terminals presumably would be considered "endpoints."

## II. Levels 1 and 2

1. **Discussion:**

Our members have expressed confusion as to where Level 2 will apply and be used in lieu of using Levels 1 or 3. There needs to be a clear justification included in the final model that explains where Level 2 will come into play. This justification will play an important role in convincing suppliers to make the investment necessary to comply with the Level 2 requirements.

Draft Version 0.7 is an improvement for Level 2 because the model has substituted the exact NIST security control language for the Level 2 Practices for the most part (but see next paragraph). References to other controls within the same Practice, such as the UK

2101 WILSON BOULEVARD, SUITE 700
ARLINGTON, VA 22201-3060
(703) 522-1820 • (703) 522-1885 FAX
WWW.NDIA.ORG

Cyber Essentials and the Australian ACSC Essential Eight, however, introduce increased compliance risk. While international standards can be instructive, reliance on a foreign government to update or enhance existing DoD security controls without U.S. Government oversight is unnecessary and could lead to inconsistencies in implementation between the NIST control and non-U.S. security control. Similarly, reliance on non-NIST (e.g., the CERT Resilience Management Model) and NIST controls for the same Practice could cause confusion in implementation, potentially resulting in greater vulnerabilities and higher costs to resolve inconsistencies. To the extent that the DoD wants to reference international or other security controls together with the NIST controls, we believe that these references should be included in a mapping table as context for contractors when implementing the CMMC Practice rather than separate and additional security requirements.

A number of the Level 2 Practices reference Federal Contract Information (FCI) in place of Controlled Unclassified Information (CUI), which is the term used in NIST SP 800-171 and applicable to DFARS 252.204-7012. FCI is properly addressed in Level 1 consistent with the security controls imposed by FAR 52.204-21. Level 2, however, includes eight controls that were derived from NIST SP 800-171, but it replaced the original term "CUI" with the more broadly defined term "FCI," as discussed in more detail below. If the FCI references are retained, the Model will be imposing standards that are different than those DoD/DCMA uses to evaluate contractor protection of CUI. The language in those controls should be modified to match the NIST/DFARS language precisely and reference CUI instead of FCI. Given that CMMC envisions that organizations requiring access to CUI and/or generating CUI should achieve CMMC Level 3, we recommend not only referencing CUI instead of FCI in those eight controls, but also moving those controls to Level 3.

In addition, those eight controls (along with one Level 1 control that references FCI) generally would require an understanding of how to identify "Federal Contract Information" (FCI) in order to be implemented effectively. If DoD retains reference to FCI in actual control language, we request that DoD provide guidance on how to identify FCI for the benefit of the presumably very large number of contractors who will be asked to meet these controls. Relatedly, we note that the definition of FCI in the CMMC document derives from FAR 52.204-21, but section C of that FAR clause indicates that contractors are not required to flow this clause in subcontracts for commercially available off-the-shelf items (COTS) even when the COTS subcontractors have FCI on their systems. Thus, to the extent DoD requires COTS providers to obtain CMMC certifications, it may be the case that many such providers are not otherwise subject to FAR 52.204-21 or familiar with the FCI term, thus adding even greater need for DoD to provide guidance on how to identify FCI is to contractors.

2101 WILSON BOULEVARD, SUITE 700
ARLINGTON, VA 22201-3060
(703) 522-1820 • (703) 522-1885 FAX
WWW.NDIA.ORG

We also note that the definition of FCI in Section 2.1.1 on page 3 of CMMC v0.7 document is inconsistent with the definition of FCI in FAR 52.204-21. To be consistent, the definition of FCI on page 3 should carve-out from the definition "simple transaction information, such as necessary to process payments."

Finally, there appear to be some errors in the "discussion and clarification" guidance in Appendix D for Level 2 that should be corrected. The guidance for AC P1014 appears in the Level 2 "discussion and clarification" section in Appendix C but is actually referencing a Level 3 control, so such guidance should be moved to Appendix D. The guidance for AC P1006 on page C-3 references CUI, but AC P1006 is a Level 2 control that does not reference CUI, so the reference to CUI should be deleted.

2. **Individual Level 2 Control Comments:** See attached **Appendix 1** for specific Level 2 comments.

III. **Level 3**

1. **Discussion:**

CMMC has been updated since the originally released draft to streamline this section's requirements to the NIST 800-171 controls not required by Levels 1 and 2 and 14 additional controls. The wording of the Level 3 NIST 800-171 based controls has been modified to use the current NIST 800-171 control language, thereby eliminating any potential inadvertent ambiguities. Unlike the Appendices for Levels 1 and 2, however, the Level 3 "discussion and clarification" in Appendix D excludes any content on the NIST 800-171 based controls.

We respectfully request that any additional content that is to be added prior to publication of CMMC Version 1.0 be made available in advance for public comment.

2. **Individual Level 3 Control Comments:**

- **P1035**, Identify, categorize, and label all CUI data, and **P1036**, Define procedures for the handling of CUI**,** are foundational requirements, however,

2101 WILSON BOULEVARD, SUITE 700
ARLINGTON, VA 22201-3060
(703) 522-1820 • (703) 522-1885 FAX
WWW.NDIA.ORG

they unfortunately cannot be implemented effectively at this time because DoD has not yet updated its own CUI identification, categorization and marking guidance in accordance with the 2016 NARA regulation. Our members have found that DoD employees are consistently unable to address questions regarding CUI on individual programs. DoD needs to update its guidance and fully educate its personnel prior to levying these requirements on private companies. As this is an ongoing concern, specific interim direction needs to be provided to ensure such questions are being properly addressed.

- **P1139**, Regularly perform complete and comprehensive data back-ups as organizationally defined and store them off-site and off-line. Given the costs associated with data back-ups, we recommend that DoD consider deleting this requirement from Level 3 (which will apply to all contracts where performance involves CUI) until DoD has studied the cost impact of imposing such a requirement. If DoD does not delete the control in its entirety, they should modify the requirement to read "Regularly perform complete and comprehensive data back-ups as organizationally defined and within organizationally-defined boundaries and store them off-line."

  **(1)** We recommend deletion of the "off-site" requirement. The underlying discussion section does not include any reference to data being stored off-site (versus off-line) and the clarification section, merely suggests that "you should consider storing at least one system backup off-site and offline to provide redundancy in the event of a disaster." This requirement would be difficult and costly for smaller companies with only one facility to implement. If not deleted, DoD should at a minimum add "as organizationally defined" to the end of the sentence.

  **(2)** We recommend the addition of the phrase "and within organizationally-defined boundaries" to clarify that this control does not apply to all internal systems as suggested in the real-world example provided in the "Discussion and Clarification" section on page D-5, including those that have no CDI, but to those that the company has determined using a risk-based approach warrant such back-ups. The Discussion and Clarification section should also be corrected to delete the reference to all systems.

- **P1162**, "Employ code reviews of enterprise software that has been developed internally for internal-use to identify areas of concern that require additional improvements." Recommend changing the requirement to read "Based on organizationally-defined risk factors, employ code reviews of enterprise software that has been developed internally for internal-use to identify areas of concern

2101 WILSON BOULEVARD, SUITE 700
ARLINGTON, VA 22201-3060
(703) 522-1820 • (703) 522-1885 FAX
WWW.NDIA.ORG

that require additional improvements" to enable companies to apply such controls where risk factors warrant such controls rather than apply to "all in-house developed software" as suggested by the Appendix D clarification of this control on page D-11. The DoD should similarly make a corresponding clarification to the referenced Appendix D clarification language.

## IV. Levels 4 and 5

### 1. Discussion:

CMMC Version 0.7 contains "Discussion and Clarification" appendices only for Levels 1-3, and not for Levels 4 and 5. We respectfully request that any additional content with respect to such appendices be made available for public comment in advance of publication of CMMC Version 1.0.

Optimized vs. Optimizing: The sentiment within the model of requiring companies to be "optimized" with regards to achieving level 5 certification should instead be replaced with language encouraging companies seeking and obtaining level 5 certification to be responsible for continually "optimizing" their system and practices. A company should be continually tweaking and enhancing its cyber processes to avoid threats and accommodate changing technologies. No company is going to be able to continually operate in an "optimized", static, state with regards to cybersecurity. The use of the concept of "optimizing" is also consistent with CMMI Level 5 requirements. We suggest making adjustments to language in the following instances to accommodate the goal of "optimizing":

- Page 2, section 2.1 => "…to being continuously optimized across the organization…"
- Page 2 graphic => "Level 5 – Optimizing"
- Page 4 first paragraph => "…ability to continuously optimize their cybersecurity capabilities. The organization has the capability to continuously optimize their cybersecurity capabilities…"
- Page 4 table => "…a proven ability to continuously optimize capabilities in an effort to repel…"
- Page 7 table => "ML 5: Optimizing"

2101 WILSON BOULEVARD, SUITE 700
ARLINGTON, VA 22201-3060
(703) 522-1820 • (703) 522-1885 FAX
WWW.NDIA.ORG

**2. Individual Level 4 and 5 Control Comments:**

Many Version 0.7 Level 4 and 5 practices rightly contain scope-limiting terms that permit contractors to apply controls to "organizationally defined" systems or boundaries, or based on "organizationally defined" risks. These important terms help to clarify that contractors should conduct a risk-informed analysis and prioritize their efforts and expenditures on the systems (or portions thereof) that matter most, such as those that process and store Covered Defense Information in connection with programs assigned maturity Levels 4 or 5. However, other L4/L5 practices lack such qualifiers but should include them, because contractors may interpret the language without such clarifiers to require them to expend resources to implement these burdensome controls indiscriminately across their entire enterprise, rather than based on a risk-informed analysis. In particular, we recommend these revisions to the following L4/L5 practices:

- **P1024**: Identify and mitigate risk associated with unidentified wireless access points connected to organizationally-defined networks.
- **P1054**: Review audit information for broad activity in addition to per-machine activity within organizationally-defined boundaries.
- **P1074**: Employ organizationally-defined roots of trust, formal verification, or cryptographic signatures to verify the integrity and correctness of security critical or essential software as defined by the organization.
- **P1102**: Use a combination of manual and automated, real-time responses to organizationally-defined anomalous activities that match incident patterns.
- **P1148**: Develop and update a plan for managing supply chain risks based on organizationally-defined risk factors associated with the IT supply chain.
- **P1149**: Catalog and periodically update threat profiles and adversary TTPs based on organizationally-defined risk factors.
- **P1155**: Analyze the effectiveness of security solutions at least annually to address anticipated risk to organizationally-defined systems and the organization based on current and accumulated threat intelligence.
- **P1171**: Establish and maintain a cyber threat hunting capability to search for indicators of compromise in organizationally-defined systems and detect, track, and disrupt threats that evade existing controls.
- **P1222**: Analyze system behavior based on organizationally-defined risk factors to detect and mitigate execution of normal systems commands and scripts that indicate malicious actions.

2101 WILSON BOULEVARD, SUITE 700
ARLINGTON, VA 22201-3060
(703) 522-1820 • (703) 522-1885 FAX
WWW.NDIA.ORG

- **P1223**: Monitor individuals and system components on an ongoing basis for anomalous or suspicious behavior based on organizationally-defined risk factors.
- **P1226**: Employ automated capability based on organizationally-defined risk factors to discover and identify systems with specific component attributes (e.g., firmware level, OS type) within your inventory.
- **P1229**: Utilize a URL categorization service and implement techniques within organizationally-defined boundaries to enforce URL filtering of websites that are not approved by the organization.
- **P1230**: Enforce port and protocol compliance within organizationally-defined boundaries.

We also have comments on these additional controls:

- **P1101:** Establish and maintain a security operations center during relevant business hours with on-call response after hours.
    - **Proposed Revision:** Establish and maintain a security operations center during relevant business hours, and establish and maintain a capability for on-call response after hours.
    - **Rationale:** As originally written, control P1101 could be interpreted to require a Level 4 contractor's after-hours on-call response capability to be part of the "centralized function" of the security operation center "within" the organization, based on the definition of "security operations center" in Appendix F. DoD should clarify instead that the "on call" function may be outsourced. Without that clarification, there is little if any distinction between the capabilities described in the Level 4 control P1101 and the Level 5 control P1007, which requires contractors to "Establish and maintain a security operations center that facilitates a 24/7 response capability."
- **P1140:** Ensure information processing facilities meet organizationally defined information security continuity, redundancy, and availability requirements.
    - **Proposed Revision:** Ensure information processing facilities meet organizationally defined information security requirements.
    - **Rationale:** The core purpose of the CMMC and other standards that preceded it (and on which it is largely based) is the confidentiality of information, in particular CDI. Controls designed to ensure "continuity,

2101 WILSON BOULEVARD, SUITE 700
ARLINGTON, VA 22201-3060
(703) 522-1820 • (703) 522-1885 FAX
WWW.NDIA.ORG

redundancy, and availability" are quite burdensome and are not designed to keep sensitive information out of the hands of our adversaries. DoD should accordingly avoid imposing and incurring costs via CMMC unrelated to that core CMMC objective.

If you would like to discuss our comments and suggestions, please let NDIA know. We would be happy to engage in a dialogue on the CMMC program, its implementation and requirement plans, to ensure that the program when implemented will address DoD concerns and industry needs.

If you or your staff have any questions, please contract Corbin Evans, Director of Regulatory Policy, at cevans@ndia.org or (703) 247-2598.

Respectfully Submitted,

National Defense Industrial Association

Enclosed:
Appendix 1: Level 2 Individual Control Comments

**Appendix 1: Level 2 Individual Control Comments**

| CMMC Draft 7 | CMMC Draft V7 Capability | Controls Cited (and comparison to Draft V4 and V7) | Compare to CMMC Draft 4 | Controls in L2 V4 deleted /moved in V7 | Comments |
|---|---|---|---|---|---|
| AC, C001, P1005 | "Provide privacy and security notices consistent with applicable Federal Contract Information rules." | 3.1.9 | Was AC, C1, L2-1<br><br>Wording changed from:<br>"System logon screens display the appropriate system use notification messages" | | FCI is properly addressed in Level 1 consistent with the security controls imposed by FAR 52.204-21. Level 2, however, anticipates that a contractor will have access to CUI but uses the term FCI instead. Consistent with the NARA rule on CUI, Level 2 security controls should address only CUI and not FCI. If the FCI references are retained, the Model will be imposing standards that are different than those DoD/DCMA uses to evaluate contractor protection of CUI. Language should be modified to match NIST control language precisely, except in the case where CMMC is adding new non-NIST practices. |
| AC, C001, P10006 | "Limit use of portable storage devices on external systems." | 3.1.21 | Was previously found at AC L2-1 in Version 0.4. Wording originally stated "CUI stored on portable storage devices on external systems are | | Agree with CMMC drafters in use of exact language of NIST control. |

| CMMC Draft 7 | CMMC Draft V7 Capability | Controls Cited (and comparison to Draft V4 and V7) | Compare to CMMC Draft 4 | Controls in L2 V4 deleted /moved in V7 | Comments |
|---|---|---|---|---|---|
| | | | identified and documented. Limits on the use of such storage devices is defined." | | |
| AC, C002, P1007 | "Employ the principle of least privilege, including for specific security functions and privileged accounts." | 3.1.5 (same) UK NCSC Cyber Essentials (new) | Was AC, C2, L2-2<br><br>Wording changed: "Only grant privileges necessary for a system user to fulfill their assigned duties."<br><br>But substance appears the same | | Agree with CMMC drafters in use of exact language of NIST control. Reference to other controls within the same Practice, such as the UK Cyber Essentials, however, introduce increased compliance risk. While international standards can be instructive, reliance on a foreign government to update or enhance existing DoD security controls without U.S. Government oversight is unnecessary and could lead to inconsistencies in implementation between the NIST control and non-U.S. security control. Similarly, reliance on multiple security controls for the same Practice could cause confusion in implementation, potentially resulting in greater |

| CMMC Draft 7 | CMMC Draft V7 Capability | Controls Cited (and comparison to Draft V4 and V7) | Compare to CMMC Draft 4 | Controls in L2 V4 deleted /moved in V7 | Comments |
|---|---|---|---|---|---|
| | | | | | vulnerabilities and higher costs to resolve inconsistencies. To the extent that the DoD wants to reference international or other security controls together with the NIST controls, we believe that these references should be included in a mapping table as context for contractors when implementing the the CMMC Practice rather than separate and additional security requirements. |
| AC, C002, P1008 | "Use non-privileged accounts or roles when accessing nonsecurity functions." | 3.1.6<br>UK NCSC Cyber Essentials | Previously found in Level 3 (L3-1) in Access Control for C2 (Control internal system access) and moved down to Level 2 | | Agree with CMMC drafters in use of exact language of NIST control. Reference to other controls within the same Practice, such as the UK Cyber Essentials, however, introduce increased compliance risk. (See comment above for AC C002, P1007). |
| AC, C002, P1009 | "Limit unsuccessful logon attempts." | 3.1.8 | Previously found in Level 1 (C2, L1-2) in V0.4 although language was different. | | Agree with CMMC drafters in use of exact language of NIST control. |

**Appendix 1: Level 2 Individual Control Comments**

| CMMC Draft 7 | CMMC Draft V7 Capability | Controls Cited (and comparison to Draft V4 and V7) | Compare to CMMC Draft 4 | Controls in L2 V4 deleted /moved in V7 | Comments |
|---|---|---|---|---|---|
| AC, C002, P1010 | "Use session lock with pattern-hiding." displays to prevent access and viewing of data after a period of inactivity." | 3.1.10 | Previously found at Level 3 (C2 L3-4) although the language was different. | | Agree with CMMC drafters in use of exact language of NIST control. |
| AC, C002, P1011 | "Authorize wireless access prior to allowing such connections." | 3.1.16 | Was C2, L2-3 Changed wording: "All wireless is authorized prior to allowing such connections." | | Agree with CMMC drafters in use of exact language of NIST control. |
| AC, C003, P014 | "Employ cryptographic mechanisms to protect the confidentiality of remote access sessions." | 3.1.13 | Previously found in Level 3 in Access Control (C3, L3-1) but language was "Ensure all remote access sessions are encrypted." | | Agree with CMMC drafters in use of exact language of NIST control. |
| AC, C003, P1015 | "Route remote access via managed access control points." | 3.1.14 | Previously found at Level 3, but was written "All remote access sessions should be routed through | | Agree with CMMC drafters in use of exact language of NIST control. |

| CMMC Draft 7 | CMMC Draft V7 Capability | Controls Cited (and comparison to Draft V4 and V7) | Compare to CMMC Draft 4 | Controls in L2 V4 deleted /moved in V7 | Comments |
|---|---|---|---|---|---|
| | | | managed access control points." | | |
| AC, C004, P1016 | "Control the flow of Federal Contract Information in accordance with approved authorizations." | 3.1.3<br>UK NCSC Cyber Essentials | Previously stated "The system architecture is implemented to control the flow of data. Enforcement occurs in boundary protection devices such as gateways, routers, guards, encrypted tunnels, firewalls." | | Agree with CMMC drafters in use of exact language of NIST control. Reference to other controls within the same Practice, such as the UK NCSC Cyber Essentials, however, introduce increased compliance risk. (See comment above for AC, C002, P1007) |
| AA, C007, P1041 | Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions. | 3.3.2 (same)<br>CERT RMM v1.2 MON:SG1.SP3 (same) | Was AA, C1, L2-1<br>Wording changed: "The content of audit records has been defined to ensure events can be traced back to a specific user." | | Agree with CMMC drafters in use of exact language of NIST control. Reference to other controls within the same Practice, such as the CERT RMM, however, introduce increased compliance risk. (See comment above for AC, C002, P1007) |
| AA, C008, P1042 | "Create and retain system audit logs and records to the extent needed to enable | 3.3.1<br>CERT RMM v1.2 MON:SG1.SP3 | Similar to AA, C3, L2-1 - The organization has defined audit data storage and retention requirements (RMM MON:SG1.SP3) | | Agree with CMMC drafters in use of exact language of NIST control. Reference to other controls within the same Practice, such as the CERT RMM, however, |

| CMMC Draft 7 | CMMC Draft V7 Capability | Controls Cited (and comparison to Draft V4 and V7) | Compare to CMMC Draft 4 | Controls in L2 V4 deleted /moved in V7 | Comments |
|---|---|---|---|---|---|
| | the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity." | | | | introduce increased compliance risk. (See comment above for AC, C002, P1007). |
| AA, C008, P1043 | "Provide a system capability that compares and synchronizes internal system clocks," with an authoritative source to generate time stamps for audit records." | 3.3.7 (same) | Used to be AA, C3, L2-2 wording changed: "A system capability is provided that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records." | | Agree with CMMC drafters in use of exact language of NIST control. |
| AA, C010, P1044 | "Review audit logs." | CMMC (new) | Similar to AA, C6, L2-1 - Staff are assigned to review and manage audit logs. This old control cited 3.3.5 (which now appears in Level 3 control) | | This Practice should be revised as follows: "Review audit logs consistent with organizationally defined risk factors." This clarification bounds the scope of the practice and ties back to the fundamental concept of risk. Our proposed language is also consistent with the CMMC discussion section |

| CMMC Draft 7 | CMMC Draft V7 Capability | Controls Cited (and comparison to Draft V4 and V7) | Compare to CMMC Draft 4 | Controls in L2 V4 deleted /moved in V7 | Comments |
|---|---|---|---|---|---|
| | | | | | which states that: "…log review should be determined based on a risk assessment…." |
| AT, C011, P1056 | "Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems." | 3.2.1 (same) CERT RMM v1.2 OTA:SG1.SP1 (same) | Was AT, C1, L2-1 Reference to RMM in 0.6 adds "v1.2" | | Agree with CMMC drafters in use of exact language of NIST control. Reference to other controls within the same Practice, such as the CERT RMM, however, introduce increased compliance risk. (See comment above for AC, C002, P1007) |
| AT, C012, P1057 | "Ensure that personnel are trained to carry out their assigned information security related | 3.2.2 Moved from C4, L2-1 CERT RMM v1.2 OTA:SG4.SP1 (same) | Was AT, C4, L2-1 Reference to RMM in 0.6 adds "v1.2" Wording changed: AT, C4, L2-1 "The organization trains personnel to carry out | | Agree with CMMC drafters in use of exact language of NIST control. Reference to other controls within the same Practice, such as the CERT RMM, however, introduce increased |

| CMMC Draft 7 | CMMC Draft V7 Capability | Controls Cited (and comparison to Draft V4 and V7) | Compare to CMMC Draft 4 | Controls in L2 V4 deleted /moved in V7 | Comments |
|---|---|---|---|---|---|
| | duties and responsibilities." | | their assigned information security-related duties and responsibilities."<br>• NIST SP 800-1713.2.2<br>• RMM OTA:SG4.SP2" | | compliance risk. (See comment above for AC, C002, P1007). |
| CM, C013, P1061 | "Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles." | 3.4.1 moved from CM, C3, L1-1<br>CERT RMM v1.2 KIM:SG5.SP2 | CM, C1, L1-1, Reference to RMM in 0.6 adds "v1.2"<br><br>Wording changed: "Configuration baselines for organizational systems are established, at least in an ad hoc manner." | | Agree with CMMC drafters in use of exact language of NIST control. Reference to other controls within the same Practice, such as the CERT RMM, however, introduce increased compliance risk. (See comment above for AC, C002, P1007). |
| CM, C013, P1062 | "Employ the principle of least functionality by configuring organizational systems to | 3.4.6 (same)<br>UK NCSC Cyber Essentials (new) | CM, C3, L2-2<br><br>Wording changed: "Configuration baselines for information technology | | Agree with CMMC drafters in use of exact language of NIST control. Reference to other controls within the same Practice, such as the UK NCSC Cyber Essentials, |

| CMMC Draft 7 | CMMC Draft V7 Capability | Controls Cited (and comparison to Draft V4 and V7) | Compare to CMMC Draft 4 | Controls in L2 V4 deleted /moved in V7 | Comments |
|---|---|---|---|---|---|
| | provide only essential capabilities." | | employ the principle of least functionality."<br><br>But substance appears the same | | however, introduce increased compliance risk. (See comment above for AC, C002, P1007) |
| CM, C013, P1063 | "Control and monitor user-installed software." | 3.4.9 (same) | CM, C3, L2-3<br><br>Wording changed: "Configuration baselines for information technology include requirements for user installed software." | | Agree with CMMC drafters in use of exact language of NIST control. |
| CM, C014, 1064 | "Establish and enforce security configuration settings for information technology products employed in organizational systems." | 3.4.2 (same)<br>Deleted RMM ADM: SG3.SP1<br>Deleted RMM KIM:SG5.SP2 | Was CM, C2, L2-1 and CM, C5, L2-1<br><br>Wording changed: "The organization establishes configuration management requirements for information technology."<br><br>"The organization performs configuration management for | | Agree with CMMC drafters in use of exact language of NIST control and deletion of additional controls. (See comment above for AC C002, P1007). |

| CMMC Draft 7 | CMMC Draft V7 Capability | Controls Cited (and comparison to Draft V4 and V7) | Compare to CMMC Draft 4 | Controls in L2 V4 deleted /moved in V7 | Comments |
|---|---|---|---|---|---|
| | | | organizational systems based on established requirements. | | |
| CM, C014, P1065 | "Track, review, approve, or disapprove, and log changes to organizational systems." | 3.4.3 (same)<br>CERT RMM v1.2 KIM:SG5.SP2 (same)<br>AU ACSC Essential Eight (new) | Was CM, C4, L2-1<br>Reference to RMM in 0.6 adds "v1.2"<br><br>Wording changed: "The organization tracks, reviews, manages, and log changes ot organizational systems based on the change management process."<br><br>But substance appears the same. | | Agree with CMMC drafters in use of exact language of NIST control. Reference to other controls within the same Practice, such as the CERT RMM and AU ACSC Esential Eight, however, introduce increased compliance risk. (See comment above for AC, C002, P1007) |
| CM, C014, P1066 | Analyze the security impact of changes prior to implementation | 3.4.4 (same) | Was CM. C4, L2-2<br><br>Wording changed: "Established security requirements are analyzed to determine impacts prior to change implementation."<br><br>But substance appears the same. | | Agree with CMMC drafters in use of exact language of NIST control. |

**Appendix 1: Level 2 Individual Control Comments**

| CMMC Draft 7 | CMMC Draft V7 Capability | Controls Cited (and comparison to Draft V4 and V7) | Compare to CMMC Draft 4 | Controls in L2 V4 deleted /moved in V7 | Comments |
|---|---|---|---|---|---|
| Identification and Authorization (V.6 uses Identification and Authentication) IDA, C015, P1078 | "Enforce a minimum password complexity and change of characters when new passwords are created" | 3.5.7 | Moved from C2, L3, L3-5 | | Agree with CMMC drafters in use of exact language of NIST control. |
| IDA, C1, L2-1 Moved to C015, L1, P1076 | "Identify information system users, processes acting on behalf of users, or devices." | 3.5.1 52.204-21 | | | Agree with CMMC drafters in use of exact language of NIST control and FAR 452.204-21(b)(v) control. |
| IDA, C015, P1079 Moved from IDA, C2, L3-6 | "Prohibit password reuse for a specified number of generations." | 3.5.8 | Moved from L3 to L2 | | Agree with CMMC drafters in use of exact language of NIST control. |
| IDA, C015, P0180 Moved from IDA, C2, L3-7 | "Allow temporary password use for system logons with an immediate change to a | 3.5.9 | Moved from L3 to L2 | | Agree with CMMC drafters in use of exact language of NIST control. |

| CMMC Draft 7 | CMMC Draft V7 Capability | Controls Cited (and comparison to Draft V4 and V7) | Compare to CMMC Draft 4 | Controls in L2 V4 deleted /moved in V7 | Comments |
|---|---|---|---|---|---|
| | permanent password." | | | | |
| IDA, C015, P1081 Moved from IDA, C2, L3-8 | "Store and transmit only cryptographically-protected passwords." | 3.5.10 | Moved from L3 to L2 | | Agree with CMMC drafters in use of exact language of NIST control. |
| IDA, C015, P1082 Moved from IDA, C2, L3-9 | "Obscure feedback of authentication information." | 3.5.11 | New Moved from L3 to L2 | | Agree with CMMC drafters in use of exact language of NIST control. |
| IR,C016, P1092 | "Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities." | 3.6.1 (same) | Was IR, C5, L2-4<br><br>Was IR, C5, L1-1 Wording changed: "The organization has a process for analyzing incidents to determine a response."(RMM IMC:SG3.SP2 deleted, 3.6.1)<br><br>Was IR, C7, L2-1 Wording changed: " The organization has a process for managing incidents to resolution including: declaring, | | Agree with CMMC drafters that an incident response plan is beneficial for this level (Level 2). |

| CMMC Draft 7 | CMMC Draft V7 Capability | Controls Cited (and comparison to Draft V4 and V7) | Compare to CMMC Draft 4 | Controls in L2 V4 deleted /moved in V7 | Comments |
|---|---|---|---|---|---|
| | | | escalating, and developing and implementing a response." ( RMM IMC:SG1.SP1)<br><br>Was IR, C7, L2-2 Wording changed: "Roles and responsibiltites for managing incidents have ben established and staff has been assigned." (RMM IMC: SG1,SP2) | | |
| IR, C017, P1093 | "Detect and report events." | CERT RMM v1.2 IMC:SG2.SP1 (same) | Was IR, C1, L2-1 Reference to RMM in 0.6 adds "v1.2"<br><br>Wording changed: "The organization has a process for detecting and reporting events."<br><br>But substance appears the same | | This control is already incorporated into Level 3 at P1098 and P1092 above.<br><br>Suggest removing this control from Level 2 and including it with Level 3 at P1098, as part of NIST 800-171 3.6.2 requirements, or clarifying and incorporating the citation into P1092. |

| CMMC Draft 7 | CMMC Draft V7 Capability | Controls Cited (and comparison to Draft V4 and V7) | Compare to CMMC Draft 4 | Controls in L2 V4 deleted /moved in V7 | Comments |
|---|---|---|---|---|---|
| IR, C017, P1094 | "Analyze and triage events to support event resolution and incident declaration." | CERT RMM v1.2 IMC:SG2.SP4 (same) | Was IR, C1, L2-2<br>Reference to RMM in 0.6 adds "v1.2"<br><br>Wording changed: "The organization has a process for categorizing events." | | This control is already incorporated into P1092 and the control should clarify that required reporting is internal and not external. If external reporting is contemplated, then we suggest moving this control to Level 3 at P1098. The cited publication does distinguish between an event and an incident, which is helpful to understand the control, but unnecessary if a new FAR or DFARS rule is introduced to enforce the CMMC.<br><br>Suggest moving this control to Level 3 or incorporating the citation into P1092. The discussion to this practice (whether it is incorporated into another or stays by itself) should also address triage that is automated. |
| IR, C018, P1096 | "Develop and implement responses to | CERT RMM v1.2 IMC:SG4.SP2 (new) | Was IR, C1, L2-3<br>Reference adds "v1.2" | | This control is already incorporated into control P1092 and control P1094. We note that control P1096 |

| CMMC Draft 7 | CMMC Draft V7 Capability | Controls Cited (and comparison to Draft V4 and V7) | Compare to CMMC Draft 4 | Controls in L2 V4 deleted /moved in V7 | Comments |
|---|---|---|---|---|---|
| | declared incidents according to predefined procedures." | Drops 3.6.1 | Wording changed: "The organization has a process for managing events to resolution."<br><br>Was IR, C5, L2-2 Wording changed: "The organization has a process for developing and implementing responses including preparation, detection, analysis, containment, recovery, and user response activities."<br><br>Was IR, C5, L2-4 Wording changed: "Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis , containment, recovery, and user response activities." (3.6.1) | | previously cited NIST 800-171 requirement 3.6.1, which is cited by control P1092.<br><br>Suggest removing this control and incorporating the citation into P1092 and P1094. |
| IR, C019, P1097 | "Perform root cause analysis on incidents | CERT RMM v1.2 IMC:SG5.SP1 | New | | The cited publication, IMC:SG5.SP1 requires a business to conduct a post- |

| CMMC Draft 7 | CMMC Draft V7 Capability | Controls Cited (and comparison to Draft V4 and V7) | Compare to CMMC Draft 4 | Controls in L2 V4 deleted /moved in V7 | Comments |
|---|---|---|---|---|---|
| | to determine underlying causes." | | | | incident review that includes obtaining input from "all relevant stakeholders," including "those affected by the incident." Such stakeholders are undefined and may not always be cooperative. Although the cited publication is only for reference, its language could confuse how this practice is applied.<br><br>We suggest moving this control to Level 3 at P1098, which covers external reporting if external reporting is contemplated.<br><br>Note that a citation to NIST 800-53, IR-4 may be sufficient because it incorporates "lessons learned" from incidents. |
| MA, C021, P111 | "Perform maintenance on organizational systems." | 3.7.1 (same)<br>RMM v1.2 TM: SG5.SP2 | Was MA, C1, L2-1<br>Reference to RMM in 0.6 adds "v1.2" | | We agree that maintenance at this level is an appropriate step beyond the basic hygiene required at Level 1. Improvement by using exact NIST language. Reference to |

| CMMC Draft 7 | CMMC Draft V7 Capability | Controls Cited (and comparison to Draft V4 and V7) | Compare to CMMC Draft 4 | Controls in L2 V4 deleted /moved in V7 | Comments |
|---|---|---|---|---|---|
| | | | | | other controls within the same Practice, such as the CERT RMM, however, introduce increased compliance risk. (See comment above for AC, C002, P1007) |
| MA, C021, P1112 | "Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance." | 3.7.2 (same) | Was MA, C2, L2-1 and L2-2<br><br>Wording changed "The organization identifies approved tools and techniques to conduct system maintenance."<br><br>"The organization identifies and implement controls on the tools, techniques, mechanism, and personnel used ot conduct system maintenance."<br><br>But substance appears the same | | We agree that maintenance at this level is an appropriate step beyond the basic hygiene required at Level 1. We note that 3.7.2 is limited to tools that "are used specifically for diagnostic and repair actions on [CUI] systems." Therefore, it does not apply to FCI that is not CUI. |

| CMMC Draft 7 | CMMC Draft V7 Capability | Controls Cited (and comparison to Draft V4 and V7) | Compare to CMMC Draft 4 | Controls in L2 V4 deleted /moved in V7 | Comments |
|---|---|---|---|---|---|
| MA, C021, P113 | "Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete." | 3.7.5 (same) | Was MA, C2, L2-3<br><br>Wording changed: "The organization identifies multifactor authentication requirements for maintenance sessions via external network connections." | | This requirement is closely tied to multifactor authentication techniques required by NIST SP 800-171 3.5.3, which applies to local and network accounts. Level 3 applies 3.5.3 at P1083, and is consistent with the more stringent authentication requirements at that level.<br><br>We suggest moving this practice to Level 3, which would be consistent with a business maturity progression and capability. |
| MA, C021, P114 | 'Supervise the maintenance activities of personnel without required access authorization." | 3.7.6 (same) | Was MA, C2, L2-4<br><br>Wording changed: "The organization supervises maintenance activities of personnel without required access authorization."<br><br>But substance appears the same. | | We agree that supervision of maintenance activities at this level is an appropriate step beyond the basic hygiene required at Level 1. |

| CMMC Draft 7 | CMMC Draft V7 Capability | Controls Cited (and comparison to Draft V4 and V7) | Compare to CMMC Draft 4 | Controls in L2 V4 deleted /moved in V7 | Comments |
|---|---|---|---|---|---|
| MP, C023, P119 | "Protect (i.e., physically control and securely store) system media containing Federal Contract Information, both paper and digital." | 3.8.1 (same) CERT RMM v1.2 KIM: SG2.SP2 (same) | Was MP, C2, L2-1 Reference to RMM in 0.6 adds "v1.2"<br><br>Wording changed: "The organization has a process for physically protecting media (non-digital and digital) containing CUI." | | We note that NIST SP 800-171 3.8.1 is a security requirement that applies to "CUI" and not "FCI." KIM:SG2.SP2 is a broad practice that applies to more than just system media. The cite can confuse proper compliance if the practice is interpreted broadly.<br><br>Suggest removing KIM:SG2.SP2. Suggest using the exact language of the NIST security requirement. |
| MP, C023, P120 | "Limit access to Federal Contract Information on system media to authorized users." | 3.8.2 (same) CERT RMM v1.2 MON: SG2.SP4 (same) | Was MC, C2, LP-2 Reference to RMM in 0.6 adds "v1.2"<br><br>Wording changed: "The organization has a process for limiting access to media containing CUI to authorized users." | | We note that NIST SP 800-171 3.8.2 is a security requirement that applies to "CUI" and not "FCI." We suggest using the exact language of the NIST security requirement in order to maintain consistency with DFARS requirements.<br><br>We agree that limiting access to FCI at Level 2 is an appropriate step beyond the |

| CMMC Draft 7 | CMMC Draft V7 Capability | Controls Cited (and comparison to Draft V4 and V7) | Compare to CMMC Draft 4 | Controls in L2 V4 deleted /moved in V7 | Comments |
|---|---|---|---|---|---|
| | | | | | basic hygiene required at Level 1.<br><br>Suggest clarifying that contracts with CUI must adhere to DFARS 252.205-7012 and 800-171 and not MON:SG2.SP4.<br><br>Reference to other controls within the same Practice, such as the CERT RMM, however, introduce increased compliance risk. (See comment above for AC, C002, P1007) |
| MP, C023, P121 | "Control the use of removable media on system components." | 3.8.7 (same)<br>CERT RMM v1.2 MON: SG2.SP4 (same) | Was MP, C6, L2-1<br>Reference to RMM in 0.6 adds "v1.2"<br><br>Wording changed: "The organization has a process for controlling the use of removable media on system components." | | We agree that the practice of controlling the use of removable media at Level 2 is an appropriate step beyond the basic hygiene required at Level 1.<br><br>Reference to other controls within the same Practice, such as the CERT RMM, however, introduce increased compliance risk. (See comment above for AC, C002, P1007) |

| CMMC Draft 7 | CMMC Draft V7 Capability | Controls Cited (and comparison to Draft V4 and V7) | Compare to CMMC Draft 4 | Controls in L2 V4 deleted /moved in V7 | Comments |
|---|---|---|---|---|---|
| | | | | | |
| PS, C026, P1127 | "Screen individuals prior to authorizing access to organizational systems containing Federal Contract Information." | 3.9.1 (same) CERT RMM v1.2HRM:SG2. SP1 (same) | Was SP, C1, L2-1 Reference to RMM in 0.6 adds "v1.2"<br><br>Wording changed: "the organization has a process for screening individuals prior ot authorizing access to organizational systems containing CUI." | | We agree that the practice of screening individuals at Level 2 is an appropriate step beyond the basic hygiene required at Level 1.<br><br>We note that NIST SP 800-171 3.9.1 is a security requirement that applies to "CUI" and not "FCI." We suggest using the exact language of the NIST security requirement in order to maintain consistency with DFARS requirements.<br><br>Reference to other controls within the same Practice, such as the CERT RMM, however, introduce increased compliance risk. (See comment above for AC, C002, P1007) |
| PS, C027, P1128 | "Ensure that organizational systems | 3.9.2 (same) CERT RMM v1.2HRM:SG4. SP2 (same) | Was SP, C2, L2-1 Reference to RMM in 0.6 adds "v1.2" | | We agree that the practice of protecting information after terminations and/or transfers at Level 2 is an appropriate step beyond the |

| CMMC Draft 7 | CMMC Draft V7 Capability | Controls Cited (and comparison to Draft V4 and V7) | Compare to CMMC Draft 4 | Controls in L2 V4 deleted /moved in V7 | Comments |
|---|---|---|---|---|---|
| | containing Federal Contract Information are protected during and after personnel actions such as terminations and transfers." | | Wording changed: "The organization has a process to ensure CUI is protected during personnel action." | | basic hygiene required at Level 1.<br><br>We note that NIST SP 800-171 3.9.2 is a security requirement that applies to "CUI" and not "FCI." We suggest using the exact language of the NIST security requirement in order to maintain consistency with DFARS requirements.<br><br>Also, in cases where CUI is involved, there should be a specific attempt to protect that information given the reporting requirements that a cyber incident may create (e.g. an employee is terminated and then leaves with CUI/CDI in a disk). Folding all information into "FCI" may confuse the need for this specific protection of CUI.<br><br>Reference to other controls within the same Practice, such as the CERT RMM, |

| CMMC Draft 7 | CMMC Draft V7 Capability | Controls Cited (and comparison to Draft V4 and V7) | Compare to CMMC Draft 4 | Controls in L2 V4 deleted /moved in V7 | Comments |
|---|---|---|---|---|---|
| | | | | | however, introduce increased compliance risk. (See comment above for AC, C002, P1007) |
| PP, C028, P1135 | "Protect and monitor the physical facility and support infrastructure for organizational systems." | 3.10.2 (same)<br>CERT RMM v1.2 KIM:SG4.SP2 (same) | Was PP, C2, L2-4<br>And<br>PP, C1, L2-1<br>And<br>PP, C5, L2-2<br><br>Reference to RMM in 0.6 adds "v1.2"<br><br>Wording changed: "The organization develops security requirements for the physical facility and supporting infrastructure."<br><br>"The organization identities systems, equipment, and respective operating environments that require limited physical access" | | We agree that the practice of protecting and monitoring at Level 2 is an appropriate step beyond the basic hygiene required at Level 1.<br><br>Agree with CMMC drafters in use of exact language of NIST control. Reference to other controls within the same Practice, such as the CERT RMM, however, introduce increased compliance risk. (See comment above for AC, C002, P1007) |

| CMMC Draft 7 | CMMC Draft V7 Capability | Controls Cited (and comparison to Draft V4 and V7) | Compare to CMMC Draft 4 | Controls in L2 V4 deleted /moved in V7 | Comments |
|---|---|---|---|---|---|
| | | | "The organization protects and monitors the physical facility and support infrastructure based on established requirements." | | |
| DR, C029, P1137 | "Regularly perform and test data back-ups." | AU ACSC Essential Eight (new)<br>ISO/IEC 27001 A.12.3.1<br>NIST CSF v1.1 PR.IP-4 (same)<br>CIS Controls v7.1 10.1 and 10.3 (same) | Was RE, C1 L2-1<br>And<br>RE, C1, L2-2<br><br>Wording changed: "Automated information back-ups are regularly performed."<br><br>"Data on back-up media is routinely tested."<br><br>But substance appears the same | | References to multiple controls within the same Practice introduce increased compliance risk. (See comment above for AC, C002, P1007) |
| DR, C029, P1138 | "Protect the confidentiality of backup Federal Contract Information at storage locations." | 3.8.9<br>CERT RMM v1.2 MON:SG2.SP4 | new | | We note that NIST SP 800-171 3.8.9 is a security requirement that applies to "CUI" and not "FCI." We suggest using the exact language of the NIST security requirement in order to maintain |

| CMMC Draft 7 | CMMC Draft V7 Capability | Controls Cited (and comparison to Draft V4 and V7) | Compare to CMMC Draft 4 | Controls in L2 V4 deleted /moved in V7 | Comments |
|---|---|---|---|---|---|
| | | | | | consistency with DFARS requirements.<br><br>Reference to other controls within the same Practice, such as the CERT RMM, however, introduce increased compliance risk. (See comment above for AC, C002, P1007) |
| RM, C031, P1141 | "Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of | 3.11.1 (same)<br>CERT RMM v1.2 RISK:SG4 (same) | Was RM, C4, L2-1<br>Reference to RMM in 0.6 adds "v1.2"<br><br>Wording changed:<br>"The organization has a process for periodically analyzing risks." | | We note that NIST SP 800-171 3.11.1 is a security requirement that applies to "CUI" and not "FCI." We suggest using the exact language of the NIST security requirement in order to maintain consistency with DFARS requirements.<br><br>Reference to other controls within the same Practice, such as the CERT RMM, however, introduce increased compliance risk. (See comment above for AC, C002, P1007) |

| CMMC Draft 7 | CMMC Draft V7 Capability | Controls Cited (and comparison to Draft V4 and V7) | Compare to CMMC Draft 4 | Controls in L2 V4 deleted /moved in V7 | Comments |
|---|---|---|---|---|---|
| | Federal Contract information." | | | | |
| RM, C031, P1142 | "Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified." | 3.11.2 (same) | Was RM, C3, L2-2<br><br>Wording changed: "Vulnerability scans are performed to identify new vulnerabilities."<br><br>But substance appears the same | | Agree with CMMC drafters in use of exact language of NIST control. |
| RM, C031, P1143 | "Remediate vulnerabilities in accordance with risk assessments." | 3.11.3 (new)<br>CERT RMM v1.2 VAR:SG3.SP1 (same) | Was RM, C5, L2-3<br>And<br>RM, C5, L2-4<br><br>Wording changed: "Risk mitigation plans are implemented."<br><br>"Actions are taken to manage exposure to vulnerabilities." | | Agree with CMMC drafters in use of exact language of NIST control.<br><br>Reference to other controls within the same Practice, such as the CERT RMM, however, introduce increased compliance risk. (See comment above for AC, C002, P1007) |
| SAS, C034, P1157 | "Develop, document, and periodically | 3.12.4 (same) | Was SAS, C1, L2-1<br>And<br>SAS, C2, L2-2 | | Agree with CMMC drafters in use of exact language of NIST control. |

| CMMC Draft 7 | CMMC Draft V7 Capability | Controls Cited (and comparison to Draft V4 and V7) | Compare to CMMC Draft 4 | Controls in L2 V4 deleted /moved in V7 | Comments |
|---|---|---|---|---|---|
| | update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems." | | Wording changed: "Develop and document a system security plan that defines security requirements for the organization to include (system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems)"<br><br>"Periodically update system security plans as security requirements change." | | |
| SAS, C035, P1158 | "Periodically assess the security controls in organizational systems to determine if the | 3.12.1 (same) | Was SAS, C2, L2-1 | | |

| CMMC Draft 7 | CMMC Draft V7 Capability | Controls Cited (and comparison to Draft V4 and V7) | Compare to CMMC Draft 4 | Controls in L2 V4 deleted /moved in V7 | Comments |
|---|---|---|---|---|---|
| | controls are effective in their application." | | | | |
| SAS, C035, P1159 | "Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems." | 3.1.2.2 (same) | Was SAS, C5, L2-2 | | |
| SCP, C039, P177 | "Employ FIPS-validated cryptography when used to protect the confidentiality of Federal Contract Information." | 3.13.11 Moved to Level 3 in Version 0.7 | Was SCP, C1, L2-4<br><br>Wording changed: "the organization establishes FIPS-validated cryptography keys for cryptography implemented organizational systems." | | |
| SCP, C039, P178 | "Prohibit remote activation of collaborative computing | 3.13.12 (same) | Was SCP, C1, L2-8<br><br>Wording changed: "The organization | | Agree with CMMC drafters in use of exact language of NIST control. |

| CMMC Draft 7 | CMMC Draft V7 Capability | Controls Cited (and comparison to Draft V4 and V7) | Compare to CMMC Draft 4 | Controls in L2 V4 deleted /moved in V7 | Comments |
|---|---|---|---|---|---|
| | devices and provide indication of devices in use to users present at the device." | | prohibits remote activation of collaborative computing devices and provides indication of devices in use to users present at the device."<br><br>But substance appears the same. | | |
| SCP, C039, P179 | "Use encrypted sessions for the management of network devices." | CIS Controls v7.1 11.5 (same) | Was SCP, C1, L2-9<br><br>Wording changed: "The organization uses encrypted sessions for the management of network devices." | | |
| SII, C041, P1214 | "Monitor system security alerts and advisories and take action in response." | 3.14.3 (same)<br>NIST CSF v1.1 RS.AN-5 (new) | Was SII, C2, L2-1 | | Agree with CMMC drafters in use of exact language of NIST control.<br><br>Reference to other controls within the same Practice, however, introduce increased compliance risk. (See comment above for AC, C002, P1007) |

| CMMC Draft 7 | CMMC Draft V7 Capability | Controls Cited (and comparison to Draft V4 and V7) | Compare to CMMC Draft 4 | Controls in L2 V4 deleted /moved in V7 | Comments |
|---|---|---|---|---|---|
| SII, C043, P1216 | ”Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.” | 3.14.6 (same) | Was SII, C4, L2-1<br><br>Wording changed: “Operational environments are monitored for anomalous behavior that may indicate a cybersecurity event.” | | Agree with CMMC drafters in use of exact language of NIST control. |
| SII, C043, P1217 | Identify unauthorized use of organizational systems. | 3.14.7 (same) | Was SII, C4, L2-2<br><br>Wording Changed: “Organizational systems are monitored for unauthorized use.”<br><br>But substance appears the same | | Agree with CMMC drafters in use of exact language of NIST control. |