NDIA

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

September 25, 2019

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

Re: Draft CMMC v0.4

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 the comment matrix and this letter have come from this diverse membership and represent a broad range of perspectives across the defense industrial base.

Thank you for sharing the first draft (version 0.4) of CMMC. NDIA welcomes DOD's robust engagement with industry on this new model for protecting Controlled Unclassified Information in the Defense Industrial Base. CMMC has the potential to be a groundbreaking improvement in defense acquisition and cybersecurity protection. To achieve its crucial goals, however, it must be developed and implemented efficiently and effectively. 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 and through our submission of the CMMC matrix.

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 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 implementation of CMMC.

1) Implementation and Timeline of the Draft CMMC Model

   a. **Comment:** The draft CMMC model released focuses on potential technical controls and processes and thus lacks crucial details on how DOD would implement CMMC in practice, such as how DOD will define the "critical" DOD programs and technologies for which contractors would need a Level 4 or 5 certification or when it would require a Level 1 versus Level 2 certification, and the assessment guidance that third party certifiers will use when assessing and certifying contractors under the CMMC model. Related areas that need clarification are as follows:

i. Many of the CMMC controls are predicated on the existence of Controlled Unclassified Information (CUI). Thus, the ability for both the Government and contractors at all tiers to be able readily to identify CUI is foundational. DOD, however, has not yet issued updated CUI guidance as contemplated by the 2016 National Archives and Records Administration rule. This situation has delayed or otherwise impeded the training of government personnel and affected the ability of contractors to identify whether they have CUI and to develop and implement the necessary underlying policies and processes. Contractor inquiries to Government programs regarding Covered Defense Information (CDI) and CUI continue to go unanswered. We believe this Government guidance and associated training of both Government and contractors is a prerequisite to effectively implementing many of the CMMC controls.

ii. The draft CMMC documentation uses the term CUI rather than the term CDI, the term DOD uses in DFARS 252.204-7012. What does DOD consider the distinction between the two terms to be? Why has DOD changed its terminology and how does it change a contractor's obligations? For example, in inserting CMMC requirements Level 3 or above in an RFI and solicitation, does DOD intend to impose requirements with respect to all contractor networks with CUI, including potentially legacy data, or only contractor networks used to protect CDI on that program?

iii. Given that DOD has identified Level 3 as the level applying the full complement of security controls contained in NIST SP 800-171 plus numerous additional requirements, but DOD also has identified Level 1 as providing "basic" cybersecurity, the draft has created some confusion regarding how these CMMC levels will be used, and what will be considered "basic" for purposes of contracting with the DOD. NDIA proposes that DoD clarify these points.

iv. The draft CMMC references the NIST SP 800-171 requirement to "implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems" in the SAS domain (Capability 2, Practice L2-2). 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.

v. DOD has indicated that Level 3 will be the minimum level required if a company has CUI on its internal business systems. When will Level 2 be required versus Level 1? Why is Level 1 not limited to the basic safeguarding requirements set forth in the FAR? Given limited Government and company resources, these resources should be focused on protecting CUI, particularly on defending against Advanced Persistent Threats (APT). CMMC may result in the potential exclusion of hundreds of contractors that cannot achieve cybersecurity beyond FAR 52.204-21 (mapped to 17 NIST SP 800-171 security requirements and controls) despite not handling CUI or CDI. What authority will DOD rely upon to exclude these contractors from competing for non-CUI related contracts? For example, certain exclusions can be made in covered procurement actions only after determinations are made and notice given. See 41 U.S.C. § 4713. Keeping Level 1 at the previously envisioned 17 NIST SP 800-171 security requirements would avoid many potentially unnecessary exclusions (but the issue would remain with respect to Level 2).

vi. The draft CMMC v0.4 provides that Level 3, the basic set of controls for a contract that would include government CUI, to include the NIST SP 800-171 security controls mandated in DFARS 252.204-7012. However, the draft CMMC includes other requirements beyond the NIST SP 800-171 controls, e.g., controls found in "CIS;" "RMM ADM"; "DIB"; "RMM MON"; "RMM OTA"; "RMM EF; "RMM IMC"; "ISO 27001." These are not well explained in the CMMC. Moreover, since the DFARS 252.204-7012 includes reference to only the NIST SP 800-171 and industry is still trying to adapt and conform to that standard, NDIA submits that the inclusion of such additional standards is likely to increase confusion regarding current requirements, and to result in further implementation delays and increased costs among contractors. It may even result in exodus of small, mid-size and commercial contractors from the market since these controls are more and greater and the time and ability of contractors to establish full compliance by Fall 2020 would be problematic. NDIA proposes that additional requirements beyond NIST SP 800-171 for Level 3 be held off, or moved to a procurement-specific requirement where such additional requirements are deemed necessary, in order to facilitate contractor efforts to achieve compliance and certification at Level 3 by the Fall 2020.

vii. How will OSD ensure that a minimum of a CMMC Level 3 will not 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.)?

viii. How, when, and by whom will CMMC levels be determined for a multi-tiered supply chain working on separate, discrete aspects of a program? Will the Government determine in the RFP which CMMC levels apply to the prime contractor's supply chain? Will the prime/high tier contractor have an opportunity to request approval to flow down less than the CMMC level that is 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?

ix. Please clarify whether CMMC would apply to Government Furnished Equipment (GFE) or classified systems?

x. Can DOD confirm that only DOD prime contractors and subcontractors on a DOD contract will 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?

xi. If, as the DOD 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? It will be important not to replace the self-attestation system with a check-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?

xii. 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 restricted from competing for or participating in Level 4 or 5 contracts for critical programs?

xiii. Will certification levels be public? How will companies know what CMMC level other companies (including their subcontractors) have obtained?

xiv. In light of the fact that DOD is adding many new controls from various different sources that go above and beyond DFARS 252.204-7012, has DOD done any analysis on the incremental costs that defense contractors are likely to incur at each level of CMMC to meet these new controls? Some of these costs will be passed through to the Government, but commercial companies in particular will have to bear these costs entirely on their own. Also, how will costs for Levels 4 and 5 be reimbursed if incurred by contractors only for program specific networks if the contractor must implement the CMMC requirements prior to contract award to be eligible to participate in the contract?

xv. Given the number of new controls that are now being considered, is DOD considering how long it will take companies to plan, budget for and actually implement such concerns? One key lesson learned from the issuance of the 2015 version of DFARS 252.204-7012 as an interim rule was that companies cannot securely implement new controls without adequate planning, schedule and funding.

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

xvii. If there are no suppliers for particular parts, equipment or services in the early implementation of CMMC 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?

xviii. 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?

xix. 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?

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

xxi. Who will be the third-party assessors and when will they begin conducting assessments? What priority will be given to which companies are assessed 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?

xxii. 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 be within the scope of the third-party assessment and certification?

xxiii. There is a concern that the contracting officer, program manager or representative will not necessarily have a way, or tool, to determine the level of assignment to a RFP and would then, to be safe, designate Level 3 as a default. Will there be some sort of matrix for the government representative to use to assist in the assigning the appropriate level?

Recommendation: We recommend that OSD provide its draft assessment guidance and a detailed draft implementation plan and provide industry the opportunity to comment on both drafts before they are finalized.

b. **Comment**: The certification timeline identified in the OSD plan notes that the CMMC will appear in RFIs in June 2020 and RFPs in September 2020, and appears to assume that all companies who want to do business with DOD must be certified by late 2020, which is not realistic. Given that the CMMC model is not scheduled to be released until January 2020, it seems extremely ambitious to assume that every DIB prime and all of their sub-tiers of suppliers can and will be certified by late 2020, raising the question of how contractors will be able to meet contract requirements for CMMC certifications.

Recommendation: We recommend using a more realistic approach to deployment, included phased models that take into account the long lead time that will likely be needed for certify all DIB companies as well as the time it will take for companies to implement any new requirements prior to seeking certification. The CMMC should incorporate a phased approach for certification in which a contractor could compete for a contract/subcontract, such as one identified as a Level 4 or 5, as long as it had a realistic plan and timetable for achieving the level.

c. **Comment**: Although an accreditation program has not been published and an accreditation methodology has not been tested, the DOD’s notional timeline anticipates the appearance of CMMC in RFPs by late 2020. There is a concern that there will not be enough certifiers to handle the volume of contractors that will need certification and that the certification process will not have adequate quality control to ensure a fair process across the entire DIB spectrum.

Recommendation: Allow time for the accreditation program to be developed with an adequate number of trained certifiers. A timeline for RFPs can be better developed once the certification process is finalized and understood, and certifier numbers are known.

2) Content of the Security Controls in the Draft CMMC Model

a. **Comment**: There are a very large number of prescriptive “practice” controls, with over 300 controls for each of Levels 4 and 5 alone (many of which do not cite standards that have been approved or proposed by any formal standards body, such as those that cite “DIB” as the source). The sheer number alone (in addition to the vagueness and cost imposed by many of these controls) will make compliance and assessment unduly difficult and time-consuming.

Recommendation: We appreciate that DOD appears to understand that the requirements need to be streamlined. We agree and recommend reducing the number of controls, removing the ones that do not move the needle on security, and adding clarity to those that remain. The quickest and easiest way to accomplish this would be to base the Level 1 through Level 3 maturity assessment on the existing NIST SP 800-171 controls, and to base the Level 4 and 5 maturity assessment on these controls plus some NIST SP 800-171B controls. At a minimum, any controls not tied to an existing published standard should be removed at this time. To the extent risks warrant, additional controls/processes could be phased in over time when existing, auditable standards are available.

b. **Comment**: The draft CMMC makes no direct reference to how it would be applied in a cloud environment, beyond a single brief reference in a Level 5 "practice" control in the "System and Informational Integrity" domain for organizations to allow access only to "authorized" cloud storage or email providers. If a company has its data in the cloud, will it be exempt from the CMMC certification requirement? In light of the fact that sensitive DOD data has been and will continue to be stored in the cloud, there should be additional discussion of cloud security and the issue of whether cloud providers will be required to obtain CMMC certifications.

Recommendation: 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).

c. **Comment**: The draft CMMC attempts to map only a fraction of the controls to international standards. The very limited reference to international standards will likely make it more difficult to scale the CMMC model across the many international suppliers in DOD's supply chain. The contracting community already has encountered difficulty in getting international suppliers to accept NIST SP 800-171 standards, even though NIST is a widely recognized and influential government standards body.

Recommendation: Map as many of the CMMC controls to international standards as possible, similar to what was done in the NIST Cybersecurity Framework.

d. **Comment**: DOD should reconsider placing NIST SP 800-171B requirements into Level 3. Industry has geared its efforts over the past few years toward FAR 52.204-21, DFARS 252.204-7012 and the version of NIST SP 800-171 referenced in the DFARS clause. Aside from one reference, all of the other proposed inclusions of NIST SP 800-171B content are reserved for CMMC Levels 4 and 5. Based on the substantial – and ongoing – industry effort involved in achieving compliance with current FAR, DFARS and NIST standards, our observation is that it would be advisable to select one level, or a "tier" within a level, to correspond with those existing requirements. Additional requirements, including those resulting from NIST SP 800-171B, should be reserved for higher levels.

Recommendation: Select one of the levels – or at a minimum, a "tier" within a level – to correspond with existing FAR 52.204-21, DFARS 252.204-7012 and NIST SP 800-171 requirements. To the extent additional requirements are desired, they should be placed in higher tiers. DOD should not incorporate elements of NIST SP 800-171B into Level 3.

3) Details on the Assessment of Security Controls in the Draft CMMC Model

a. **Comment**: Many of the CMMC Level 1 and Level 2 controls require various types of protection of CUI. However, DOD has indicated that all contractors who do business with the DOD will need to be at least CMMC Level 1 certified, even if the contractor is not subject to the requirements of the DFARS Cybersecurity Clause (252.204-7012) to protect CDI (i.e., the contractor is not receiving, using, or developing CDI). Thus, it is unclear how DOD expects contractors who have no contact with CDI/CUI or DFARS obligations to protect CDI/CUI to be able to protect (or even identify) CDI/CUI.

   Recommendation: Remove references to CUI in the CMMC Level 1 and 2 controls, or in the alternative, clearly explain how CMMC Level 1 or 2 certified contractors are to be expected to identify and protect CUI and under what contractual or legal authority.

b. **Comment**: It is unclear how the "practices" for each CMMC maturity level are supposed to interact with the "processes" for that level, particularly since the four "processes" identified in the Maturity Level Capability for each Domain are similar in nature to practices. For example, it is unclear what maturity level a contractor would be deemed to have it if has Level 3 "practices" but Level 4 "processes," or if it has Level 4 "practices" but Level 3 "processes."

   Recommendation: Restate the "Maturity Level Capability" category as a "Capability" and recharacterize 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 indistinguishable from practices.

c. **Comment**: In general, the "process" maturity levels have controls that are vaguer than the "practices" identified in the domains. For example, the Level 5 "process" maturity levels require "standardized documentation." It is unclear what exactly is expected of contractors to demonstrate they have "standardized documentation."

   Recommendation: If DOD intends to maintain the distinction between "processes" and "practices" despite the recommendation in #2 above, it should provide greater clarity on the meaning of the "process" maturity levels. For example, the draft maturity Level 5 controls that require "standardized documentation" for domain controls should be changed to require “standard processes for documenting” the domain controls.

Given the shortness of time to respond to the CMMC ver. 0.4 draft, NDIA requests permission to supplement this set of comments with additional points to be identified by the NDIA.

Further, DoD has been transparent in seeking industry comment on CMMC Rev. 0.4, released on Sept 4th, with comments due 21 days later on Sept. 25th. As stated in the Overview Briefing, DoD intends that CMMC be a unified cybersecurity standard for all DoD acquisitions. A 21-day period for comment during the last month of the fiscal year is an insufficient timeframe to adequately review a rule that will impact all DoD acquisitions. NDIA respectfully requests a 60-day comment period for submission of public comments on CMMC Rev 0.6, which we understand will be released in November. Extending the next comment period will allow us to engage in greater communications with a greater number of stakeholders, and thus we will be able to provide more extensive comments on this proposal.

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

	Point of Contact
First Name	Corbin
Last Name	Evans
Organization	NDIA
Position	Director of Regulatory Policy
Email address	Cevans@NDIA.org
Phone #	703-247-2598

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
1	NDIA	C	7	AM	C1 Identify Assets	L1-1 • NIST SP 800-171 3.4.1 • RMM ADM:SG1.SP1	L1	This is a comprehensive requirement per the citations, which will be administratively intensive and will require regular updates to categorize "hardware, software, firmware, and documentation." Small businesses in particular may find the requirement prohibitive and/or onerous.	Don't include as part of Level 1
2	NDIA	C	10	AA	C4 Auditing is performed	L1-1 • NIST SP 800-171 3.3.1	L1	This is a comprehensive requirement per the citations, which will be administratively intensive and will require extensive audit logs and records of regular "monitoring, analysis, investigation, and reporting" of activities. Small businesses in particular may find the requirement prohibitive and/or onerous.	Don't include as part of Level 1
3	NDIA	C	10	AA	C4	L1-1	L1	Per the comment above, this is a comprehensive monitoring requirement that is	Don't include as part of Level 1

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
					Auditing is performed	• RMM MON:SG2.SP3		administratively intensive. The citation elaborates detailed monitoring that would add to a small business' workforce requirements and likely be too onerous. The practice mentions "CUI" but at Level 1 it will likely be imposed on contractors that do not handle CUI.	
4	NDIA	C, S	11	AA	C7 Audit logs are reviewed	L1-1 • NIST SP 800-171 3.3.5	L1	The citation's use of the term "reporting" triggers questions related to identifying what to report, how to report, to whom to report, and where to report. It also raises concerns about attribution. This is particularly important where DFARS 252.204-7012 is not applicable to a contract.	If the reporting requirement is meant to be only internal, then provide more detailed information about the process. If the reporting requirement is to external sources, then don't include as part of Level 1. The requirement raises significant issues and there must be better detail – in such cases, suggest only reporting well defined incidents and provide protection to the contractor concerning attribution and privacy.
5	NDIA	C	16	CM	C3 Configuration baselines are established	L1-1 • RMM KIM:SG5.SP2	L1	This requirement is similar to NIST 800-171 3.4.1. The same comments above apply. The requirement will be too onerous for small businesses to comply.	Don't include as part of Level 1
6	NDIA	C, S	25	IR	C1 Detect and report events	L1-1 • RMM IMC:SG2.SP1	L1	Is an "event" the same as a "cyber incident" as defined in DFARS 252.204-7012? Reporting per the CERT RMM Incident Management and Control publication does not require reporting to the federal government. Is that an accurate interpretation of this rule or will it require reporting to DOD?	Don't include as part of Level 1. If it must be included, we suggest clarification. If reporting is external, then suggest including comprehensive instruction on reporting, as with 7012. There should be established non-attribution and privacy as to the event reported.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
									Additionally, if reporting to DOD is not contemplated, then the L1-1 language should be changed as follows: - Events are detected and investigated, at least in an ad hoc manner.
7	NDIA	C, S	25	IR	C3 Declare and report incidents	L1-1 • RMM IMC:SG3.SP1 –	L1	This requirement is so broad that different contractors can vary significantly as to what an "incident" is and criteria used to define the incident. This is particularly true where DFARS 252.204-7012 is not applicable due to a lack of CUI/CDI. It could lead to unfair results in a competitive scenario. More instruction is needed from DOD.	Don't include as part of Level 1 If it must be included, we suggest a comprehensive instruction on reporting. There should be established non-attribution and privacy as to the incident reported.
8	NDIA	C, S	25	IR	C5 Develop and implement a response to a declared incident	L1-1 • RMM IMC:SG4.SP1	L1	While the internal escalation of incidents is appropriate, the external escalation of incidents must be better defined, particularly where CUI is not a part of a contact. Escalation to other contractors (as the CERT RMM citation suggests) could lead to unfair consequences affecting a contractor's reputation and perceived performance. Escalating to external sources could adversely affect a small business. Escalation to the DOD would require a level of confidentiality, non-attribution and process that is not outlined in the CERT RMM citation. Better guidance from DOD is required.	Don't include in Level 1. Per the comment, better guidance is required even at higher levels.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
9	NDIA	C	34	PS	C1 Screen Personnel	L1-1 • RMM HRM:SG2.SP1	L1	The requirement is sensible to the extent it applies to employees who handle CUI; however, verification criteria should be better defined.	Verification criteria should be better defined. If this requirement is meant to apply to all employees, regardless of whether they will handle CUI, then suggest the requirement not be implemented at Level 1 due to the administrative burden of implementing a comprehensive screening, particularly for small businesses.
10	NDIA	C, S	45	SAS	C4 Define controls	L1-1 • RMM CTRL: SG2.SP1 –	L1	This is a broad category that should be better defined to apply for DOD purposes. The requirement places a heavy administrative burden on small businesses if the cited CERT RMM guidance is followed.	Don’t include as part of Level 1
11	NDIA	C	49	SA	C4 Communicate threat information to stakeholders	L1-1 • CSF: RS.CO-5	L1	Making this requirement mandatory in order to attain Level 1 certification defeats the purpose of information sharing being “voluntary.” A mandatory requirement is contrary to the executive orders that created the cybersecurity framework.	Suggest taking out this requirement for certification.
12	NDIA	C, A	10	AA	C2 Identify stakeholders	L2-1 The organizational and external entities that rely upon information collected from the audit and accountability	L2	Identifying stakeholders needs to be more specific and in what format. Is this needed for Level 2?	Re-word or take out.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
						process are identified • RMM MON:SG1:SP3			
13	NDIA	C, A	10	AA	C3 Define audit storage requirements	L2-1 The organization has a process to create and retain audit logs, ensuring that all events defined are included. • RMM MON:SG2.SP3	L2	Identifying stakeholders needs to be more specific and in what format. Is this needed for Level 2?	Re-word or take out.
14	NDIA	C, A	11	AA	C8 The information collected is distributed to the appropriate stakeholders	L2-1 The audit information collected is distributed to the appropriate stakeholders. • RMM MON:SG2.SP4	L2	Identifying stakeholders needs to be more specific and in what format. Is this needed for Level 2?	Re-word or take out.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
15	NDIA	C, S	25	IR	C1 Detect and report events	L2-1 The organization has a process for detecting and reporting events. • RMM IMC:SG2.SP1	L2	Is an "event" the same as a "cyber incident" as defined in DFARS 252.204-7012? Reporting per the CERT RMM Incident Management and Control publication does not require reporting to the federal government. Is that an accurate interpretation of this rule or will it require reporting to DOD?	If the requirement must be included at this level, we suggest clarification. If reporting is external, then suggest including comprehensive instruction on reporting, as with 7012. There should be established non-attribution and privacy as to the event reported. Additionally, if reporting to DOD is contemplated, then the L2-1 language should be changed as follows: - The organization has a process for detecting and reporting incidents
16	NDIA	C, S	25	IR	C2	L3-1 The criteria for declaring incidents is defined. • RMM IMC:SG3.SP1	L3	The criteria for declaring an incident when the information involves CUI is defined by DFARS 252.204-7012; for contracts that do not have CUI, there is no DOD instruction and no CERT RMM citation. Are contractors required to develop their own criteria or will the criteria be defined by DOD? Additionally, there currently are restrictions for reporting on international incidents. Will contractors be required to rely on international best business practices to declare an incident, or will DOD provide guidance?	We suggest that DOD provide an instruction on the criteria for declaring an incident in non-CUI related contracts, including both domestic and international incidents. The criteria could be tied to 7012.
17	NDIA	C, S	31	MP	C2	L3-1 The organization has a process for implementing	L3	Is DOD requiring contractors to implement cryptographic mechanisms to protect the confidentiality of <ins>all</ins> CUI digital data at rest? Is this required even if adequate security is established with physical protections (*e.g.*, a server within an access controlled and	Clarify whether the requirement addresses all existing CUI, including CUI on legacy systems with other means for protection of at rest data. Clarify whether the requirement applies only to CUI that

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
						cryptographic mechanisms to protect the confidentiality of CUI digital data at rest. • CIS 7.1: 14.8		physically protected data center in contrast with a solid state disk in a notebook computer)? Many contractors systems include legacy servers and it may be cost prohibitive to either retire or encrypt.	exists in contracts awarded after CMMC is implemented.
18	NDIA	C, S	39	RE	C2	L3-1 Develop an information security continuity plan that includes redundancy and availability requirements. • ISO 27001 A.17.1.1	L3	This requirement is not included in the initial NIST SP 800-171 controls. Shouldn't the requirements of NIST SP 800-171 be retained as the Level 3 controls, and any additional control for redundancy included in the specific solicitation where such a requirement would actually be needed. If redundancy is required, the term "continuity" needs to be further defined. Will a cloud service with separate backup be sufficient to meet continuity and redundancy requirements? Can other forms of redundancy be used? Would DOD provide examples? Does DOD expect contractors to develop a continuity plan in all cases of disaster? If so, will CMMC negate FAR clauses which recognize non-performance during circumstances beyond a contractor's control. E.g., FAR 52.249-8(c).	Delete this requirement and consider whether redundancy can be required where needed for a specific Level 3 solicitation. With regard to rules on redundancy, when and if included, better examples and definition should be provided, including whether and to what extent a defined secure cloud service, or other controls, may serve as a redundancy.
19	NDIA	C, S	39	RE	C2	L3-2 Ensure	L3	The ISO citation specifically mentions cloud providers for meeting redundancy	DOD should confirm whether cloud providers are adequate to meet this practice and, if so, the level of

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
						information processing facilities meet redundancy and availability requirements. • ISO 27001 A.17.2.1		requirements. On CUI-related contracts, DFARS 252.204-7012 specifies that at least a FEDRAMP Moderate equivalent cloud provider is necessary. However, it is unclear whether contracts that do not have CUI should also adhere to this requirement.	security that a cloud provider must meet if a DOD contract does not contain CUI.
20	NDIA	C, S	46	SAS	C6	L3-1 Employs human performed code reviews to identify areas of concern that require additional improvements. • NIST SP 800-171B: 3.11.6e partial assessment.	L3	Is the intent to incorporate this element of NIST SP 800-171B into Level 3? This appears to be the only instance where this occurs, with the nearly 40 other references to 171B appearing in relation to Levels 4 and 5. Further the SP reference cited deals more with supply chain risks as opposed to the topic cited in Capability C6, which addresses "in-house developed software."	DOD should not incorporate elements of NIST SP 800-171B into Level 3. A broader suggestion is that one of the proposed CMMC Levels (perhaps Level 3, or a "tier" within Level 3) should correspond with the controls toward which much of industry has been gearing its efforts over the past few years, namely DFARS 252.204-7012 and NIST SP 800-171. Additional requirements, including those resulting from NIST SP 800-171B, should be reserved for higher levels.
21	NDIA	C,S	49	SA	C3	L3-2 The organization has identified stakeholders to whom threat information	L3	Communication with external stakeholders, particularly for contracts that do not involve CUI, can present challenges. If DOD does not specifically define external stakeholders (e.g. entities within DOD, next tier contractors) communication plans may be different for each certified contractor. When contracts do	DOD should specify who stakeholders are in a federal contract for communicating threat information. DOD should also have in place strict non-attribution policies when such information is communicated.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
						must be communicated. • RMM COMM: SG1.SP1		involve CUI, is communication with stakeholders the same as reporting requirements under DFARS 252.204-7012?	
22	NDIA	C, S	49	SA	C4	L3-1	L3	The practice cites the NIST Cybersecurity Framework, which is a voluntary program per EO 13636. It does not rely upon mandatory reporting per DFARS 252.205-7012. Per the comment above, does the practice envision an ad hoc communication with stakeholders on an individual contract basis or a more delineated communication process?	This practice should be deleted, excepted in cases where CUI exists in a contract, which triggers the requirements under DFARS 252.204-7012. At the very least DOD should clarify who stakeholders are and timeliness requirements for communication.
23	NDIA	S	2	AC	C2	L4-1	L4	"Separation of duties" is already a requirement of L2-1.	Remove "separation of duties" from L4-1.
24	NDIA	S	2	AC	C2	L5-1	L5	The proposed practice of adapting the security posture "to the most restrictive viable settings is potentially unduly restrictive. In addition, it is unclear what proposed practice would qualify as "context-aware" and "security posture to the most restrictive viable settings." These are not well-known, defined, auditable terms.	Network, host, and software access control is conditional and proportional based on multiple factors such as location, time of day, device type and activities.
25	NDIA	S	3	AC	C3	L5-1	L5	The proposed practice of adapting the security posture “to the most restrictive viable settings” is potentially unduly restrictive. In addition, it is unclear what proposed practice would	Network, host, and software access control is conditional and proportional based on multiple

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
								qualify as "context-aware" and "security posture to the most restrictive viable settings." These are not well-known, defined, auditable terms.	factors such as location, time of day, device type and activities.
26	NDIA	S	3	AC	C3	L5-2	L5	The proposed practice states that "access to higher value assets, as defined by 800-171B, and data are restricted based on context-aware configurations. . . ." NIST has not defined the term "high value assets" in SP 800-171B. (See NDIA comments to NIST on draft SP 800-171B.) Furthermore, SP 800-171B does not use the term "high value assets" with respect to data. Until the terms "high value assets" and "high value data" are defined by NIST or DOD, this practice cannot be implemented or reasonably serve as an objective, auditable basis for assessment.	Delete proposed practice.
27	NDIA	S	4	AC	C5	L4-1	L4	The proposed practice would "enforce access control to data through automated tools." It is unclear what "enforce access control to data" means. It is also unclear what qualifies as an "automated tool." It is also unclear whether "automated" practices are reasonable or sensible for all environments.	Delete proposed practice.
28	NDIA	S	4	AC	C5	L4-2	L4	The proposed practice would require the organization to apply "need-to-know" and "fine-grained access control" for CUI data access. It is unclear what "fine-grained" access control means.	Limit CUI data access to "need-to-know."

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
29	NDIA	S	4	AC	C5	L5-2	L5	The proposed practice of “applying data obfuscation and deception to reduce the confidence [of] an unauthorized user” raises significant legal, ethical, and administrative issues. For example, would organizations be required to deceive their own shareholders, employees, customers, and/or regulators in order to successfully deceive an unauthorized user? If so, what safe harbors would exist for organizations that violate their legal and ethical obligations in order to implement this practice? Would organizations be able to claim the costs of obfuscation and deception, including deception of U.S. Government customers and regulators, as an “allowable cost” for government contract purposes? There could be considerable costs associated with maintaining duplicate sets of the same documents. There also is a risk that organizations may ultimately lose configuration control over obfuscated documents over time such that organizational users mistakenly believe that obfuscated designs or other documents are in fact legitimate, unintentionally leading to vulnerabilities in products delivered to the Government. In light of these and other legal and ethical issues, this proposed practice should be deleted from the CMMC Level 5 practices.	Delete proposed practice.
30	NDIA	S	4	AC	C5	L5-3	L5	The proposed practice envisions keeping CUI data cryptographically secured “at all times,” including “execution.” It is unclear how this practice would be accomplished where the CUI	Require that CUI data be encrypted at rest when feasible, but not cryptographically secured "at all times."

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
								data is maintained by a third-party cloud provider or a third party vendor such as an outside law firm. DOD also has not published guidance in furtherance of the NARA CUI program, leaving uncertainty on exactly what is CUI requiring protection, and what is not. It is also unclear how CUI data can be cryptographically secured in all stages of execution.	
31	NDIA	S	4	AC	C4	All	All	The phrase "from the internal network" unduly limits the applicability of the capability and should be deleted. The general structure of the capabilities across the various domains appears to mirror the high-level steps of a business process, following the general pattern of: "establish," "identify," "act/implement/manage," then "monitor." As this capability relates to identification, it would be more properly placed higher in the domain.	The capability should be restated as follows: "Identify access requirements for each class of data." The capability should be shifted upwards to follow behind C1. The resulting order of the capabilities (as currently numbered) would be C1, C4, C2, C3, C5.
32	NDIA	S	6	AC	MLC	ML4-1	L4	It is unclear why DOD views "inform high-level management" as a process rather than a practice. Assuming that "inform high-level management" is a process, it is too vague and general to serve as an objective, auditable basis for determining Level 5 maturity. "High-level management" is undefined, and there is no description of what types of information should be provided to such management. Furthermore, it is unclear why DOD chose this process as one of only two processes that	Restate MLC as a "Capability" rather than a "Maturity Level Capability," and make ML4-1 a practice within that Capability. Provide clearer definition of this practice.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
								determine Level 4 maturity in the Access Control Domain.	
33	NDIA	S	6	AC	MLC	ML4-2	L4	It is unclear why DOD views "Review Access Control activities for effectiveness" as a process rather than a practice. Assuming it is a process, it is unclear why DOD chose this process as one of only two processes that determine Level 4 maturity in the Access Control Domain.	Restate MLC as a Capability and make ML4-2 a practice within that Capability.
34	NDIA	S	6	AC	MLC	ML5-1	L5	It is unclear why DOD views “Standardize documentation for Access Control” as a process rather than a practice. Assuming it is a process, it is too vague and general to serve as an objective, auditable basis for determining Level 5 maturity. Furthermore, it is unclear why DOD chose this process as one of only two processes that determine Level 5 maturity in the Access Control Domain.	Restate MLC as a Capability and make ML5-1 a practice within that Capability. Provide clearer definition of this practice.
35	NDIA	S	6	AC	MLC	ML5-2	L5	It is unclear why DOD views “Share Access Control improvements across the organization” as a process rather than a practice. Assuming it is a process, it is unclear why DOD chose this process as one of only two processes that determine Level 5 maturity in the Access Control Domain.	Restate MLC as a Capability and make ML5-2 a practice within that Capability.
36	NDIA	S	7	AM	C1	L4-1	L4	The description of this practice is too general to serve as a reasonable basis for assessment of Level 4 maturity. The description gives contractors no guidance on how or the extent to which operational technology should be	Provide clarity as noted or delete the practice.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
								included in asset definition or in the scope of the cybersecurity program.	
37	NDIA	S	7	AM	C3	L4-1	L4	This practice lacks sufficient definition and clarity to be workable.	Provide clarity as noted or delete the practice.
38	NDIA	S	7	AM	C3	L4-2	L4	"Use DHCP logging to update assets." is a requirement on page 10.	Remove L4-1.
39	NDIA	S	8	AM	C4	L4-1	L4	The term “automated” in this practice is undefined. It is also unclear whether "automated" practices are reasonable or sensible for all environments.	Provide clarity as noted.
40	NDIA	S	8	AM	C4	L4-2	L4	This practice is limited to performing periodic spot checks to ensure that “semi-automated systems” managing assets are not missing any assets in the enterprise. Why is this practice limited to semi-automated systems?	Provide clarity as noted or delete the practice.
41	NDIA	S	9	AM	MLC	ML4-1	ML4	It is unclear why DOD views "inform high-level management" as a process rather than a practice. Assuming that "inform high-level management" is a process, it is too vague and general to serve as an objective, auditable basis for determining Level 4 maturity. "High-level management" is undefined, and there is no description of what types of information should be provided to such management. Furthermore, it is unclear why DOD chose this process as one of only two processes that determine Level 4 maturity in the Asset Management Domain.	Restate MLC as a "Capability" rather than a "Maturity Level Capability," and make ML4-1 a practice within that Capability. Provide clearer definition of this practice.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
42	NDIA	S	9	AM	MLC	ML4-2	ML4	It is unclear why DOD chose to treat "Review Asset Management activities for effectiveness" as a process rather than a practice. Assuming it is a process, it is unclear why DOD chose this process as one of only two processes that determine Level 4 maturity in the Asset Management Domain.	Restate MLC as a Capability and make ML4-2 a practice within that Capability.
43	NDIA	S	9	AM	MLC	ML5-1	ML5	It is unclear why DOD views “Standardize documentation for Asset Management” as a process rather than a practice. Assuming it is a process, it is too vague and general to serve as an objective, auditable basis for determining Level 5 maturity. It is also unclear why DOD chose this process as one of only two processes that determine Level 5 maturity in the Asset Management Domain.	Restate MLC as a Capability and make ML5-1 a practice within that Capability. Provide clearer definition of this practice.
44	NDIA	S	9	AM	MLC	ML5-2	ML5	It is unclear why DOD views “Share Asset Management improvements across the organization” as a process rather than a practice. Assuming it is a process, it is unclear why DOD chose this process as one of only two processes that determine Level 5 maturity in the Asset Management Domain.	Restate MLC as a Capability and make ML5-2 a practice within that Capability.
45	NDIA	S	10	AA	C4	All	All	This capability is stated in the passive voice.	The capability should be restated as follows: “Perform audit.”
46	NDIA	S	10	AA	C4	All		The reference to "DHCP logging" is too general. Logging requirements should be specified.	Specify log and network packet retention requirements - e.g. 30 days, 90 days, 365 days

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
47	NDIA	S	10	AA	C5	All	All	The identification of audit information in this capability is redundant, as it is already addressed by C1. The capability is also stated in the passive voice.	The capability should be restated as follows: "Protect audit information."
48	NDIA	S	10-11	AA	C2 / C8	All	All	Capabilities C2 and C8 can be merged to simplify the model. Each capability has only one practice, both of which are assigned to Level 2, and are not distinct enough to warrant separate treatment. Identifying stakeholders is also a necessary part of distributing information to such stakeholders.	Merge capabilities C2 and C8 with the resulting capability stated as follows: "Distribute audit information to appropriate stakeholders."
49	NDIA	S	11	AA	C6	L4-1	L4	The term "semi-automated" is ambiguous, particularly as applied to audit log analysis. In addition, there is no measurable or auditable distinction between "review and manage" in L2-1 and "oversee and guide" in L4-1.	Remove L4-1.
50	NDIA	S	11	AA	C6	L5-1	L5	The term "fully automated audit log analysis" is unclear, particularly in light of the reference to "semi-automated" audit log analysis in L4-1. It is also unclear why overseeing and guiding a semi-automated audit log analysis should be a defining practice for Level 4, while validating the findings of a fully automated audit log analysis should be a defining practice for Level 5.	Provide clarity as noted or delete the practice.
51	NDIA	S	11	AA	C6 / C7	All	All	Capabilities C6 and C7 can be merged to simplify the model. Assigning staff to review and manage audit logs is an inherent part of reviewing audit logs.	Merge capabilities C6 and C7 with the resulting capability stated as follows: "Review audit logs."

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
52	NDIA	S	12	AA	MLC	ML4-1	L4	It is unclear why DOD views "inform high-level management" as a process rather than a practice. Assuming that "inform high-level management" is a process, it is too vague and general to serve as an objective, auditable basis for determining Level 5 maturity. It is also unclear why DOD chose this process as one of only two processes that determine Level 4 maturity in the Audit and Accountability Domain.	Restate MLC as a "Capability" rather than a "Maturity Level Capability," and make ML4-1 a practice within that Capability. Provide clearer definition of this practice.
53	NDIA	S	12	AA	MLC	ML4-2	L4	It is unclear why DOD chose to treat "Review Audit and Accountability activities for effectiveness" as a process rather than a practice. Assuming it is a process, it is unclear why DOD chose this process as one of only two processes that determine Level 4 maturity in the Audit and Accountability Domain.	Restate MLC as a Capability and make ML4-2 a practice within that Capability.
54	NDIA	S	12	AA	MLC	ML5-1	L5	It is unclear why DOD views “Standardize documentation for Audit and Accountability” as a process rather than a practice. Assuming it is a process, it is too vague and general to serve as an objective, auditable basis for determining Level 5 maturity. It is also unclear why DOD chose this process as one of only two processes that determine Level 5 maturity in the Audit and Accountability Domain.	Restate MLC as a Capability and make ML5-1 a practice within that Capability. Provide clearer definition of this practice.
55	NDIA	S	12	AA	MLC	ML5-2	L5	It is unclear why DOD views “Share Audit and Accountability improvements across the organization” as a process rather than a practice. Assuming it is a process, it is unclear why DOD chose this process as one of only	Restate MLC as a Capability and make ML5-2 a practice within that Capability.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
								two processes that determine Level 5 maturity in the Audit and Accountability Domain.	
56	NDIA	S	13	AT	C1	All	All	This capability is stated in the passive voice.	The capability should be restated as follows: “Identify security awareness needs.”
57	NDIA	S	13	AT	C2	All	All	This capability is stated in the passive voice.	The capability should be restated as follows: “Conduct security awareness activities.”
58	NDIA	S	13	AT	C3	All	All	This capability is stated in the passive voice. “Training capabilities” may be better expressed as “training needs” or “training requirements” for consistency with the identified practices as well as the phrasing of C1 in this domain.	The capability should be restated as follows: “Identify training needs for information security-related duties and responsibilities.”
59	NDIA	S	13	AT	C3	L4-1	L4	This practice would require the organization to train "defensive cyber operations personal" to have "full enterprise cyber understanding" in order to reduce the negative impact of their defensive actions." The key terms "defensive cyber operations personnel" and "full enterprise cyber understanding" are undefined in the practice and the referenced standards, which makes it difficult to implement this practice or use it to assess Level 4 maturity.	Provide clarity as noted.
60	NDIA	S	14	AT	C4	All	All	This capability is stated in the passive voice. The phrasing should be consistent with C2 in this domain.	The capability should be restated as follows: “Conduct training activities for those with information security-related duties and responsibilities.”
61	NDIA	S	14	AT	C4	L4-2	L4	The term "cross-training" in this practice is vague and general, which will complicate	Provide clarity as noted or delete the practice.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
								implementation of this practice and its use in assessing Level 4 maturity.	
62	NDIA	S	15	AT	MLC	ML4-1	L4	It is unclear why DOD views "inform high-level management" as a process rather than a practice. Assuming that "inform high-level management" is a process, it is too vague and general to serve as an objective, auditable basis for determining Level 4 maturity. "High-level management" is undefined, and there is no description of what types of information should be provided to such management. Furthermore, it is unclear why DOD chose this process as one of only two processes that determine Level 4 maturity in the Awareness and Training Domain.	Restate MLC as a "Capability" rather than a "Maturity Level Capability," and make ML4-1 a practice within that Capability. Provide clearer definition of this practice.
63	NDIA	S	15	AT	MLC	ML4-2	L4	It is unclear why DOD views "Review Awareness and Training activities for effectiveness" as a process rather than a practice. Assuming it is a process, it is unclear why DOD chose this process as one of only two processes that determine Level 4 maturity in the Awareness and Training Domain.	Restate MLC as a Capability and make ML4-2 a practice within that Capability.
64	NDIA	S	15	AT	MLC	ML5-1	L5	It is unclear why DOD views "Standardize document for Awareness and Training" as a process rather than a practice. Assuming it is a process, it is too vague and general to serve as an objective, auditable basis for determining Level 5 maturity. It is also unclear why DOD chose this process as one of only two processes	Restate MLC as a Capability and make ML5-1 a practice within that Capability. Provide clearer definition of this practice.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
								for determining Level 5 maturity in the Awareness and Training Domain.	
65	NDIA	S	15	AT	MLC	ML5-2	L5	It is unclear why DOD views "Share Awareness and Training improvements across the organization" as a process rather than a practice. Assuming it is a process, it is unclear why DOD chose it as one of only two processes for determining Level 5 maturity in the Awareness and Training Domain.	Restate MLC as a Capability and make ML5-2 a practice within that Capability.
66	NDIA	S	16	CM	C3	All	All	This capability is stated in the passive voice.	The capability should be restated as follows: “Establish configuration baselines.”
67	NDIA	S	16-17	CM	C1 / C4	All	All	This capability does not describe the associated practices, and it duplicates C5 in this domain. C4 could therefore be grouped with C1 in this domain to simplify the model. Such a consolidation would be consistent with the NIST approach to the practices in C1 and C4.	Merge capabilities C1 and C4. The resulting capability should be stated as follows: “Establish and analyze change management requirements.”
68	NDIA	S	17	CM	C5	All	All	This capability is stated in the passive voice.	The capability should be restated as follows: “Perform configuration management.”
69	NDIA	S	17	CM	C5	L4-1	L4	There is no definition of the term "automated mechanisms" in either the description of this practice or in the reference NIST standard. (SP 800-171b 3.4.2e.) This practice will therefore be difficult to implement and to use as an objective, auditable basis for assessing Level 4 maturity. It is also unclear whether "automated" practices are reasonable or sensible for all environments.	Provide clarity as noted or delete the practice.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
70	NDIA	S	17	CM	C5	L4-3	L4	The term "roots of trust" is not defined in the proposed practice or in the referenced NIST standard (SP 800-181B 3.14e.) Absent a clear and practical definition of "roots of trust," this practice will be difficult to implement or to use as an objective, auditable basis for assessing Level 4 maturity.	Provide clarity as noted or delete the practice.
71	NDIA	S	18	CM	MLC	ML4-1	L4	It is unclear why DOD views "inform high-level management" as a process rather than a practice. Assuming that "inform high-level management" is a process, it is too vague and general to serve as an objective, auditable basis for determining Level 4 maturity. "High-level management" is undefined, and there is no description of what types of information should be provided to such management. Furthermore, it is unclear why DOD chose "inform high-level management" as one of only two processes that determine Level 4 maturity in the Configuration Management Domain.	Restate MLC as a "Capability" rather than a "Maturity Level Capability," and make ML4-1 a practice within that Capability. Provide clearer definition of this practice.
72	NDIA	S	18	CM	MLC	ML4-2	L4	It is unclear why DOD chose to treat "Review Configuration Management activities for effectiveness" as a process rather than a practice. Assuming it is a process, it is unclear why DOD chose this process as one of only two processes that determine Level 4 maturity in the Configuration Management Domain.	Restate MLC as a Capability and make ML4-2 a practice within that Capability.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
73	NDIA	S	18	CM	MLC	ML5-1	L5	It is unclear why DOD views "Standardize documentation for Configuration Management " as a process rather than a practice. Assuming it is a process, it is too vague and general to serve as an objective, auditable basis for determining Level 5 maturity. Furthermore, it is unclear why DOD chose this process as one of only two processes that determine Level 5 maturity in the Configuration Management Domain.	Restate MLC as a Capability and make ML5-1 a practice within that Capability. Provide clearer definition of this practice.
74	NDIA	S	18	CM	MLC	ML5-2	L5	It is unclear why DOD views "Share Configuration Management improvements across the organization" as a process rather than a practice. Assuming it is a process, it is unclear why DOD chose this process as one of only two processes that determine Level 5 maturity in the Configuration Management Domain.	Restate MLC as a Capability and make ML5-2 a practice within that Capability.
75	NDIA	S	19	CG	C3	L4-1	L4	[Pending feedback on whether a majority of companies currently meet controls proposed to shift down to L3] L4 requirement should be included in L3.	Combine L3 and L4. Eliminate L4.
76	NDIA	S	19	CG	C3	All	All	This capability pre-supposes the existence of a "cybersecurity plan," which is not required for Level 1. The capability could instead refer to the management of "cybersecurity objectives" for consistency with C1 in this domain as well as the associated practices.	The capability should be restated as follows: "Manage cybersecurity objectives."

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
77	NDIA	S	20	CG	C4	L4-3, L4-4, L4-5	L4	L4-3, L4-4 and L-5 are basic practices that should be in L3.	Combine L4-3, L4-4, and L4-5 into L3.
78	NDIA	S	21	CG	MLC	ML4-1	L4	It is unclear why DOD views "inform high-level management" as a process rather than a practice, particularly since it is similar to "Senior management is informed on the performance of cybersecurity critical success factors," which C4-L42 defines as a CG practice. Assuming "inform high-level management" is a process, it is too vague and general to serve as an objective, auditable basis for determining Level 4 maturity. Furthermore, it is unclear whey DOD chose this process as one of only two processes that determine Level 4 maturity in the Cybersecurity Governance Domain.	Restate MLC as a "Capability" rather than a "Maturity Level Capability," and make ML4-1 a practice within that Capability. Provide clearer definition of this practice.
79	NDIA	S	21	CG	MLC	ML4-2	L4	It is unclear why DOD chose to treat "Review Cybersecurity Governance activities for effectiveness" as a process rather than a practice. Assuming it is a process, it is unclear why DOD chose this process as one of only two processes that determine Level 4 maturity in the Cybersecurity Governance Domain.	Restate MLC as a Capability and make ML4-2 a practice within that Capability.
80	NDIA	S	21	CG	MLC	ML5-1	L5	It is unclear why DOD views "Standardize documentation for Cybersecurity Governance" as a process rather than a practice. Assuming it is a process, it is too vague and general to serve as an objective, auditable basis for determining Level 5 maturity. Furthermore, it is unclear why DOD chose this "process" as one of only	Restate MLC as a Capability and make ML5-1 a practice within that Capability. Provide clearer definition of this practice.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
								two processes that determine Level 5 maturity in the Cybersecurity Governance Domain.	
81	NDIA	S	21	CG	MLC	ML5-2	L5	It is unclear why DOD views "Share Cybersecurity Governance improvements across the organization" as a process rather than a practice. Assuming it is a process, it is unclear why DOD chose this process as one of only two processes that determine Level 5 maturity in the Cybersecurity Governance Domain.	Restate MLC as a Capability and make ML5-2 a practice within that Capability.
82	NDIA	S	22	IDA	C1	All	All	The phrase "before access is granted" is limiting. Identification could occur on an iterative basis. If DOD considers pre-access analysis critical to this capability, it could be better described at the practice level. This capability is also stated in the passive voice.	The capability should be restated as follows: "Identify system users, processes, and devices."
83	NDIA	S	22	IDA	C2	All	All	The current phrasing of the proposed capability only refers to granting access, when it is entirely possible that access may be denied, withheld, or otherwise restricted at times. This capability could instead refer to the "management" of access to account for this concern. This would also better align the capability phrasing to the general structure followed by the capabilities in other domains. This capability is also stated in the passive voice.	The capability should be restated as follows: "Manage system access."
84	NDIA	S	22	IDA	C2	L5-1	L5	The requirement to "eliminate the use of dynamic passwords by unprivileged system users through the application of alternate	Provide clarity as noted or delete the practice.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
								means of knowledge-based or other authentication mechanisms" is too vague and general to serve as objective, auditable basis for assessing Level 5 maturity. No reference is given for this practice that could provide further guidance as to what key terms such as "dynamic passwords" mean.	
85	NDIA	S	22	IDA	C1	L5-1	L5	It is unclear what proposed practice would qualify as "alternate means of knowledge-based or other authentication mechanisms."	Remove L5-1.
86	NDIA	S	22	IDA	C2	L5-2	L5	The description of this practice is too vague and general to serve as an objective, auditable basis for assessing Level 5 maturity. Key terms such as "step up authentication" and "behavioral anomalies" are not defined.	Remove L5-2.
87	NDIA	S	24	IDA	MLC	ML4-1	L4	It is unclear why DOD views "inform high-level management" as a process rather than a practice. Assuming that "inform high-level management" is a process, it is too vague and general to serve as an objective, auditable basis for determining Level 4 maturity. "High-level management" is undefined, and there is no description of what types of information should be provided to such management. It is also unclear why DOD chose this process as one of only two processes that determine Level 4 maturity in the Identification and Authorization Domain.	Restate MLC as a "Capability" rather than a "Maturity Level Capability," and make ML4-1 a practice within that Capability. Provide clearer definition of this practice.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
88	NDIA	S	24	IDA	MLC	ML4-2	L4	It is unclear why DOD chose to treat "Review Identification and Authorization activities for effectiveness" as a process rather than a practice. Assuming it is a process, it is unclear why DOD chose this process as one of only two processes that determine Level 4 maturity in the Identification and Authorization Domain.	Restate MLC as a Capability and make ML4-2 a practice within that Capability.
89	NDIA	S	24	IDA	MLC	ML5-1	L5	It is unclear why DOD views "Standardize documentation for Identification and Authorization" as a process rather than a practice. Assuming it is a process, it is too vague and general to serve as an objective, auditable basis for determining Level 5 maturity. It is also unclear why DOD chose this process as one of only two processes that determine Level 5 maturity in the Identification and Authorization Domain.	Restate MLC as a Capability and make ML5-1 a practice within that Capability. Provide clearer definition of this practice.
90	NDIA	S	24	IDA	MLC	ML5-2	L5	It is unclear why DOD views "Share Identification and Authorization improvements across the organization" as a process rather than a practice. Assuming it is a process, it is unclear why DOD chose this process as one of two processes for determining Level 5 maturity in the Identification and Authorization Domain.	Restate MLC as a Capability and make ML5-2 a practice within that Capability.
91	NDIA	S	25	IR	C1	L4-1	L4	The term "semi-automated fashion" is undefined.	Provide clarity as noted.
92	NDIA	S	25	IR	C4	L5-1	L5	This proposed practice (which lacks any reference) would require the organization to	Provide clarity as noted or delete the practice.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
								"fully employ[] autonomous initial response actions at machine speed . . . without needing human intervention." Many of the key terms of this practice are undefined and unclear, including "fully employ," "autonomous initial response actions," "machine speed," and "human intervention." Absent reasonable and practical definitions of these terms, this practice will be difficult to implement and assess.	
93	NDIA	S	25	IR	C5	L4-1	L4	The requirement to "maintain" a security operations center could be interpreted as precluding the organization from using a third party to provide this service.	Provide clarity as noted.
94	NDIA	S	25	IR	C5	L5-1	L5	The requirement to "maintain" a full-time security operations center could be interpreted as limiting or precluding the organization from using a third party to provide this service.	Provide clarity as noted.
95	NDIA	S	26	IR	C5	L4-3	L4	The practice's requirement to use a combination of manual and real-time responses to anomalous activities "that matches incident patterns" will be difficult to implement due to the difficulty of determining when a response "matches" incident patterns.	Provide clarity as noted or delete the practice.
96	NDIA	S	26	IR	C5	L5-3	L5	The practice's requirement that the organization "establishes and maintains a cyber incident response team that can be deployed to any location within 24 hours" could be interpreted to limit or preclude the organization from using a third party to provide the service.	Clarify that third parties can be used and that deployment does not mean that personnel would need to physically be at the location where an incident is occurring, nor would they be expected to leave the United States.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
								In addition, during a cyber incident, it may be costly and take valuable time away from a response and remediation action to physically deploy staff when they can be more effective in a centralized cybersecurity operations center. To the extent that a cyber incident occurs outside the continental United States, it also can be very difficult, if not impossible, to get staff to that location in 24 hours. In addition, there could be potential privacy issues implicated if United States personnel are involved in reviewing cyber incidents that occur overseas due to foreign law.	
97	NDIA	S	27	IR	C5 / C9	All	All	This capability appears out of order compared to the general structure of the capabilities across the various domains, which appears to follow the high-level steps of a business process. To resolve this and simplify the model, C9 could be merged with C5 as C5 inherently involves planning activities, especially at the higher levels and maturity levels.	Merge capabilities C5 and C9. The resulting capability should be stated as follows: "Plan, develop, and implement response to a declared incident."
98	NDIA	S	27	IR	C8	L5-1	L5	This proposed practice would require half of all simulated tabletop exercises to be unannounced. This requirement is unnecessarily prescriptive and inflexible. Further, not all exercises need to be "tabletops," in which case the requirement for unannounced exercises could be more feasible.	Clarify the meaning of "exercise" to include other types of simulations or tests and delete the requirement for a specific percentage of unannounced exercises. Or, delete the proposed practice in favor of less prescriptive requirements.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
99	NDIA	S	27	IR	C8	L5-2	L5	The requirement to apply "proactive, real-time forensics data gathering across all connected devices" is unduly broad and burdensome.	Delete the practice.
100	NDIA	S	27	IR	C8	L5-3	L5	The requirement to employ "automated, real-time methods to measure actual incidence response effectiveness for further analysis and lessons learned" is confusing. What is an "automated" method to measure actual incidence response effectiveness? What is a "real-time" method to measure incidence response effectiveness?	Provide clarity as noted.
101	NDIA	S	28	IR	MLC	ML4-1	ML4	It is unclear why DOD views "Inform high-level management" as a process rather than a practice. Assuming that "inform high-level management" is a process, it is too vague and general to serve as an objective, auditable basis for determining Level 4 maturity. What constitutes "high-level management," and what must such management be informed of? Furthermore, it is unclear why DOD chose this process as one of only two processes that determine Level 4 maturity in the Incident Response Domain.	Restate MLC as a "Capability" rather than a "Maturity Level Capability," and make ML4-1 a practice within that Capability. Provide clearer definition of this practice.
102	NDIA	S	28	IR	MLC	ML4-2	L4	It is unclear why DOD views "Review Incident Response activities for effectiveness" as a process rather than a practice, particularly when IR L5-3 defines employing automated, real-time methods to measure actual incidence response effectiveness" as a practice. Assuming that "Review Incident Response activities for effectiveness" is a process, it is	Restate MLC as a Capability and make ML4-2 a practice within that Capability.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
								unclear why DOD chose this practice as one of only two practices that determine Level 4 maturity in the Incident Response Domain.	
103	NDIA	S	28	IR	MLC	ML5-1	L5	It is unclear why DOD views "Standardize document for Incident Response" as a process rather than a practice. Assuming that it is a practice, it is too vague and general to serve as an objective, auditable basis for determining Level 5 maturity. Furthermore, it is unclear why DOD chose this process as one of only two processes that determine Level 5 maturity in the Incident Response Domain.	Restate MLC as a Capability and make ML5-1 a practice within that Capability. Provide clearer definition of this practice.
104	NDIA	S	28	IR	MLC	ML5-2	L5	It is unclear why DOD views "Share Incident Response improvements across the organization" as a process rather than a practice. Assuming it is a process, it is unclear why DOD chose it as one of only two processes that determine Level 5 maturity in the Incident Response Domain.	Restate MLC as a Capability and make ML5-2 a practice within that Capability.
105	NDIA	S	29	MA	C1 / C2	All	All	The capabilities in this domain appear out of order compared to the general structure of the capabilities across the various domains, which appears to follow the high-level steps of a business process. C1 and C2 would ideally be switched. Both are also stated in the passive voice.	Capability C1 should be :"Identify and control maintenance activities." Capability C2 should be: "Perform maintenance activities."
106	NDIA	S	29	MA	C2	L4-1	L4	This practice would require that "all maintenance systems are treated as if they contain the highest level of CUI data contained on any system they maintain." Absent some	Delete proposed practice.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
								practice or process calling for segregation of CUI data by levels, this practice makes no sense. Further, contractors should be allowed and encouraged to prioritize risks and have the flexibility needed to manage risk according to a risk profile.	
107	NDIA	S	30	MA	MLC	ML4-1	L4	It is unclear why DOD views "inform high-level management" as a process rather than a practice. Assuming that "inform high-level management" is a process, it is too vague and general to serve as an objective, auditable basis for determining Level 5 maturity. "High-level management" is undefined, and there is no description of what types of information should be provided to such management. Furthermore, it is unclear why DOD chose this process as one of only two processes that determine Level 4 maturity in the Maintenance Domain.	Restate MLC as a "Capability" rather than a "Maturity Level Capability," and make ML4-1 a practice within that Capability. Provide clearer definition of this practice.
108	NDIA	S	30	MA	MLC	ML4-2	L4	It is unclear why DOD views "Review Maintenance activities for effectiveness" as a process rather than a practice. Assuming it is a process, it is unclear why DOD chose this process as one of only two processes that determine Level 4 maturity in the Maintenance Domain.	Restate MLC as a Capability and make ML4-2 a practice within that Capability.
109	NDIA	S	30	MA	MLC	ML5-1	L5	It is unclear why DOD views “Standardize documentation for Maintenance” as a process rather than a practice. Assuming it is a process, it is too vague and general to serve as an objective, auditable basis for determining	Restate MLC as a Capability and make ML5-1 a practice within that Capability. Provide clearer definition of this practice.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
								Level 5 maturity. Furthermore, it is unclear why DOD chose this process as one of only two processes that determine Level 5 maturity in the Maintenance Domain.	
110	NDIA	S	30	MA	MLC	ML5-2	L5	It is unclear why DOD views "Share Maintenance improvements across the organization" as a process rather than a practice. Assuming it is a process, it is unclear why DOD chose this process as one of only two processes that determine Level 5 maturity in the Maintenance Domain.	Restate MLC as a Capability and make ML5-2 a practice within that Capability.
111	NDIA	S	31	MP	C1 / C4	All	All	Capabilities C4 and C1 could be merged to simplify the model because "marking" media may also be an important component of its "identification" as containing CUI. Only one practice is listed in each current capability. Both capabilities are also in passive voice.	Merge capabilities C1 and C4. The resulting capability should be restated as follows: "Identify media."
112	NDIA	S	31	MP	C3	All	All	This capability is stated in the passive voice.	The capability should be restated as follows: "Sanitize media."
113	NDIA	S	31-32	MP	C2 / C5	All	All	Capabilities C5 and C2 could be merged to simplify the model because they are not mutually exclusive. C2—regarding media protection—would clearly include practices associated with protecting media during transport. Both capabilities are also in passive voice.	Merge capabilities C2 and C5. The resulting capability should be restated as follows: "Protect media."
114	NDIA	S	32	MP	C5	L5-1	L5	This proposed practice would require the organization to maintain consistent awareness of the locations and times of use of removable	Suggest CSF: PR.PT-2 definition "Removable media is protected and its use restricted according to policy"

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
								media storing "critical technology CUI." The term "critical technology CUI" is undefined, which makes the proposed practice difficult to implement and to use to assess Level 5 maturity. Furthermore, the requirement is unclear. Is the expectation for real-time location tracking of removal media?	
115	NDIA	S	32	MP	C6 / C7	All	All	Capabilities C6 and C7 could be merged to simplify the model. Both proposed capabilities are currently quite narrowly framed. Capability C7 is essentially a restatement of the sole associated practice.	Merge capabilities C6 and C7. The resulting capability should be restated as follows: “Control the use of removable media on system components.”
116	NDIA	S	33	MP	MLC	ML4-1	L4	It is unclear why DOD views "inform high-level management" as a process rather than a practice. Assuming that "inform high-level management" is a process, it is too vague and general to serve as an objective, auditable basis for determining Level 5 maturity. "High-level management" is undefined, and there is no description of what types of information should be provided to such management. Furthermore, it is unclear why DOD chose this process as one of only two processes that determine Level 4 maturity in the Media Protection Domain.	Restate MLC as a "Capability" rather than a "Maturity Level Capability," and make ML4-1 a practice within that Capability. Provide clearer definition of this practice.
117	NDIA	S	33	MP	MLC	ML4-2	L4	It is unclear why DOD views "Review Media Protection activities for effectiveness" as a process rather than a practice. Assuming it is a process, it is unclear why DOD chose this process as one of only two processes that	Restate MLC as a Capability and make ML4-2 a practice within that Capability.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
								determine Level 4 maturity in the Media Protection Domain.	
118	NDIA	S	33	MP	MLC	ML5-1	L5	It is unclear why DOD views "Standardize documentation for Media Protection" as a process rather than a practice. Assuming it is a process, it is too vague and general to serve as an objective, auditable basis for determining Level 5 maturity. Furthermore, it is unclear why DOD chose this process as one of only two processes that determine Level 5 maturity in the Media Protection Domain.	Restate MLC as a Capability and make ML5-1 a practice within that Capability. Provide clearer definition of this practice.
119	NDIA	S	33	MP	MLC	ML5-2	L5	It is unclear why DOD views "Share Media Protection improvements across the organization" as a process rather than a practice. Assuming it is a process, it is unclear why DOD chose this process as one of only two processes that determine Level 5 maturity in the Media Protection Domain.	Restate MLC as a Capability and make ML5-2 a practice within that Capability.
120	NDIA	S	35	PS	MLC	ML4-1	L4	It is unclear why DOD views "inform high-level management" as a process rather than a practice. Assuming that "inform high-level management" is a process, it is too vague and general to serve as an objective, auditable basis for determining Level 5 maturity. "High-level management" is undefined, and there is no description of what types of information should be provided to such management. Furthermore, it is unclear why DOD chose this process as one of only two processes that	Restate MLC as a "Capability" rather than a "Maturity Level Capability," and make ML4-1 a practice within that Capability. Provide clearer definition of this practice.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
								determine Level 4 maturity in the Personnel Security Domain.	
121	NDIA	S	35	PS	MLC	ML4-2	L4	It is unclear why DOD views "Review Personnel Security activities for effectiveness" as a process rather than a practice. Assuming it is a process, it is unclear why DOD chose this process as one of only two processes that determine Level 4 maturity in the Personnel Security Domain.	Restate MLC as a Capability and make ML4-2 a practice within that Capability.
122	NDIA	S	35	PS	MLC	ML5-1	L5	It is unclear why DOD views “Standardize documentation for Personnel Security” as a process rather than a practice. Assuming it is a process, it is too vague and general to serve as an objective, auditable basis for determining Level 5 maturity. Furthermore, it is unclear why DOD chose this process as one of only two processes that determine Level 5 maturity in the Personnel Security Domain.	Restate MLC as a Capability and make ML5-1 a practice within that Capability. Provide clearer definition of this practice.
123	NDIA	S	35	PS	MLC	ML5-2	L5	It is unclear why DOD views “Share Personnel Security improvements across the organization” as a process rather than a practice. Assuming it is a process, it is unclear why DOD chose this process as one of only two processes that determine Level 5 maturity in the Personnel Security Domain.	Restate MLC as a Capability and make ML5-2 a practice within that Capability.
124	NDIA	S	37	PP	C4	All	All	The phrase “operation environments” in capability C4 is phrased inconsistently with capabilities C2 and C3, which refer to “operating environments.”	The capability should be restated as follows: “Limit physical access to organizational systems, equipment, and respective operating environments based on defined physical security access requirements.”

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
125	NDIA	S	38	PP	MLC	ML4-1	L4	It is unclear why DOD views "inform high-level management" as a process rather than a practice. Assuming that "inform high-level management" is a process, it is too vague and general to serve as an objective, auditable basis for determining Level 5 maturity. "High-level management" is undefined, and there is no description of what types of information should be provided to such management. Furthermore, it is unclear why DOD chose this process as one of only two processes that determine Level 4 maturity in the Physical Protection Domain.	Restate MLC as a "Capability" rather than a "Maturity Level Capability," and make ML4-1 a practice within that Capability. Provide clearer definition of this practice.
126	NDIA	S	38	PP	MLC	ML4-2	L4	It is unclear why DOD views "Review Physical Protection activities for effectiveness" as a process rather than a practice. Assuming it is a process, it is unclear why DOD chose this process as one of only two processes that determine Level 4 maturity in the Physical Protection Domain.	Restate MLC as a Capability and make ML4-2 a practice within that Capability.
127	NDIA	S	38	PP	MLC	ML5-1	L5	It is unclear why DOD views “Standardize documentation for Physical Protection” as a process rather than a practice. Assuming it is a process, it is too vague and general to serve as an objective, auditable basis for determining Level 5 maturity. Furthermore, it is unclear why DOD chose this process as one of only two processes that determine Level 5 maturity in the Physical Protection Domain.	Restate MLC as a Capability and make ML5-1 a practice within that Capability. Provide clearer definition of this practice.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
128	NDIA	S	38	PP	MLC	ML5-2	L5	It is unclear why DOD views "Share Physical Protection improvements across the organization" as a process rather than a practice. Assuming it is a process, it is unclear why DOD chose this process as one of only two processes that determine Level 5 maturity in the Physical Protection Domain.	Restate MLC as a Capability and make ML5-2 a practice within that Capability.
129	NDIA	S	39	RE	C1 / C2	All	All	This domain is entirely missing a capability and associated practices relating to the identification of back-up requirements. The identification of back-up needs, requirements, and associated systems is a critical part of the recovery process. Organizations should think critically about what back-ups are needed, the frequency of back-ups relevant to the data stored and its risks, and the appropriate methods and systems for back-ups.	A new capability and associated practices should be referred to as C1. The capability should be stated as follows: "Identify system back-up and recovery requirements." Capabilities currently referred to as C1 and C2 would then become C2 and C3 respectively.
130	NDIA	S	40	RE	MLC	ML4-1	L4	It is unclear why DOD views "inform high-level management" as a process rather than a practice. Assuming that "inform high-level management" is a process, it is too vague and general to serve as an objective, auditable basis for determining Level 5 maturity. "High-level management" is undefined, and there is no description of what types of information should be provided to such management. Furthermore, it is unclear why DOD chose this process as one of only two processes that determine Level 4 maturity in the Recovery Domain.	Restate MLC as a "Capability" rather than a "Maturity Level Capability," and make ML4-1 a practice within that Capability. Provide clearer definition of this practice.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
131	NDIA	S	40	RE	MLC	ML4-2	L4	It is unclear why DOD views "Review Recovery activities for effectiveness" as a process rather than a practice. Assuming it is a process, it is unclear why DOD chose this process as one of only two processes that determine Level 4 maturity in the Recovery Domain.	Restate MLC as a Capability and make ML4-2 a practice within that Capability.
132	NDIA	S	40	RE	MLC	ML5-1	L5	It is unclear why DOD views “Standardize documentation for Recovery” as a process rather than a practice. Assuming it is a process, it is too vague and general to serve as an objective, auditable basis for determining Level 5 maturity. Furthermore, it is unclear why DOD chose this process as one of only two processes that determine Level 5 maturity in the Recovery Domain.	Restate MLC as a Capability and make ML5-1 a practice within that Capability. Provide clearer definition of this practice.
133	NDIA	S	40	RE	MLC	ML5-2	L5	It is unclear why DOD views “Share Recovery improvements across the organization” as a process rather than a practice. Assuming it is a process, it is unclear why DOD chose this process as one of only two processes that determine Level 5 maturity in the Recovery Domain.	Restate MLC as a Capability and make ML5-2 a practice within that Capability.
134	NDIA	S	41	RM	C1	L4-1	L4	The proposed practice is too general to be useful.	Provide clarity or delete the practice.
135	NDIA	S	41	RM	C3	L5-1	L5	This proposed practice uses general terms such as "advanced automation" and "advanced analytic capabilities" that are undefined. The proposed practice is therefore too general to serve as an objective, auditable basis for	Provide clarity as noted or delete the practice.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
								assessing Level 5 maturity. As noted elsewhere, it is also unclear whether "automated" practices are reasonable or sensible for all environments.	
136	NDIA	S	41	RM	C2 / C3	All	All	Capabilities C2 and C3 could be merged to simplify the model. Risk identification and documentation are closely related, as reflected in the underlying NIST and RMM classifications of the practices associates with both capabilities in the proposed model. The fact that C2 currently has only one associated practice supports its inclusion in a slightly broader capability. The current phrasing of C2 to document only "organizational risk" is also too limiting to capture the risks otherwise contemplated by this domain.	Merge capabilities C2 and C3. The resulting capability should be stated as follows: "Identify and document risks."
137	NDIA	S	42	RM	C3	L4-3	L4	The term "automated" in this proposed practice is undefined and too general to serve as an objective, auditable basis for assessing Level 4 maturity. It is also unclear whether "automated" practices are reasonable or sensible for all environments.	Provide clarity as noted or delete the practice.
138	NDIA	S	42	RM	C5	L5-2	L5	The term "prioritize subcontractors and vendors" is unclear. Does the practice contemplate giving a preference to certain subcontractors and vendors in subcontract formation and administration? If so, that would be problematic. In addition, it is unclear how anti-tamper techniques of suppliers relates	Delete practice.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
								directly to protection of DOD data on internal contractor systems.	
139	NDIA	S	43	RM	C6	L4-2	L4	It is unclear how preserving integrity of supplier software, hardware, and firmware through the combined use of integrity measurement, data labeling, and source authentication relates specifically to the protection of DOD data on internal contractor systems.	Clarify the direct relationship to protection of DOD data on internal contractor systems or delete.
140	NDIA	S	43	RM	C6	L5-1	L5	It is unclear how anti-tamper techniques of s suppliers relates directly to protection of DOD data on internal contractor systems.	Clarify the direct relationship to protection of DOD data on internal contractor systems or delete.
141	NDIA	S	42-43	RM	C5 / C6	All	All	Capabilities C5 and C6 could be merged to simplify the model. These capabilities as currently proposed are not mutually exclusive. Managing supply chain risk (C6) is a more specific and more advanced subset of managing risk more generally (C5). Accordingly, the management of supply chain risk is better articulated at the practice level within one larger capability.	Merge capabilities C5 and C6. The resulting capability should be stated as follows: “Manage risk.”
142	NDIA	S	43	RM	C5	L5-3	L5	This proposed practice would require the organization to use methods to "obfuscate" its true identity when procuring "sensitive products or services." A requirement to knowingly obfuscate in transactions with third parties raises significant legal and ethical concerns. In addition, the term "sensitive" is undefined and potentially extremely broad.	Delete proposed practice.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
143	NDIA	S	44	RM	MLC	ML4-1	L4	It is unclear why DOD views "inform high-level management" as a process rather than a practice. Assuming that "inform high-level management" is a process, it is too vague and general to serve as an objective, auditable basis for determining Level 5 maturity. "High-level management" is undefined, and there is no description of what types of information should be provided to such management. Furthermore, it is unclear why DOD chose this process as one of only two processes that determine Level 4 maturity in the Risk Management Domain.	Restate MLC as a "Capability" rather than a "Maturity Level Capability," and make ML4-1 a practice within that Capability. Provide clearer definition of this practice.
144	NDIA	S	44	RM	MLC	ML4-2	L4	It is unclear why DOD views "Review Risk Management activities for effectiveness" as a process rather than a practice. Assuming it is a process, it is unclear why DOD chose this process as one of only two processes that determine Level 4 maturity in the Risk Management Domain.	Restate MLC as a Capability and make ML4-2 a practice within that Capability.
145	NDIA	S	44	RM	MLC	ML5-1	L5	It is unclear why DOD views “Standardize documentation for Risk Management” as a process rather than a practice. Assuming it is a process, it is too vague and general to serve as an objective, auditable basis for determining Level 5 maturity. Furthermore, it is unclear why DOD chose this process as one of only two processes that determine Level 5 maturity in the Risk Management Domain.	Restate MLC as a Capability and make ML5-1 a practice within that Capability. Provide clearer definition of this practice.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
146	NDIA	S	44	RM	MLC	ML5-2	L5	It is unclear why DOD views “Share Risk Management improvements across the organization” as a process rather than a practice. Assuming it is a process, it is unclear why DOD chose this process as one of only two processes that determine Level 5 maturity in the Risk Management Domain.	Restate MLC as a Capability and make ML5-2 a practice within that Capability.
147	NDIA	S	45	SAS	C1	L4-2	L4	The proposed practice of applying "cybersecurity analysis" to "all acquisition and merger activities" is too broad and vague to serve as an objective, auditable standard for assessing Level 4 maturity.	Delete proposed practice.
148	NDIA	S	45	SAS	C5	L4-1	L4	The phrases "leveraging automated scanning tools" and "ad hoc tests using human experts" are not defined.	Define key terms of practice.
149	NDIA	S	45	SAS	C5	L5-1	L5	The term "test bed" for elements not typically tested in production is not defined.	Define key terms of practice.
150	NDIA	S	45-46	SAS	All	All	All	The capabilities in this domain appear out of order compared to the general structure of the capabilities across the various domains, which appears to follow the high-level steps of a business process. Reordering the capabilities to reflect that natural flow would be more consistent with the rest of the model and would facilitate understanding. Capabilities C5 and C6 could be merged to simplify the model. As currently proposed, C6 is very narrowly construed and lacks context. It would be appropriate grouped with C5	Reorder the capabilities in this domain. The resulting order of the capabilities (as currently numbered) would be C3, C4, C1, C2, C5 (merged with C6). Merge capabilities C5 and C6. The resulting capability should be stated as follows: “Manage and implement controls.”

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
								because the practices currently contemplated in C6 are things an organization would do as a part of managing its security controls.	
151	NDIA	S	46	SAS	C5	L4-2	L4	The terms "red teaming" and "defensive capabilities" are not defined.	Define key terms of practice.
152	NDIA	S	46	SAS	C5	L5-2	L5	The term "advanced adversarial assessment" is not defined.	Define key terms of practice.
153	NDIA	S	47	SAS	C6	L4-1	L4	It is not clear how performing code reviews on open source software as an application vetting processor prior to being included in the organization’s approved software list relates specifically to protection of DOD data on internal contractor systems.	Clarify the direct relationship to protection of DOD data on internal contractor systems or delete.
154	NDIA	S	47	SAS	MLC	ML4-1	L4	It is unclear why DOD views "inform high-level management" as a process rather than a practice. Assuming that "inform high-level management" is a process, it is too vague and general to serve as an objective, auditable basis for determining Level 5 maturity. "High-level management" is undefined, and there is no description of what types of information should be provided to such management. Furthermore, it is unclear why DOD chose this process as one of only two processes that determine Level 4 maturity in the Security Assessment Domain.	Restate MLC as a "Capability" rather than a "Maturity Level Capability," and make ML4-1 a practice within that Capability. Provide clearer definition of this practice.
155	NDIA	S	47	SAS	MLC	ML4-2	L4	It is unclear why DOD views "Review Security Assessment activities for effectiveness" as a process rather than a practice. Assuming it is a	Restate MLC as a Capability and make ML4-2 a practice within that Capability.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
								process, it is unclear why DOD chose this process as one of only two processes that determine Level 4 maturity in the Security Assessment Domain.	
156	NDIA	S	47	SAS	MLC	ML5-1	L5	It is unclear why DOD views “Standardize documentation for Security Assessment” as a process rather than a practice. Assuming it is a process, it is too vague and general to serve as an objective, auditable basis for determining Level 5 maturity. Furthermore, it is unclear why DOD chose this process as one of only two processes that determine Level 5 maturity in the Security Assessment Domain.	Restate MLC as a Capability and make ML5-1 a practice within that Capability. Provide clearer definition of this practice.
157	NDIA	S	47	SAS	MLC	ML5-2	L5	It is unclear why DOD views “Share Security Assessment improvements across the organization” as a process rather than a practice. Assuming it is a process, it is unclear why DOD chose this process as one of only two processes that determine Level 5 maturity in the Security Assessment Domain.	Restate MLC as a Capability and make ML5-2 a practice within that Capability.
158	NDIA	S	48-49	SA	C1 / C3	All	All	Capabilities C1 and C3 could be merged to simplify the model. This would emphasize the need for organizations to effectively communicate about threats as an inherent function of the monitoring itself to increase their relative maturity within the model. This would also be consistent with the placement of the associated practices in the NIST framework.	Merge capabilities C1 and C3. The resulting capability should be stated as follows: “Establish threat monitoring requirements.”

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
159	NDIA	S	49	SA	C4	L4-1	L4	Key terms of this proposed practice such as "automates ingestion and initial analysis of intel feed" are undefined. In addition, the requirement to "share initial indicators within 24 hours" is unclear and potentially unworkable. As noted elsewhere, it is also unclear whether "automated" practices are reasonable or sensible for all environments.	Delete proposed practice.
160	NDIA	S	49	SA	C4	L5-1	L4	The requirement to "automate[] the response to intel analysis and sharing of indicators" is unclear and potentially burdensome. As noted elsewhere, it is also unclear whether "automated" practices are reasonable or sensible for all environments.	Delete proposed practice.
161	NDIA	S	50	SA	MLC	ML4-1	L4	It is unclear why DOD views "inform high-level management" as a process rather than a practice. Assuming that "inform high-level management" is a process, it is too vague and general to serve as an objective, auditable basis for determining Level 5 maturity. "High-level management" is undefined, and there is no description of what types of information should be provided to such management. Furthermore, it is unclear why DOD chose this process as one of only two processes that determine Level 4 maturity in the Situational Awareness Domain.	Restate MLC as a "Capability" rather than a "Maturity Level Capability," and make ML4-1 a practice within that Capability. Provide clearer definition of this practice.
162	NDIA	S	50	SA	MLC	ML4-2	L4	It is unclear why DOD views "Review Situational Awareness activities for effectiveness" as a process rather than a practice. Assuming it is a process, it is unclear	Restate MLC as a Capability and make ML4-2 a practice within that Capability.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
								why DOD chose this process as one of only two processes that determine Level 4 maturity in the Situational Awareness Domain.	
163	NDIA	S	50	SA	MLC	ML5-1	L5	It is unclear why DOD views "Standardize documentation for Situational Awareness" as a process rather than a practice. Assuming it is a process, it is too vague and general to serve as an objective, auditable basis for determining Level 5 maturity. Furthermore, it is unclear why DOD chose this process as one of only two processes that determine Level 5 maturity in the Situational Awareness Domain.	Restate MLC as a Capability and make ML5-1 a practice within that Capability. Provide clearer definition of this practice.
164	NDIA	S	50	SA	MLC	ML5-2	L5	It is unclear why DOD views "Share Situational Awareness improvements across the organization" as a process rather than a practice. Assuming it is a process, it is unclear why DOD chose this process as one of only two processes that determine Level 5 maturity in the Situational Awareness Domain.	Restate MLC as a Capability and make ML5-2 a practice within that Capability.
165	NDIA	S	51	SCP	C1	L4-2	L4	This proposed practice, which is described as an "enhancement" of NIST SP 800-171 3.13.2, would require that "administration of high value critical network infrastructure components and servers are physically separated from production networks (e.g., through out-o-band networks)." The key term "high value critical" is undefined. Without a definition of that term and other key terms, this practice cannot serve as an objective, auditable basis for assessment of Level 4 maturity.	Define key terms of proposed practice.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
166	NDIA	S	51	SCP	CI	L5-2	L5	This proposed practice requires the organization to employ technical and procedural means to confuse and mislead adversaries." This requirement raises significant legal and ethical issues to the extent such technical and procedural means would be likely to confuse and mislead the organization's customers, employees, shareholders, and regulators.	Delete proposed practice.
167	NDIA	S	51	SCP	CI	L5-3	L5	A key term of this proposed practice -- "zero trust concepts --" is undefined. Absent a clear and practical definition of this key term, the proposed practice cannot serve as an objective, auditable basis for assessing Level 5 maturity.	Define key terms of proposed practice.
168	NDIA	S	51	SCP	CI	L4-4	L4	A key term of this proposed practice -- "secure cryptographic schemes" -- is undefined. Absent a clear and reasonable definition of this key term, the proposed practice cannot serve as an objective, auditable basis for assessing Level 4 maturity.	Define key terms of proposed practice.
169	NDIA	S	51	SCP	C1	L5-4	L5	Key terms of the proposed practice, including "advanced, automated infrastructure implementation and configuration management techniques," are undefined. Absent clear and reasonable definitions of key terms, the proposed practice cannot serve as an objective, auditable basis for assessing Level 5 maturity. As noted elsewhere, it is also unclear whether "automated" practices are reasonable or sensible for all environments.	Define key terms of proposed practice.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
170	NDIA	S	51	SCP	C1	L4-5	L5	This proposed practice would require the organization to analyze all outgoing emails, including personal emails, for the presence of CUI data. That requirement raises significant legal and privacy issues and could be extremely costly and difficult to implement, since it is unlikely that any existing software program could comprehensively distinguish CUI form non-CUI information under existing guidance.	Delete proposed practice.
171	NDIA	S	53	SCP	C2	L5-1	L5	Key terms of this proposed practice are undefined, including "custom" and "not widely deployed boundary protection systems." Absent clear and reasonable definitions of these key terms, the proposed practice cannot serve as an objective, auditable basis for assessing Level 5 maturity.	Define key terms of proposed practice.
172	NDIA	S	53	SCP	C2	L5-2	L5	Key terms of this proposed practice -- including "granular network control" and "microsegmentation" -- are undefined. Absent clear and reasonable definition of these key terms, the proposed practice cannot serve as an objective, auditable basis for assessing Level 5 maturity.	Define key terms of proposed practice.
173	NDIA	S	53	SCP	C2	L4-4	L4	Key terms of this proposed practice -- including "mechanisms to sandbox" -- are undefined. Absent clear and reasonable definition of these key terms, this proposed practice cannot serve as an objective, auditable basis for assessing Level 4 maturity.	Define key terms of proposed practice.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
174	NDIA	S	53	SCP	C2	All	All	The phrase “at system boundaries” is unnecessarily limiting and should be deleted. It does not appear to encompass internal system communications. Nor is it consistent with the overall concept of “defense in depth.”	Delete “at system boundaries” from C2. The capability should be restated as follows: “Control communications.”
175	NDIA	S	54	SCP	C3	L5-1	L5	Key terms of this proposed practice -- including "hardware rooted integrity verification," "secure boot," "boot attestation," and "measured boot" -- are undefined. Absent clear and reasonable definitions of these key terms, the proposed plan cannot serve as an objective, auditable basis for assessing Level 5 maturity.	Provide clarity as noted or delete the practice.
176	NDIA	S	55	SCP	MLC	ML4-1	L4	It is unclear why DOD views "inform high-level management" as a process rather than a practice. Assuming that "inform high-level management" is a process, it is too vague and general to serve as an objective, auditable basis for determining Level 5 maturity. "High-level management" is undefined, and there is no description of what types of information should be provided to such management. Furthermore, it is unclear why DOD chose this process as one of only two processes that determine Level 4 maturity in the Systems and Communications Protection Domain.	Restate MLC as a "Capability" rather than a "Maturity Level Capability," and make ML4-1 a practice within that Capability. Provide clearer definition of this practice.
177	NDIA	S	55	SCP	MLC	ML4-2	L4	It is unclear why DOD views "Review System and Communications Protection activities for effectiveness" as a process rather than a practice. Assuming it is a process, it is unclear why DOD chose this process as one of only	Restate MLC as a Capability and make ML4-2 a practice within that Capability.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
								two processes that determine Level 4 maturity in the System and Communications Protection Domain.	
178	NDIA	S	55	SCP	MLC	ML5-1	L5	It is unclear why DOD views “Standardize documentation for System and Communications Protection” as a process rather than a practice. Assuming it is a process, it is too vague and general to serve as an objective, auditable basis for determining Level 5 maturity. Furthermore, it is unclear why DOD chose this process as one of only two processes that determine Level 5 maturity in the System and Communications Protection Domain.	Restate MLC as a Capability and make ML5-1 a practice within that Capability. Provide clearer definition of this practice.
179	NDIA	S	55	SCP	MLC	ML5-2	L5	It is unclear why DOD views “Share System and Communications Protection improvements across the organization” as a process rather than a practice. Assuming it is a process, it is unclear why DOD chose this process as one of only two processes that determine Level 5 maturity in the System and Communications Protection Domain.	Restate MLC as a Capability and make ML5-2 a practice within that Capability.
180	NDIA	S	56	SII	C1	All	All	The SII domain appears to have been a catch-all domain in that the capabilities are quite distinct from one another and do not follow the general structure followed by the capabilities in other domains. The capabilities can likely be successfully integrated into other domains to simplify the model. Capability C1, phrased actively, could be	Rephrase C1 as “Identify and correct information system flaws.” Insert C1 into either the Risk Management or Security Assessment domain as appropriate, which may include merging it with an existing capability. Rephrase C2 as “Identify and monitor sources of vulnerability information.” Insert C2 into either the Incident Response or Security Assessment domain as

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
								inserted into the Risk Management or Security Assessment domains as the capability and associated practices pertain to the identification and correction of system security flaws, topics already addressed by those domains. Capability C2, phrased actively, could be inserted into the Incident Response or Security Assessment domains as the capability and associated practices pertain to the monitoring of security issues, topics already addressed by those domains. Capability C3, phrased actively, could be inserted into the Incident Response or Security Assessment domains as the capability and associated practices pertain to the identification of malicious content, a topic already address by those domains. Capability C4, rephrased actively, could be inserted into the Incident Response or Security Assessment domains as the capability and associated practices pertain to the monitoring for potential anomalous or malicious behavior, a topic already addressed by those domains. Capability C5 could be inserted into the System and Communications Protection domain as it relates to advanced protections for email systems applicable to Levels 4 and 5.	appropriate, which may include merging it with an existing capability. Rephrase C3 as “Identify malicious content.” Insert C3 into either the Incident Response or Security Assessment domain as appropriate, which may include merging it with an existing capability. Rephrase C4 as “Monitor network and systems.” Insert C4 into either the Incident Response or Security Assessment domain as appropriate, which may include merging it with an existing capability. Insert C5 into the System and Communications Protection domain, which may include merging it with an existing capability.
181	NDIA	S	57	SII	C5	L4-1	L4	A key term of this proposed practice -- "asymmetric cryptography email protections" -	Define key terms of the proposed practice.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
								- is undefined. Absent a clear and reasonable definition of this key term, the proposed practice cannot serve as an objective, auditable basis for assessing Level 4 maturity.	
182	NDIA	S	57	SII	C5	L5-1	L5	The requirement of this practice to "implement email authenticity and integrity technologies" is too vague and general to serve as an objective, auditable basis for assessing Level 5 maturity.	Better define scope of proposed practice.
183	NDIA	S	58	SII	MLC	ML4-1	L4	It is unclear why DOD views "inform high-level management" as a process rather than a practice. Assuming that "inform high-level management" is a process, it is too vague and general to serve as an objective, auditable basis for determining Level 5 maturity. "High-level management" is undefined, and there is no description of what types of information should be provided to such management. Furthermore, it is unclear why DOD chose this process as one of only two processes that determine Level 4 maturity in the System and Informational Integrity Domain.	Restate MLC as a "Capability" rather than a "Maturity Level Capability," and make ML4-1 a practice within that Capability. Provide clearer definition of this practice.
184	NDIA	S	58	SII	MLC	ML4-2	L4	It is unclear why DOD views "Review System and Informational Integrity activities for effectiveness" as a process rather than a practice. Assuming it is a process, it is unclear why DOD chose this process as one of only two processes that determine Level 4 maturity in the System and Informational Integrity Domain.	Restate MLC as a Capability and make ML4-2 a practice within that Capability.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
185	NDIA	S	58	SII	MLC	ML5-1	L5	It is unclear why DOD views "Standardize documentation for System and Informational Integrity" as a process rather than a practice. Assuming it is a process, it is too vague and general to serve as an objective, auditable basis for determining Level 5 maturity. Furthermore, it is unclear why DOD chose this process as one of only two processes that determine Level 5 maturity in the System and Informational Integrity Domain.	Restate MLC as a Capability and make ML5-1 a practice within that Capability. Provide clearer definition of this practice.
186	NDIA	S	58	SII	MLC	ML5-2	L5	It is unclear why DOD views "Share System and Informational Integrity improvements across the organization" as a process rather than a practice. Assuming it is a process, it is unclear why DOD chose this process as one of only two processes that determine Level 5 maturity in the System and Informational Integrity Domain.	Restate MLC as a Capability and make ML5-2 a practice within that Capability.
187	NDIA	S	Multiple	Multiple	Multiple	Practice	Multiple	Several Domains have no Level 4 or 5 practices, yet they have level 4 and 5 Processes, for example Physical protection.	Need clarity on the linkages between practice and process

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
188	NDIA	S	Multiple	Multiple	Multiple	Practice	Multiple	Several Domains have no Level 4 or 5 practices, does this mean when you hit the highest-level practice you are automatically level 5?	Need clarity on how scoring works for practices that have no Level 4 or 5 requirements.
189	NDIA	A	Multiple	Multiple	Multiple	Practice	Multiple	Need consistency on where the requirement resides (e.g. on the organization or on a system, etc.) For example CM C5 L4-2 “employs configuration enforcement with adjustable..” is this at the organizational level or is it to the system/tool level?	Need clarity and consistency to what object the requirement applies too.
190	NDIA	C	Multiple	Multiple	Multiple	Practice	Multiple	Unclear how level requirements stack. In some capabilities, Level 1 Ad Hoc process becomes automated at Level 5, so there is a clear replacement of one requirement for another. Other capabilities it is difficult to discern if a higher-level requirement replaces the lower level requirement or if they stack on top of each other.	Need clarity on of practices stack on top of each other so that Level 3 or must also do all requirements at Level 2 and Level 1, or if there are capabilities, where higher-level requirements replace lower level requirements.
200	NDIA	C	Multiple	Multiple	Multiple	Practice	Multiple	Based on DIB CS Working Group on 9.17.2019 it was noted by Vicki Michetti that protection of CUI could not be less than full NIST 800-171 Compliance. If so then L1 and L2 should remove references to CUI as it could lead to confusion.	Clarify at which level an organization is approved to handle CUI and revise requirement statements as appropriate to remove CUI language from Levels ineligible to handle CUI.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
201	NDIA	S	2	AC	C2	Practice	2	L2-1 An organization at this level may not have the dedicated staff numbers or skillset to split off system ownerships.	Recommend moving to level 3
202	NDIA	S	2	AC	C2	Practice	3	L3-1 Should be imposed on organizations that have dedicated IT admins as soon as possible.	Recommend moving to level 2
203	NDIA	S	4	AC	C5	Practice	5	L5-3 Level 3 and 4 organizations should have the capabilities to cryptographically secure data, though not during execution.	Recommend cryptographic security requirement be lowered to Level 4 or 3. Keep execution requirement at Level 5.
204	NDIA	S	7	AM	C1	Practice	1	L1-1 Agree, but needs supporting requirements in C2, C3, C4. How can they identify assets if they have not defined them? How will inventories be useful if they are no criteria around when they should be updated?	Recommend adding additional Level 1 requirements to C2, C3, and C4 to round out a basic asset management program for a level 1 organization.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
205	NDIA	S	7	AM	C1	Practice	3	L3-2 Active discovery is more fitting to a proactive organization.	Recommend moving to level 4
206	NDIA	S	7	AM	C2	Practice	2	L2-1 This should be a basic control for any organization handling CUI.	Recommend moving to level 1, unless intent is that level 1 orgs will not be allowed to handle CUI.
207	NDIA	S	8	AM	C4	Practice	2	L2-1 This is more in line with a good practice org or a proactive org	Recommend swapping with C4 L3-1 or moving to L4
208	NDIA	S	8	AM	C4	Practice	3	L3-1 Level 3 org and above should have continuous updated asset inventory.	Recommend swapping with C4 L2-1

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
209	NDIA	A	8	AM	C4	Practice	4	L4-2 is there an associated reference for this requirement?	Please provide reference or amplifying information.
210	NDIA	S	10	AA	C4	Practice	1	L1-1 Skillset to even know what audit logs are or how to properly configure likely do not exist at level one org. Also missing supporting actions in other capabilities, such as defining the content of audit records.	Recommend moving up to L2
211	NDIA	A	10	AA	C4	Practice	4	L4-1 This is the same statement as AM C1 L4-2, but with different references.	Recommend making the requirements unique to their references.
212	NDIA	S	11	AA	C7	Practice	1	L1-1 Skillset to understand what are in the audit logs unlikely at level 1 Org.	Recommend moving up to L2

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
213	NDIA	A	13	AT	C1	Practice	3	L3-1 since this requires “updated” then it needs to be time bound (e.g. annually, every three years, etc.)	Since L4-1 is already time bound at 1 year, then L3 should be every 2 or 3 years.
214	NDIA	S	19	CG	C1	Practice	2	L2-2 Seems more suited to C3 otherwise it is repetitive.	Recommend move to C3 or removing.
215	NDIA	S	19	CG	C1	Practice	3	L3-1 Seems more suited to C3 otherwise it is repetitive.	Recommend move to C3 or removing.
216	NDIA	A	19	CG	C1	Practice	2	L2-2 typo on “has a defined plans”	Recommend changing to “has a defined plan”, no ‘s’.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
217	NDIA	S	19	CG	C4	Practice	2	Lots of overlap between C2, C3, and C4. Maybe more useful to collapse all into on capability that covers both.	Recommend collapse C2, C3, and C4.
218	NDIA	A	20	CG	C4	Practice	4	L4-5 is there an associated reference for this requirement?	Please provide reference or amplifying information.
219	NDIA	S	22	IDA	C1	Practice	1	L1-1 needs supporting requirements in C2.	Add supporting requirements in C2 L1
220	NDIA	S	22	IDA	C1	Practice	1	L1-2 needs supporting requirements in C2.	Add supporting requirements in C2 L1

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
221	NDIA	S	22	IDA	C1	Practice	2	L2-1 Needs supporting requirements in C2, otherwise what actions are taken as result of L2-1 process?	Add supporting requirements in C2 L2.
222	NDIA	S	22	IDA	C2	Practice	3	L3-1 MFA should be imposed on privileged users as soon as possible.	Recommend that MFA for privileged accounts be moved to L2, while MFA for non-privileged remain at L3.
223	NDIA	S	22	IDA	C2	Practice	4	L4-1 Seems repetitive of L3-1. If network access to non-privileged accounts is MFA at L3, not sure what L4 adds, as users of those items mentioned would be either privileged or non-privileged and need MFA at L3.	Recommend deleting. Alternatively, providing clarity on the distinction between L3 and L4.
224	NDIA	A	22	IDA	C2	Practice	5	L5-1 is there an associated reference for this requirement? Need more clarity on what alternate means would be acceptable.	Please provide reference or amplifying information.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
225	NDIA	S	23	IDA	C2	Practice	3	L3-5 Minimum password requirements should be a basic security measure.	Recommend lowering to L1
226	NDIA	S	23	IDA	C2	Practice	3	L3-6 Password reuse limits should be capable at intermediate orgs.	Recommend lowering to L2
227	NDIA	A	23	IDA	C2	Practice	3	L3-6 Password should be a plural in this context.	Recommend changing to Passwords.
228	NDIA	S	23	IDA	C2	Practice	3	L3-7 Password change upon login is a basic capability that should be present in intermediate orgs.	Recommend lowering to L2

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
229	NDIA	S	25	IR	C1	Practice	1	L1-1 Unlikely that the skill set or tools for event detection and reporting will be present at this level of maturity.	Recommend moving up to L3.
230	NDIA	S	25	IR	Multiple	Practice	2	Most of L2 requirements should be moved up to L3 as the skills, tools and other resource to meet most of these requirements are unlikely at L2. L2 should have define, identify and report as requirements, but not more granular than that.	Recommend L2 be limited to Define, identify, and report at a high level. Granular break down of IR requirements should be at L3 and above.
231	NDIA	S	25	IR	C3	Practice	1	L1-1 Unlikely that skillset or tools for incident detection are present at this level of maturity.	Recommend moving up to L2 or above.
232	NDIA	A	25	IR	C4	Practice	5	L5-1 is there an associated reference for this requirement?	Please provide reference or amplifying information.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
233	NDIA	S	25	IR	C5	Practice	4	L4-1 With internet connected systems handling level 4 data there should be a requirement for 24x7 SOC not just business hours, even if it passes over to a third party after business hours. Otherwise adversaries can plan and stage events for after hours.	Recommend that SOC requirements for L4 and L5 be full-time.
234	NDIA	A	26	IR	C5	Practice	4	L4-3 is there an associated reference for this requirement?	Please provide reference or amplifying information.
235	NDIA	A	26	IR	C5	Practice	5	L5-2 is there an associated reference for this requirement?	Please provide reference or amplifying information.
236	NDIA	A	27	IR	C9	Practice	4	L4-1 is there an associated reference for this requirement?	Please provide reference or amplifying information.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
237	NDIA	S	27	IR	C9	Practice	4	L4-1 Pre-Planned responses should already be part of a good cyber orgs playbook incorporating their existing tools.	Recommend moving this down to L3.
238	NDIA	S	29	MA	C2	Practice	2	L2-1 at this level it is more likely that admins will use whatever tool is available, unlikely that there will be the maturity present to have centralized approved tool list. This maybe burdensome to an immature org with limited resources.	Recommend moving this requirement to L3 or above.
239	NDIA	S	29	MA	C2	Practice	2	L2-2 at this level it is more unlikely that admin tools and maintenance tools will be locked down. This maybe burdensome to an immature org with limited resources.	Recommend moving this requirement to L3 or above.
240	NDIA	S	29	MA	C2	Practice	2	L2-3 At this level organization wide MFA maybe over burdensome. Agree that privileged-accounts should have MFA, but all others maybe too much based on maturity and resources at this level.	Recommend moving his up L3 or above.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
241	NDIA	S	31	MP	C3	Practice	1	L1-1 Without supporting requirements in the other Capabilities, there is little value in this requirement. Media needs to be identified and marked at a minimum for users to be aware of what need to be sanitized and destroyed. There is also question if L1 orgs will even be allowed to handle/develop CUI.	Recommend adding additional requirements in other L1 capabilities that round out a basic MP practice and/or move this up to L2 only especially if L1 orgs won't be allowed to handle CUI.
242	NDIA	S	31	MP	C4	Practice	3	L3-1 Marking CUI media should be required at the lowest level in which organization will receive, handle or develop CUI. Difficult to protect what is not known.	Recommend making this a requirement at the lowest level in which an organization will be allowed to handle CUI. Based on other requirements, I would push down to L1.
243	NDIA	S	34	PS	C1	Practices	1	L1-1 Ad-hoc screening is a bad practice and should not be acceptable at any level. It will dis-incentivize any screening.	Recommend replacing L1-1 with L2-1. Alternatively, if to contentious at least make it mandatory screening for folks that have privileged access.
244	NDIA	S	34	PS	C2	Practices	1	L1-1 If CUI is being handled at this level then it should not be at an Ad Hoc manner, it should be mandatory for all personnel with access to CUI.	Recommend replacing L1-1 with L2-1.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
245	NDIA	S	37	PP	C4	Practices	1	L1-1 Without supporting requirements in C1, C2, C3 this requirement will be difficult to implement. How can you protect what hasn't been identified?	Recommend adding supporting requirements in C1, C2, and C3.
246	NDIA	S	37	PP	C4	Practices	3	L3-1 Unclear how this requirement is not satisfied by requirement lower requirements.	Recommend removing or collapsing into other requirements. Alternatively, clarifying the specific requirements for Alt sites that would not be part of lower requirements.
247	NDIA	S	41	RM	C2	Practices	2	L2-1 Needs supporting requirements at C1 level. Cannot record what has not been determined to be a risk category first.	Recommend adding requirement at C1 L2.
248	NDIA	S	41	RM	C2	Practices	2	L2-1 Would be a good candidate to collapse into either C1 or C3; assuming no other requirements will be added to C2.	Recommend removing C2 and moving L2-1 to C1 or C3.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
249	NDIA	A	42	RM	C3	Practices	4	L4-4 Typo. Should be a plural.	Recommend changing to “Scans are performed”
250	NDIA	A	42	RM	C4	Practices	4	L4-1 Think “external service providers is used” should be “external service providers are used”	Recommend changing word.
251	NDIA	S	43	RM	C5	Practices	4	L4-3 GRC Cyber practice should be part of L3 organization at least in a basic form. GRC Cyber requirements at L3 level would need clarity as well.	Recommend moving down to L3, even if at an introductory level. Set basic requirements for GRC Cyber.
252	NDIA	S	43	RM	C5	Practices	4	L4-4 management of non-vendor supported products should be a capability available in an L3 organization.	Recommend moving down to L3 level.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
253	NDIA	S	43	RM	C6	Practices	4	L4-1 Basic supply chain management should be supportable at L3.	Recommend moving down to L3 level.
254	NDIA	S	43	RM	C6	Practices	4	L4-3 Basic supply chain management plan should be supportable at L3.	Recommend moving down to L3 level.
255	NDIA	A	45	SAS	C1	Practices	4	L4-2 is there an associated reference for this requirement?	Please provide reference or amplifying information.
256	NDIA	S	45	SAS	C5	Practices	2	L2-1 The resources for control testing across the organization are likely to be burdensome at L2.	Recommend that this be moved to L3 or the requirements be tailored back for an L2 org.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
257	NDIA	S	45	SAS	C5	Practices	4	L4-3 advanced adversarial assessments should be reserved for advanced level organization at L5. Maybe internal adversarial testing or tabletops would me more appropriate at proactive org level.	Recommend moving up to L5.
258	NDIA	S	48	SA	C2	Practices	1	L1-1 Without supporting requirements in other capabilities, this requirement has little value. Unlikely that the skillset and resources at this level would make cyber threat intelligence very actionable.	Recommend removing this requirement from L1.
259	NDIA	S	49	SA	C4	Practices	1	L1-1 Unlikely that skillset and resource exist at this level to collect, analyze, and communicate threat information.	Recommend moving up to L3 or above.
260	NDIA	S	49	SA	C4	Practices	1	L1-1. C3 does not require organization to identify stakeholders until L3-2, So hard to understand how C4 L1-1 can communicate to stakeholders that have not been identified.	Recommend that C4 L1-1 be moved up to higher level. Identification of stakeholders must happen before notification/communication can occur.

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
261	NDIA	S	51	SCP	C1	Practices	4	L4-5 is there an associated reference for this requirement?	Please provide reference or amplifying information.
262	NDIA	A	51	SCP	C1	Practices	4	L4-2 Reference is listed as enhancement of NIST, where other references use NIST SP 800-171B 3.13.3e to illustrate enhancement.	Recommend clarifying if L4-2 reference is NIST 800-171B or if there is some other kind of enhancement document.
263	NDIA	A	57	SII	C5	Practices	4	L4-2 Typo. “attachments all emails” should be “attachments in all emails”	Recommend making changes.