MITRE's Response to the DoD RFI on Cybersecurity Maturity Model Certification

February 26, 2024

For additional information about this response, please contact:

Duane Blackburn
Center for Data-Driven Policy
The MITRE Corporation
7596 Colshire Drive
McLean, VA 22102-7539

policy@mitre.org
(434) 964-5023

About MITRE

MITRE is a not-for-profit company that works in the public interest to tackle difficult problems that challenge the safety, stability, security, and well-being of our nation. We operate multiple federally funded research and development centers (FFRDCs), participate in public-private partnerships across national security and civilian agency missions, and maintain an independent technology research program in areas such as artificial intelligence, intuitive data science, quantum information science, health informatics, policy and economic expertise, trustworthy autonomy, cyber threat sharing, and cyber resilience. MITRE's ~10,000 employees work in the public interest to solve problems for a safer world, with scientific integrity being fundamental to our existence. We are prohibited from lobbying, do not develop or sell products, have no owners or shareholders, and do not compete with industry—allowing MITRE's efforts to be truly objective and data driven. Our multidisciplinary teams (including engineers, scientists, data analysts, organizational change specialists, policy professionals, and more) are thus free to dig into problems from all angles, with no political or commercial pressures to influence our decision making, technical findings, or policy recommendations.

MITRE has an extensive history of working with the National Institute of Standards and Technology (NIST) to establish federal guidelines and industry best practices. For example, MITRE worked with NIST to develop the 800-171 and 800-172 requirements. These documents serve as the cornerstone of the larger effort to define the core set of controls the Defense Industrial Base (DIB) will need to meet to ensure the security of Controlled Unclassified Information (CUI). When Congress identified the need for additional steps to protect CUI against foreign actors, MITRE worked with the Department of Defense (DoD) to provide guidance on what would become Cybersecurity Maturity Model Certification (CMMC) 1.0, and later on CMMC 2.0.

MITRE is an active proponent of the DoD's cyber security initiatives and acknowledges the need for the DIB to play its role in bolstering its security controls. However, we also understand the unique challenges posed to the DIB in implementing 800-171 controls and meeting the requirements of the CMMC program. As an FFRDC, MITRE is an active participant in the DIB and subject to the provisions of 800-171 and CMMC. MITRE participates in a variety of forums, exchanging ideas with peers and interacting with the DoD to request clarifications and provide feedback. MITRE's enterprise and lab environments have undergone control assessments from multiple government entities, covering a variety of control frameworks and customized assessment methodologies. This puts MITRE in a unique position to understand the challenges the industry will face in trying to attain CMMC certifications.

Comments on the Proposed Rule

High-Level Comments on CMMC

Necessity of CMMC – The CMMC program is in the best long-term interests of the DoD, the DIB, and the nation. In-person, independent audits are a fundamental necessity for ensuring implementation of contractual requirements laid out in Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012. The number and nature of intrusions by third

parties since 2017 demonstrate that contractual requirements coupled with self-assessments are not an effective deterrent. Many, if not all, of the attacks have been linked to or exacerbated by the failure to implement fundamental controls required by 800-171. The need to validate controls via in-person assessments has been sufficiently demonstrated, to the point where it is no longer a subject for debate. The CMMC model facilitates assessing the DIB without excessive DoD resources, and is designed in such a way as to scale with the number of DIB contractors and the sensitivity of the CUI information they possess. While there will surely be growing pains as the model is implemented, it is the only viable long-term solution to ensure controls are in place to secure the DIB.

Impact of CMMC to DIB Ecosystem – The DoD needs to have a plan to track the status of the DIB and be prepared to make quick changes to the program to accommodate unintended outcomes of the process. MITRE is concerned about the potential impact to the DIB based on the limited ability to use Plan of Action and Milestones (POAMs) and waivers. The costs to implement controls are substantially underestimated by the DoD's accounting practices, both in terms of money spent on products to achieve solutions and in terms of personnel resources required to assess, implement, and maintain them. Assessments are a substantial undertaking as well, with pre-assessments likely to be mandatory to even assess the current state. These costs will fundamentally change the nature of DoD work, limiting the number of contractors who are capable of bidding on government contracts. Initial evidence of compliance rates based on recent DoD assessments indicates that *very few* contractors are likely to pass an initial CMMC assessment, further limiting the number of contractors who will be available to bid on early CMMC-required government contracts. The use of 800-171A changes the nature of how assessments are performed, and the methodology will generate a significant number of failures for any contractor who has not been assessed previously. There is a very real possibility that this will create significant issues, with the DoD unable to find certified contractors to qualify for work. DoD will pay escalating prices to have work completed, and some work may go uncompleted while contractors strive to receive a certification. MITRE recommends that DoD describe its plans to address this possibility. Could the rules for POAMs be loosened? Could certain controls with high failure rates be abandoned? Could the score for approval be lowered based on evidence of sufficient mitigation?

Future Changes to Control Requirements – The DoD needs to define a process for how requirements will be added or modified over the long term, such that contractors can work toward adopting new controls within reasonable periods of time to facilitate successful implementation and certification. MITRE is concerned about how changes to the list of underlying NIST SP 800-171/172 requirements will be handled. While it is necessary for security controls to be continuously updated due to new and emerging threats, constant changes to those controls will undermine the DIB's ability to keep up with compliance expectations. Many controls will require new products to be purchased or significant changes to be made to existing business processes, as well as require new training for assessors. While basing the CMMC program on NIST SP 800-171 was an initial benefit, there is no process described for how future changes or additions to CMMC will be handled and synced with documents like 800-171 and 800-53. This is already a significant concern, as NIST SP 800-171 is publishing a Revision 3 with new and re-written controls, and NIST 800-53 has adopted a continuous change model where new controls can be added at any time. It is entirely possible that there will be a period of time in which MITRE will be responsible for maintaining CMMC compliance against

800-171 Revision 2, while also being contractually required to meet Revision 3 and have contracts with other government agencies asking for their own compliance requirements (e.g., 800-171 Revision 3 with non-DoD ODPs, 800-53, etc.).

Additional General Comments

Standardization of Levels and Reduction in Requirements – Ongoing changes can stress the model. MITRE views the simplification of the model from five levels to three to be a positive change. Levels 2 and 4 of the original model served only to track progress to the next level and lacked assessment criteria. Similarly, the removal from the model of custom requirements that were outside the scope of 800-171 and 800-172 drastically improves CMMC's compatibility with NIST requirements, streamlining the way contractors can treat compliance. The existing levels and linkage to the Federal Acquisition Regulation (FAR) requirements, 800-171, and 800-172 are a solid foundation for the CMMC program and an appropriate basis on which to establish compliance expectations for the DIB. A degree of caution is warranted, however, as ongoing changes to 800-53 and 800-171 are likely to put stress on Levels 2 and 3 of the model.

Third-Party Assessments – The use of third-party assessors as part of the certification process should be effective in meeting the goals of the program. The third-party assessor program outlined within CMMC is a reasonable way to address the existing gap in qualified DoD assessors. The DoD and the CMMC Accreditation Body will need to ensure that a) all controls are assessed in a reasonably consistent manner; b) special arrangements do not infringe on the integrity of the assessments; c) costs are kept reasonably in line to allow sufficient numbers of contractors to afford assessments; and d) enough assessors are available to schedule assessments, including POAM close-out assessments, in a reasonable timeframe before a certification is needed.

POAMs Allowed – DoD needs to seriously evaluate how it could facilitate authorizing mitigated security controls, security controls that are being actively implemented, and controls that do not align perfectly with the 800-171A audit methodology. Allowing some NIST SP 800-171 security requirements to be addressed through POAM is a valuable addition to the program. POAMs introduce flexibility that will allow a company that is "close" to obtain a time-limited conditional certificate. Without this flexibility, it is unlikely that many companies would meet the requirements for certification on initial assessment. The DoD should continue to expand the POAM capability to facilitate contractors who are making a genuine attempt to meet and mitigate information security risks.

NOTE: CMMC's 100% compliance posture is not consistent with traditional government information security and risk management practices. Within the government, the Risk Management Framework (RMF) process allows non-compliance with government standards to be accepted as part of a risk approval by the authorizing party via an Authority to Operate (ATO). CMMC's requirement for a) 100% compliance with 800-171 and b) the added use of 800-171A as an audit framework presents an incredibly high bar for contractors to meet. The limitation on POAMs further raises the bar. It is understandable that DoD would see these controls as already being required by contracts, and that those contractors have already established a poor track record of enforcement. But this undersells the difficulty of meeting 800-171, especially if the contractor has never had their controls audited before.

DoD Waivers Allowed – DoD should develop its own set of criteria for when these types of waivers are appropriate, closely monitor the use of them, and (when possible) provide access to environments where contractors could perform and store work on DoD systems that are approved for this type of work. This could include providing compliant environments on a per-account fee basis, which could be particularly beneficial for smaller vendors. This approach would cover many use cases and could potentially reduce the burden of compliance for these vendors. The decision to allow the DoD to waive the certification requirements for a small subset of contracts is a potential benefit to the program. While this should be used very infrequently, it may be necessary for critical acquisitions to delay or even waive the requirements.

Reciprocity – The value of the CMMC program would be significantly enhanced if having a CMMC certification could facilitate the sharing of sensitive information both domestically and internationally, providing a yard stick by which companies and governments could effectively evaluate each other's controls. A method must be in place to establish norms across government agencies, industry, and foreign countries. The fundamental security controls necessary for protecting sensitive information should not vary significantly, and by extension the assessment mechanisms for those controls should provide sufficient confidence to establish a basis for sharing information between organizations. The DoD's decision to rely on 100% compliance with security controls will limit opportunities for establishing 1:1 reciprocity with other assessment mechanisms. However, it could develop a process by which a CMMC-certified contractor could reasonably establish how it can share information with other organizations with similar certifications. Additionally, the DoD should continuously work with standards bodies (e.g., NIST, CISA) and external parties to eliminate differences in security expectations between government agencies, industry, and foreign governments. A CMMC certification should suffice for more than just protecting DoD CUI, and non-CMMC certifications should provide a baseline from which a CMMC-certified company can evaluate information-sharing options.

Document-Specific Issues for Consideration

Specific issues for consideration:

1. CMMC Level 2 Self-Assessment (170.3.e.1, p. 164 and 170.16.a.1.ii-iii, p. 203)
    a. Comment: The document does not explain why a Level 2 Self-Assessment would be needed. Self-assessments do not make sense to address the need for validation of CMMC requirements. Self-assessments have proved to be unreliable in establishing that controls are in place, minimizing the value of assigning all 110 controls. The significant time and cost savings from self-assessments would also create a dramatic competitive advantage for any contractor receiving them. This would create opportunities for misuse of the designation for Level 2 Self-Assessments, causing contractors who go through the certification process to question the value of their commitment to the program. If the DoD believes that contractors with certain types of information should not need to undergo the burden of CMMC Level 2 certification, it should find a way to identify information as not being CUI (e.g., Federal Contract Information [FCI]) or it should consider creating a new category of information that sits between CUI and FCI.

b. Recommendation: Remove references to Level 2 Self-Assessments. If the DoD believes that some CUI should be handled in a way other than full Level 2 CMMC Third Party Assessment Organization (C3PAO) assessments, it should either change the DoD CUI program to create a class of CUI that can be handled differently or find a way to allow CUI to be treated as FCI for the purpose of information protection.

2. External Service Providers (ESPs) Needing CMMC Certifications (170.19.c2, p. 220)

   a. Comment: The rule states that ESPs (which include cloud service providers [CSPs], managed service providers [MSPs], and managed security service providers [MSSPs]) that have access to a company's CUI must have their own CMMC L2 or L3 certification. This is new in this version of the rule, and introduces several intentional or non-intentional consequences:

      1) The number of C3PAOs and assessors is not planned to accommodate this extra assessment load.

      2) It is unlikely that ESPs are aware that this would be in the rule. While the DoD has been communicating with the DIB on the CMMC rule, the DoD has not focused on communicating with ESPs.

      3) Costs to the DIB for using ESPs will increase.

         a) Note that most MSPs and MSSPs are themselves small companies. They will be subject to considerable burden if they need to be assessed. They are not planning for the cost and resources for this requirement.

         b) If ESPs need to absorb the cost of becoming compliant, they will need to raise their costs, possibly making their services and offerings too expensive for the companies they currently support, including DIB small and medium-sized businesses (SMBs).

   b. Recommendation: Whether CUI is present or not, MSPs and MSSPs should be required to use only secure connections when connecting to a DIB company.

3. Senior Official Affirmations (1.c, 2.c, 3.c, 170.22, p. 226)

   a. Comment: The term "Organization Seeking Assessment (OSA) senior official" is not defined. The variety of roles that might be identified for this requirement is significant. Given that this person will be a likely target for False Claims Act actions, it should be clear who should be identified within the organization to fill this role. Additionally, while acknowledging that company executives should be aware of assertions of compliance, it would be unwieldy for senior executives to be the individuals entering the data into the Supplier Performance Risk System (SPRS). Trying to arrange for senior executives to understand all the requirements, understand the full breadth of the company's compliance program, and agree to sign is a challenging process that can take weeks in larger organizations. Trying to get this executive access to SPRS, then having them go into SPRS to document the information, is not a reasonable expectation at larger companies.

   b. Recommendation: Allow the contractor to capture the affirmation in a separate document, to be submitted with the SPRS score. The name of the executive could be

entered into SPRS for reference. "OSA senior official" should be defined in Section 170.4.

4. CMMC Document Organization
    a. Comment: The document is 234 pages long, and it is very difficult to parse out the important details. While context can be very helpful in understanding how the policy was developed, the way it was incorporated into this document will limit the number of people reviewing the language and providing comments to the parts that are critically important for both the DoD and the DIB. Some of the issues with the document's format include:
        1) Lack of a table of contents highlighting where important concepts can be found
        2) Lack of an index of critical ideas showing where topics are referenced across different sections
        3) Lack of page numbers
        4) Indentation methodology in which only one level of indentation exists, making it hard to determine when ideas are tied to one another
        5) Multiple pages of "incorporation by reference" terms that are not relevant to the final policy
        6) Inclusion of user comments that are not relevant to the final policy
        7) Two separate "Background" sections, neither of which is relevant to the final policy
    b. Recommendation: The length of the document and lack of effective document organization limited the number of readers within MITRE who could commit to evaluating the language. While additional time to evaluate the policy language is unlikely to happen at this point, the DoD (or perhaps the Office of Management and Budget [OMB]) should evaluate how future policy language is written and focus on separating the actual proposed policy from the background/context that led to the creation of the draft. While there is a need to document the background for programs like CMMC that will have a substantial impact on the industry, the main emphasis of the proposed rule should be on the specific details and implications of the rule itself. This will help ensure that reviewers are given maximum opportunity to focus on the specific rules and provide appropriate feedback.
5. 800-171A and Cost Estimates (pp. 95–96)
    a. Comment: The following content is from p. 95:

        DoD did not consider the cost of implementing the security requirements themselves because implementation is already required by FAR clause 52.204-21, effective June 15, 2016, and by DFARS clause 252.204-7012, requiring implementation by Dec. 31, 2017, respectively; therefore, the costs of implementing the security requirements for CMMC Levels 1 and 2 should already have been incurred and are not attributed to this rule.

Compliance with 800-171 was required by December 31, 2017. That said, costs were never re-evaluated for compliance with 800-171A, which CMMC now requires. Given the number of individual objectives in 800-171A, establishing a compliance program is considerably more challenging, let alone modifying solutions to ensure they address every individual objective. It cannot be stressed enough how 800-171A changes the nature of the program originally developed by the DoD and the DIB back in 2015. Instead of focusing on the intent of the control, 800-171A puts the emphasis on the processes and documentation needed to formalize the control over the long term. While certainly a best practice, the level of maturity to establish these controls takes years to develop and carries a significant operational cost. Focusing assessments on these maturity aspects over the functional intent and implementation of the controls was a significant expansion of the requirements for contractors, and was never factored into the costs to implement the controls themselves.

b. Recommendation: Acknowledge that CMMC's reliance on 800-171A has changed the cost to comply with controls. At a minimum, it has increased the standard cost of managing compliance by tripling the number of items that need to be tracked to prepare for an assessment. In practice, the processes/technologies needed to ensure compliance with the 800-171A objectives do increase the cost above and beyond what was originally needed for 800-171. The DoD needs to monitor CMMC assessment rates, paying special attention to how many of the failures are related to implementing the intent of the control versus those tied to specific aspects of documenting the control.

6. Scoring Requirements (170.24)

   a. Comment: While the option to have partially met scoring requirements for Federal Information Processing Standard (FIPS) and multi-factor authentication (MFA) does offer some respite for those who will need POAMs to complete them, this adds significant complexity to what is already a fairly complex scoring process. The complexity offered some value when DIB contractors were creating self-assessments for SPRS and the self-assessment score helped portray general levels of compliance risk. Now that 100% compliance will be required for certification, that complexity is no longer valuable, and changing the model to make each requirement worth 1 point would significantly simplify the language.

   b. Recommendation: Remove the rules for 1-, 3-, and 5-point values, and make each question worth 1 point. Change the base score for the assessment to the number met divided by the number of controls, resulting in a percentage of controls met. The CMMC program can still emphasize the differing levels of risk associated with each control, but removing these risk levels from the formal scoring methodology will simplify the process for thousands of contractors.

7. Availability of CMMC Third-Party Assessment Organizations and Trained Assessors for Assessments (Impact and Cost Analysis of CMMC 2.0, p. 91)

   a. Comment: The document says:

      In addition, the CMMC Program relies upon free market influences of supply and demand to propel implementation. Specifically, the Department does not

> *control which defense contractors aspire to compete for which business opportunities, nor does it control access to the assessment services offered by C3PAOs. OSAs may elect to complete a self-assessment or pursue a certification assessment at any time after issuance of the rule, in an effort to distinguish themselves as competitive for efforts that require an ability to adequately protect CUI. For that reason, the number of CMMC assessments for unique entities per level per year may vary significantly from the assumptions used in generating the cost estimate.*

The notion that the DoD is not responsible for the market forces of supply and demand is problematic. If the DoD's program implementation leads to a limited number of certified contractors due to high failure rates or insufficient assessors, this could inadvertently shrink the market for DoD contractors. Furthermore, if companies without an immediate need for CMMC seek assessments on Day 1 to gain a competitive edge, this could limit assessment opportunities for other companies that require the assessment to bid on upcoming contracts. The rush to process numerous assessments in a short timeframe could also potentially compromise the quality of initial assessments. While there is a pressing need to establish third-party assessors swiftly, the DoD plays a crucial role in managing the assessment process and ensuring its flexibility to accommodate a sufficient number of qualified contractors to carry out the necessary work.

b. Recommendation: Remove the comment about "distinguish(ing) themselves as competitive." Furthermore, the DoD should have plans to address contracts for which the inability to obtain a timely assessment becomes an impediment to bidding. This is even more important when it is the first assessment that the contractor will receive, because having minimal, fixable failures should not be a strong impediment to being able to work with CUI. Addressing these issues may require expansion of POAMs and changes to the assessment process, especially in the initial stages of implementation.

8. CMMC Level 3 Requirements (170.14, pp. 195–199)

a. Comment: Table 1 to § 170.14(c)(4) identifies 24 security requirements and applicable ODPs selected from NIST SP 800-172 to represent CMMC Level 3 requirements. The following 800-172 security requirement is *not* included among them:

> ***SC L3-3.13.3.e** Employ techniques to confuse and mislead adversaries*

In defining CMMC Level 3, is important to consider that 800-172 references NIST SP 800-160-2 for guidance on developing cyber-resilient systems and system components, specifically regarding SC L3-3.13.3.e. NIST SP 800-160-2 defines "cyber resiliency" as more than simply recovering from attacks—it involves anticipating and withstanding them, as well as evolving systems and practices to address future needs and emerging threats. Specifically, 800-160-2 states:

> *Twelve of the 14 cyber resiliency techniques can be applied to adversarial or non-adversarial threats (including cyber-related and non-cyber-related*

threats). The cyber resiliency techniques specific to adversarial threats are Deception and Unpredictability.

Based on more than 10 years of research and operational experience, MITRE observes adversary engagement[1] (the combination of cyber denial and deception with strategic planning and analysis) and unpredictability as crucial to addressing advanced threats. Adversary engagement, informed by threat intelligence, enables:

1) More rapid detection of threat activities (and prevention where possible) so that resources can be redeployed and safeguards (to detect as well as to prevent attacks) put in place
2) Minimization of the effects of threat activities on critical operations
3) More effective recovery efforts, because they can focus threat targets and on resources adversaries seek to infiltrate or corrupt
4) Evolution of systems and practices to be better aligned to changes in the threat landscape
5) Lowering the value while increasing the costs of malicious operations

b. Recommendation: Include ***SC L3-3.13.3.e*** *Employ techniques to confuse and mislead adversaries* among the requirements for CMMC Level 3 listed in Table 1 to § 170.14(c)(4).

9. Plan of Action and Milestone Terminology (170.21, p. 224)
   a. Comment: In part (a), the rule indicates that there are two types of POAMs: those that will be part of a contractor's regular risk assessment process and those that will be part of a contractor's attempt to pass a CMMC assessment. The overlapping terminology creates problems when DIB contractors start trying to determine whether a particular POAM is valid. For example, a POAM may be valid within the contractor's risk system due to an individual, isolated, or temporary deficiency, but the CMMC requirement for the same control would not allow POAMs due to how many points the control is worth.
   b. Recommendation: DoD should consider using different terminology to describe the action plans generated for items deemed Not Met during a CMMC assessment. Use of the term "POAM" should be avoided so as not to raise confusion with terminology used within a contractor's standard risk program.
10. FIPS (170.24, p. 230)
    a. Comment: FIPS has been addressed by the DIB as a compliance problem for a decade, and there is evidence that up to 50% of assessments could fail due to FIPS alone. Despite this, FIPS continues to be a staple of 800-171 and now CMMC. While the goal of validating cryptographic algorithms and implementations is an important

[1] NIST SP 800-172 and other NIST documents typically use the term "cyber deception" rather than "adversary engagement" to refer to these activities. MITRE Engage prefers the term "adversary engagement" to avoid ambiguity with other terms, such as "military deception" or "disinformation." Adversary engagement activities, in this context, require no government authorities and are activities that private sector InfoSec teams can legally conduct within the bounds of their internal networks to protect their infrastructure and assets.

security control, the FIPS program cannot keep up with the pace of software/hardware development. This leads to minor software upgrades and vulnerability fixes creating non-compliance with the documented assessment methodology, while legacy crypto algorithms with known vulnerabilities remain valid long after they should be removed. While this has not been a significant issue with self-assessments due to the lack of knowledge among DIB contractors about how FIPS will be assessed, it is likely to become a significant issue when every company is assessed in CMMC. Enabling FIPS mode in a system or software presents additional problems, because it limits crypto options for all systems, not just those that need to be CUI compliant. There are secure cryptographic solutions that are not recognized as FIPS compliant, and companies are restricted from employing these or any applications that incorporate them when FIPS mode is enabled. Contractors who enable FIPS mode may need to establish a second set of servers that will accept non-FIPS algorithms or they may need to confine all internal applications to FIPS-compliant software, which significantly reduces flexibility in providing internal services.

b. Recommendation: Revise audit guidelines for CMMC to accommodate the limitations of the FIPS program. Allow contractors to demonstrate compliance with the intent of the control in ways that go beyond just having FIPS mode checked and a certificate in the current FIPS list. Consider removing the FIPS requirement altogether until it can allow for modern software development practices to be accounted for when establishing what constitutes failure of the control.

11. Level 2 Assets in Scope (170.19.c.1, p. 217)

    a. Comment: CMMC identifies assets falling into the "Contractor Risk Managed Assets" category and the "Specialized Assets" category in the table beginning on page 217. Although it is important to understand how these assets fit into the CMMC assessment scope, the program is somewhat vague regarding how this would happen, noting only that these items would be documented in the asset inventory, documented in the System Security Plan (SSP), and documented in the network diagram. It is not clear whether the intention here is to document each and every asset in this way or to identify that there is a category of asserts that fit the description. Including these assets in an asset inventory for the assessor to evaluate is logical, but if every asset that meets these criteria is to be embedded into the SSP, it could result in an excessively lengthy document filled with system, application, and database names. A similar issue could arise with the network diagram.

    b. Recommendation: Clarify what it means to document assets in the SSP and network diagram. If the intent is to not list the systems individually, clearly specify what level of detail needs to be documented for these assets, outside of what is already captured in the asset inventory.

12. Level 1 Assets in Level 2 Scope (170.16, p. 203)

    a. Comment: There is no clarity in the document about how Level 2 and 3 contractors would document Level 1 systems. Do they need to be included in the SSP? Do they need a documented self-assessment? Are they in scope for Level 2 assessors to review?

b. Recommendation: Given that these systems were not previously identified as being in scope for Level 2 and 3 assessments, the document should make clear that they are out of scope for Level 2 and 3 assessors. If additional documentation needs to be maintained, the document should outline what is expected of the contractor for compliance.