NDIA Cyber Legal Policy Committee

Notes of 9/6/19 Teleconference re Potential CMMC Comments

1. Meeting convened

Present on the call were Susan Ebner (Stinson), Sandeep Kathuria (NGC), Corbin Evans (NDIA), Dave Chesebrough (NDIA), Bob Huffman (Akin Gump), Chris Haile (Raytheon), Joel Landau (Aerojet-Rocketdyne), John Nell (Nell 360), Mike Pierson (SAIC), John Smith (Raytheon), Rolando Sanchez (Rolando Sanchez LLC), Hartmann Young (GE), Bob Metzger (RJO), Alicia Lynch (SAIC), Brian Dobbs (SAIC), Sam Moorthland (SeraBrynne), Sam Singer (Boeing). Maureen Kelly (NGC).

2. NDIA will be hosting two meetings on cybersecurity developments in Tampa – one of 9/11/19 (Sam Moorthland will participate) and a second one on 11/13/19 (Katie Arrington will participate re CMMC).

3. CMMC Draft Out for Comments

DOD released initial draft version of the CMMC maturity model for comment. Comments are due to be submitted by September 25, 2019. NDIA's Corbin Evans will coordinate comments received from various NDIA Divisions and Committees. Corbin will be reconciler of comments and clean up language; sanitize for commenter and company so that the ultimate comment will be a purely NDIA product.

1. DOD has provided a comment matrix for comments on the various technical aspects of the draft.
2. It was determined that the best way to address draft was in two parts – 1) letter to be prepared to address NDIA's comments on CMMC draft overall, overarching questions and issues with the CMMC draft, and summary of comments on the technical aspects, and 2) individual comments on the specific CMMC draft modules, processes, practices identified to be furnished in bulleted form wtihin the matrix provided by DOD.
3. Those participating in the comment process were asked to go back to their firms/companies and technical personnel to identify comments on the specifics of the draft CMMC and to furnish them in para or bullet form.
4. It was agreed that we need to seek and get comments from as many divisions as possible. It will help the process if we can get input from individual companies – what they think of the requirements and their thoughts on the ability to achieve the process/procedures identified. It also will be valuable to provide legal input. Core is having companies consider the level they would seek to attain.
5. The CMMC has a huge leap in requirements for levels 4 and 5. CMMC contemplates that a small set of companies will be asked to complete and meet level 5 requirements as these are quite demanding. However, it is perceived at least at this point that level 4 will be the hardest to achieve – there is a lot in there and it requires more than NIST SP 800-171 and NIST SP 800-53, it contains new processes and procedures. Critical that CISO and cyber counsel for a company assess if the company can do it and when.
6. Assignments, Schedule and Points for potential comments
   1. Assignments
      1. Overaching comments /major themes – Susan, Sandeep
      2. Technical comments on individual controls
         1. Individual groups to go through controls [need more technical folks]
         2. Assemblies by level – [get inputs from clients to see if capable of doing different levels, e.g. DIB supply chain can it do level 3]
         3. Level 1 and 2 comments, how affect them – Rolando, Nell, Morthland
         4. Level 3 – Alicia Lynch team, Hartmann Young, Morthland
         5. Level 4 and 5 - Huffman, Maureen, Chris Haile, Morthland
   2. Schedule
      1. Circulate notes from call – 9/10
      2. Groups above to provide initial draft bullet points for technical and big pictures – 9/15
      3. Bullet points to be combined and circulated to the group at large, for input and comments on techical and big picture points – 9/18
      4. Once draft is circulated and input received, Group to schedule call to discuss to determine any further comments/input
      5. Draft to be revised based on any further input and provided to Corbin for integration into NDIA comments to be submitted 9/25.
      6. Each piece should to go to Susan for her to combine and circulate
   3. Discussion points during call
      1. The draft CMMC level 1 does not identify whether all existing controls in NIST SP 800-171 are to be complied with.
      2. Number of controls in CMMC are not in standard, they identify a variety of sources, e.g., DIB members, CMU and JHU.
      3. Draft focuses on having a process in place vs. actuall meeting the requirements. Is it becoming more of a "check the box" for the audit guide? Shouldn’t it be more than just a checklist?
      4. Traditionally the military gives out a basic instruction and then individual activities and organizations issue more restrictive instructions. The CMMC has a number of "individual" activity/organization type comments – beyond NIST SP 800-171. Shouldn’t these be taken out of the CMMC and put in an addendum for the specific activity/organization. Wasn’t the point of CMMC to get away from agency by agency requirements?
      5. The draft does not address how the CMMC will be implemented through Sections L and M of future procurements. How does the DOD intend to implement this? It is a lot of controls and new stuff. Given that there are a lot of new controls, processes, requirements, it would help in evaluating the draft CMMC and putting together comments to see how DOD intends to implement this.
      6. For example, does DOD intend to implement the level requirements for the "program level" and have those reuqirements apply to all tiers, or does DOD intend to allow contractors to have the ability to establish different levels that the different lower tier subcontractors in the supply chain will be doing? How will this work?
      7. Katie Arrington in her listening tours has said that Sections L and M will chunk out which levels are required for particular tasks so primes can partner with subs at the lower levels, e.g., for a particular program/procurement the contractor engaged in manufacture will require x level, but for lower level tiers, the contractor will require a lower level of compliance.
      8. We have had the DFARS clause since 2015 and we are still struggling with having the govt identify CDI. How is this going to be handled?
      9. The UK model has handled things differently – when it rolled out its requirements it did not require implementation of all controls; it rolled them out to certain levels.
      10. Implementation issues – several requirements in levels 1 and 2 require that contractors protect CUI. Will level 1 be required of all contractors, what of Level 3?
      11. The CMMC FAQ website provides that the contractor needs to be certified even if no CUI data. Levels of certification appear to be tied to the particular work/what have. How is this going to be reconciled?
      12. The draft contains more requirements at level 3 than are in the NIST SP 800-171 – it refers to DIB, CIS, RMM [resilence management model – a component of CMU, etc. Was this intended?
      13. DFARS 252.204-7012 called for contractors to provide "adequate security", the CMMC refers to "building upon" NIST SP 800-171, does this mean that DOD is interpreting adequate security to be something more than what is contained in NIST SP 800-171?
      14. Why is DOD using levels to establish cybersecurity requirements in draft CMMC when this is not in the DFARS? Will DOD amend the DFARS clause?
      15. If DOD's authority to issue the draft CMMC is DFARS 252.204-7012, how can DOD impose cyber requirements on folks that don’t get CUI? Does govt take the position that everyone has to have this level of compliance even if the Govt has not furnished any CUI because the contractor has its own CUI?
      16. Will DOD require that some sort of CMMC certification be required for any one that receives CDI?
      17. The template provided for comments does not afford comments on the grand strategy. However, how is DOD going to handle the costs of implementation and compliance for the contractor?
      18. Comments on the controls themselves – would the controls differ based on the scope of the activities of the individual contractor/vendor? E.g., is the intent to do source code reviews for all vendors? Or does it depend on who you are giving it to and what it is being used for?
      19. What freedom will the contractor have re flowdown? Shouldn’t the prime have ability to make risk-informed judgments? Is CMMC requiring that contractors inform the govt. of the individual levels required foor their suppliers? Is it requiring them to provide notice and receive consent?
      20. Under the CMMC, how will DOD handle / treat contractor updates to certified CMMC systems? Will it apply the current CPSR model – requiring new certification prior to implementation of any updates?
      21. What will be the role of the third party auditors? How will the DOD ensure consistent evaluations by these various external auditors?
      22. How will DOD handle situations where it finds a contractor system is not compliant?
      23. Will a contractor be afforded a safe harbor if it was certified as having a compliance system and then a breach occurred? What consequences will a contractor have to face?
      24. Add in compliance and enforcement questions
      25. The CMMS lists practices and processes. However, the processes are written more vaguely. How are they going to be addressed? If a contractor meets all practices but doesn’t satisfy the assessor that it has all processes, will you still determine the contractor to be compliant with the designated level for procurement purposes? What is the meaning of these different aspects of CMMC [see, e.g., slide 11 of the CMMC briefing]
      26. The CMMC provides for practices that are implemented "ad hoc" and that are "institutionalized" for different levels, what does this really mean? Could a contractor have all processes, but not have a policy thath has been institutionalized? Can DOD better define what is expected for policies and what credit or deference should be given to good policies? If look at way CMMC has been structured – at the end of domain, it refers to maturity capability. Will the audit determine if policies and procedures exists, and then get to maturity capability to see if the contractor has the processes and practices.
      27. CMMC draft does not use precise wording, how will this be implemented?
      28. Slides put out are very vague. How can we undersatnd what is really meant? Will more documentation be drafted?
      29. On the CMMC website, the speaking tour slides are no longer posted so one cannot see the details originally posited for CMMC, what does this mean? Need more on implementation.
      30. What if existing program vendors cannot meet the levels required for a particular program – if a vendor can't meet that requirement, how can it continue do the program?
      31. Long ongoing programs with sole source providers, how will CMMC be implemented for them? Will CMMC focus on new starts and new programs and not existing programs? Will it start only with RFI, RFP for new programs?
      32. The CMMC does not address cloud services. We have heard DOD discuss and encourage contractors to use the cloud to address security concerns. How does going to the cloud impact the analysis of this and compliance under CMMC?