COSMOS
Navigate the Compliance Universe

CEP Magazine - June 2024

Janet Himmelreich (janet.himmelreich@3comply.com, linkedin.com/in/janethimmelreichgrcexpert/) is a Managing Director of 3Comply LLC in King of Prussia, Pennsylvania, USA.

Are you an ostrich? For CMMC, you'd best be a roadrunner

By Janet Himmelreich, CIPP/E/US, CMMC RA, RPA, formerly CCEP

In the last issue, we discussed the fuss around the Cybersecurity Maturity Model Certification (CMMC).[1] Although the final regulations have recently been published establishing the CMMC validation program as a formal "program" for the U.S. Department of Defense (DoD), the long of it—it's been discussed since 2017—and the short of it—the effective date of the final rules is expected in Q1 2025—is now reality.[2] Many people had taken the position they would believe it when they see it. Well, here it is.

CMMC is designed to validate that the controls of NIST SP 800-171 Rev. 2 have been implemented.[3] An independent assessment demonstrates that the controls are implemented correctly, operating as intended, and that the required outcome can be evidenced. This validation is necessary for contracting with the DoD but also helps companies protect their intellectual property for any business operations. All supply chains are under attack from cybercriminals, and the safer your information and data are, the better off you will be.

Many companies in the defense industrial base preferred that security achievements— particularly ISO 27001 certification and/or SOC 2 attestation—be used in place of CMMC validation. These activities are considered significantly different by the DoD and, thus, are not acceptable. However, the good news is if you have achieved either or both, your environment is significantly advanced relative to a company with no security framework compared to the controls of NIST SP 800-171. At the end of the day, any security frameworks, whether from NIST or another entity, cover people, processes, and systems—not just technology. It is key that the people involved are trained, knowledgeable of the processes and procedures, and able to demonstrate compliance to an auditor or an assessment team. As is true for any framework a company must comply with, it is *always* about the people.

Rulemaking statuses

The DoD published its final proposed rules for the *program* of CMMC on December 26, 2023. The public comment date closed on February 26, 2024, and so far, the website for collecting and reporting on the comments states that there are almost 800 comments received by the end of the first week in March.[4] Thus far, 368 comments have been made available through the docket. The next step in rulemaking is publication of the final proposed rules under 48 C.F.R. Chapter 2, which will define the *acquisition* rules that need to be refined to reflect the program as defined in 32 C.F.R. § 170.[5] DoD spokespersons said the rulesets are expected to have the same effective dates: after the 60-day comment period expected for the revised Defense Federal Acquisition Regulation Supplement (DFARS) rules when published. (The February 9, 2024, Regulatory Flex Agenda pointed to the link for weekly updates by the DoD regarding open cases).[6] As of March 8, 2024, the proposed DFARS regulations were still described as: "02/23/2024 Case manager forwarded draft proposed rule to DARS Regulatory Control

Officer. DARS Regulatory Control Officer reviewing."[7] Based on the Fall 2023 Regulatory Agenda, most pundits expected that the DFARS rules would be published in March 2024. As of April 15, 2024, the rules have not been published. This is crucial, as both pieces are needed prior to the rules going into effect.

The DoD promised a statement before the end of the comment period for 32 C.F.R. § 170; a video statement was released on February 7, 2024.[8] It seems the philosophy was that a picture is worth a thousand words. The video reiterates many of the statements found in the body of the proposed rules from December 2023, but it may make some of the requirements a bit clearer than if one were to simply follow the written mass of words.

It is worth noting that CMMC and the DFARS 254.204-7012 procurement clauses refer to NIST SP 800-171 Rev. 2, which only addresses *nonfederal* systems use. Thus, this applies to situations where the contractor provides and uses its own systems. If a contractor provides systems to the federal government that *it* uses, then these cybersecurity requirements can be found in NIST SP 800-53 Rev. 5b.[9] This is the set of requirements that drive the smaller number of requirements found in NIST SP 800-171 Rev. 2.