Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

What's Next For Cybersecurity Maturity Model Certification

By **Robert Metzger, Deborah Rodin and Eleanor Ross**
(December 21, 2020, 4:09 PM EST)

Robert Metzger

Deborah Rodin

Eleanor Ross

The U.S. Department of Defense's new cyber interim rule took effect on Nov. 30, and changes are now reflected in Defense Federal Acquisition Regulations Supplement. On the same date, the comment period for the interim rule closed.

This rule affects tens of thousands of organizations that do business with the DOD. At least 20,000 companies soon will be required to self-assess their compliance with cyber requirements and submit their assessment scores to the Pentagon.

Many more companies will find themselves subject to the new Cybersecurity Maturity Model Certification, or CMMC, program, which involves third-party assessment of cybersecurity. The DOD received more than 180 comment submittals on the CMMC interim rule.[1] This rule has generated enormous interest among government contractors and commercial organizations in the defense supply chain.

Stakeholders of all types have a keen interest in knowing what to expect as the DOD considers the comments, and proceeds to produce and promulgate the final rule. Over the same period, there will be a change in administration. Agencies are bound by very strict requirements for rulemaking. This constrains the new Biden administration's ability to make dramatic changes to the content or implementation of the CMMC interim rule.

This article provides principles for companies to bear in mind as they consider what lies ahead for the rule.

1. Changes to the interim rule are likely to proceed slowly.

On Sept. 29, the DOD released the interim rule addressing implementation of a DOD assessment methodology and the CMMC framework. Typically, an agency is required to issue a new regulation as a proposed rule with a 30- or 60-day public comment period. After considering all the comments, the agency issues a final rule with a specified effective date. Here, however, the DOD issued an interim rule, meaning it was to take effect before the notice and comment period ended.[2]

Even though the interim rule became effective on Nov. 30, the Pentagon still must conform with the statutory comment period for the final rule.[3] Each of the comments received must be assessed to determine whether they warrant changes to the rule. In the final rule, the DOD must review each of the comments — or thematic groupings of comments — and provide its response, including whether any changes were made from the interim version to the final rule to address concerns raised in the comments.

Given the volume of comments received and the possibility of changes, the process of reviewing and addressing comments could take several months. A DOD committee will be assigned to review and analyze the public comments. It is likely to take at least 12 weeks before the DOD's internal review of the comments is completed and a revised rule is drafted.

Here, it could take longer. The comments received raise a wide variety of issues, and much of the subject matter is complex. Work to complete review and action upon the comments, and prepare a final rule, will not be completed until well after the inauguration Jan. 20, 2021.

Once the DOD has approved a revised rule, the next step is review and approval by the Office of Management and Budget, which will take additional time. The OMB's Office of Information and Regulatory Affairs, or OIRA, reviews the rule to ensure that the agency has properly considered the consequences of its rulemaking and whether the rule's impact could be limited while still achieving the regulatory objectives.

OIRA also ensures that the agency has complied with its obligations under statutes and regulations. OIRA may return the CMMC rule to the DOD if it determines that the rule does not comply with legal obligations, if the DOD's impact analysis is inadequate or if the rule is not justified by the analysis.

OIRA must complete its review within 90 days. Only after OIRA has approved the final, revised CMMC rule, will it go to the Defense Acquisition Regulation System editor for publication. And it could take more weeks before the final regulation is published in the Federal Register.

Another wrinkle is that a rulemaking moratorium may be imposed as the new administration assumes power.[4] This would further retard the process toward a revised, final rule.

Organizations are subject to the new DFARS provisions implemented by the interim rule until the change process is complete.

2. The ability of the new administration to change the current interim rule is limited by the rulemaking process.

Many in the defense industrial base wonder whether the new administration will stay on the same course for the CMMC initiative and the interim rule. Some prospective policymakers have expressed serious doubts about the CMMC.[5]

The interim rule is already operative and will remain so as new leadership takes over at the Pentagon. The new administration will have limited ability to make immediate and material changes to the interim rule.

While the submitted comments on the interim rule are adjudicated within the DOD,[6] the new administration likely is constrained from making any changes outside the frame of the interim

rulemaking. New subject areas may not be added following the comment period on the interim rule, since those changes are not contemplated in the original rulemaking.[7]

The notice requirement of the Administrative Procedure Act requires that agencies provide adequate information to allow the public to understand the particular issues the agency is considering in the rule or otherwise make clear that the agency is contemplating a particular change.[8]

Accordingly, the scope and content of the final rule will be guided by the interim rule and the disposition of the public comments received. Notably, courts have recognized that a final rule with a dramatic change in content from the initial rulemaking is not a logical outgrowth of the proposed rule and fails to comply with the APA's requirement to provide adequate notice to the public.[9]

Thus, the interim rule, now effective, is likely to be applied, unchanged, for months, and possibly for much of 2021. Companies should neither assume nor expect that the new administration will act rapidly or drastically to change the rule or its application.

This is a good-news/bad-news outcome. Companies can have some confidence that work to comply now will not be for naught. But companies who seek dramatic changes or immediate relief from the interim rule's application likely will be disappointed.

3. The DOD leadership would have to engage in separate rulemaking to overhaul the approach to CMMC or stop its implementation.

As concerns the future of the CMMC rule, the most important positions to watch in the new administration include the secretary of defense, the deputy secretary of defense, the under secretary of defense for acquisition and sustainment, and the DOD chief information officer.

The president-elect has nominated retired General Lloyd Austin to be the next secretary of defense — his views on CMMC have not been made public.

It is not known who will serve in these other important posts. A few Trump administration appointees could remain in place for some months after the inauguration on Jan. 20, 2021.

Once nominees are announced for top positions, such as deputy secretary, under secretary for acquisition and sustainment, and chief information officer, U.S. Senate confirmation could take weeks, and key second and third tier positions will take even longer to fill.

While senior positions are vacant during the transition, civil service personnel holding temporary responsibility will be reluctant to make significant changes to existing policies and programs. As the interim regulation is now effective and the CMMC program is now active, they have acquired a certain incumbency status that could pose a further constraint on how much the CMMC rule can change in the coming months.

Once in place, new leadership may reconsider the direction and particulars of DOD cyber measures for the defense industrial base. It is possible the new administration will be hostile to the scope, method and costs of the interim rule and the CMMC initiative. Even so, substantial changes can be accomplished only by formal rulemaking actions, which themselves take time.

Revisions to the interim rule are likely to be pending, not complete, when new leadership is in place in

2021. The DOD can effectively suspend finalization of the rule by slowing progress internal to the DOD or even withdrawing it from OIRA's deliberations — but the interim rule will remain in place and effective.

Also possible is that the DOD would reopen the comment period and hold a public meeting — presumably virtual. However, now that the interim rule is in effect, the DOD cannot withdraw it without going through a new notice and comment period.[10] So the new administration cannot easily suspend or even withdraw the present interim rule, even if and while it contemplates major changes.[11]

Further, with the interim rule now on the books, the DOD acquisition workforce and oversight authorities are likely to implement the new DFARS provisions in accordance with their terms.

We fully expect the new administration to support measures to improve the cyber protection of the defense industrial base, even if they seek different security strategies. The CMMC final rule may be changed to address public comments received on the interim rule. Yet, the interim rule is already effective and cannot be changed materially, much less abandoned, without conformance with existing rulemaking law, policy and process.

Companies contemplating the new DFARS should bear these principles in mind. There is no reason to hesitate in taking prudent security measures which will conform with the interim rule's near-term requirements, given that it is likely to remain effective for the foreseeable future.

Robert S. Metzger is a shareholder, and Deborah Norris Rodin and Eleanor Ross are associates, at Rogers Joseph O'Donnell PC.

[1] https://www.regulations.gov/document?D=DARS-2020-0034-0001.

[2] The DoD concluded that "urgent and compelling reasons exist to promulgate this interim rule without prior opportunity for public comment." 85 Fed. Reg. 61517 (Sep. 29, 2020). The statutory authority for waiver of usually applicable "notice and comment" rules requires the agency to consider comments before it issues a final rule. 41 U.S.C. §1707(e)(2).

[3] 41 U.S.C. § 1707.

[4] When a new administration takes office, it generally implements an Executive-Branch-wide moratorium on rulemaking pending review of existing efforts. See, e.g., "Memorandum for the Heads of Executive Departments and Agencies: Regulatory Freeze Pending Review," Reince Priebus, Assistant to the President and Chief of Staff (Jan. 20, 2017), https://www.whitehouse.gov/presidential-actions/memorandum-heads-executive-departments-agencies/. Placing a hold on revising rules which are pending does not generally impact rules already in effect, since rescinding or changing the effective date of a rule is a "rule-making activity" subject to notice and comment. See 5 U.S.C. § 551(5); Nat'l Resources Defense Council v. Dep't of Energy, 355 F.3d 179 (2d Cir. 2004) (holding that new administration's effort to delay effective date of final rule was subject to the APA's notice and comment provisions).

[5] See Frank Kendall, "Cybersecurity Maturity Model Certification: An Idea Whose Time Has Not Come And Never May," Forbes, Apr. 29, 2020.

[6] See "DoD Regulatory Program: Stage/Timeline Matrix for Federal Register Issuances," at https://open.defense.gov/Regulatory-Program/Process/Timeline/.

[7] See 5 U.S.C. § 551(5); 553b (requiring adequate notice prior to rulemaking).

[8] See CSX Transp. Inc. v. Surface Transp. Bd., 584 F.3d 1076, 1081 (D.C. Cir. 2009).

[9] See Long Island Care at Home, Ltd., v. Coke, 551 U.S. 158, 174 (2007) (finding it reasonably foreseeable that the agency might choose to allow certain exemptions to its rule since the proposed rule contained a discussion of the proposed exemptions, and sustaining the final rule); Environmental Integrity Project v. EPA, 425 F.3d 992, 996 (D.C. Cir. 2005) (holding that the final rule was not the logical outgrowth of the proposed rule where the final rule included items that had not even been mentioned in the proposed rule, such that the final rule "finds no roots in the agency's proposal" and the public "would have had to divine the agency's unspoken thoughts" to know the agency was considering such a dramatic change).

[10] 5 U.S.C. § 551(5) (rulemaking includes "repealing" an already existing rule); Long Island Care at Home, Ltd., v. Coke, 551 U.S. 158, 174 (2007) (notice and comment procedures required for changes to rule outside the "logical outgrowth" of the original rule).

[11] Conceivably, a new administration might invoke existing exceptions to notice and comment, in order to accelerate suspension or withdrawal of the interim rule, but it seems dubious that a change in administration or changed policy of a new administration would constitute valid urgent and compelling circumstances.