CMMC Update

Contractors Have Brief Window To Comment on Sweeping Cybersecurity Mandate

BY JOSH LUCKENBAUGH

The Defense Department chose the day after Christmas to release its much-anticipated proposed rule to make contractors adhere to a series of cybersecurity standards.

The department's chief information officer on Dec. 26 published its proposed rule for obtaining the Cybersecurity Maturity Model Certification, or CMMC, which will eventually be required for any company doing business with the Defense Department. Contractors have until Feb. 26 to provide comments on the proposed requirements.

This is the second version of the CMMC rule, which was initially released in 2020. After widespread criticism of the first version, the Defense Department kicked off CMMC 2.0 in November 2021. Refining those rules took two years and one month. The program will require contractors to comply with a list of cybersecurity requirements to prevent theft or electronic espionage of federal contract information and controlled unclassified information, or CUI.

Eric Noonan, CEO of CyberSheath, noted that many of the cybersecurity requirements themselves "have been required for — depending on how you count — about eight years now."

"A better way to think of [CMMC], I would offer, is that it's the compliance, the verification and enforcement mechanism of the existing requirements," Noonan said in an interview. "These requirements are in ... well over a million contracts today — and have been since 2015 — and CMMC is just the government's verification and enforcement mechanism to make sure contractors are in fact doing what is in most of the contracts that already exist today."

And many companies in the defense industrial base currently are not meeting the existing cybersecurity requirements, Noonan said. While the major prime contractors "largely have these controls in place ... as you get into their supply chains, it very quickly drops off ... there's a massive disparity today in implementation of the actual controls."

A major reason for the lack of implementation to this point is the fact enforcement guidelines such as CMMC have not existed, he said. "It's like speeding down a highway: everybody slows down when they see the speed trap, and that's where we are with CMMC. ... I think there were a lot of companies who were waiting until they saw the speed trap, and now that the speed trap is there, we're going to see massive levels of implementation."

A key attribute of CMMC 2.0 is the implementation of a tiered system of three levels for cybersecurity standards and compliance, with prime contractors required to flow the appropriate CMMC requirement down throughout the entire supply chain relevant to a particular contract, the proposed rule stated.

Defense contractors or subcontractors that handle federal contract information must meet the requirements for CMMC Level 1, while defense contractors that handle controlled unclassified information must meet the requirements for CMMC Level 2 or higher, depending on the sensitivity of the information associated with a program or technology being developed.

For CMMC Level 1, businesses can do self-assessments and must comply with 15 basic cybersecurity requirements spelled out in Federal Acquisition Regulation clause 52.204–21, "Basic Safeguarding of Covered Contractor Information Systems." The proposed rule called for the self-assessment to be performed annually and the results entered electronically in the Supplier Performance Risk System.

For CMMC Level 2, contractors and applicable subcontractors are already required to implement the 110 security requirements currently required by Defense Federal Acquisition Regulation Supplement clause 252.204–7012,

"Safeguarding Covered Defense Information and Cyber Incident Reporting," which are aligned with the National Institute of Standards and Technology Special Publication 800–171 Rev. 2, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations." To verify contractors meet these requirements, program contracts will include either a self-assessment requirement or a certification assessment requirement, the proposed rule stated.

Self-assessment must be performed on a triennial basis, while certification must be carried out by third-party assessors known as CMMC Third-Party Assessment Organizations, which must be authorized or accredited to carry out the assessments by the Defense Department. Third-party assessor certification will have up to a three-year duration.

CMMC Level 3 adds another 24 requirements on top of Level 2's 110 requirements, with assessments conducted by the Defense Department's Defense Industrial Base Cybersecurity Assessment Center, with certification valid for up to three years.

For each level, a senior official from the prime contractor and any applicable subcontractor will be required to affirm continuing compliance with the specified security requirements. For Level 1, affirmation is required annually, while for Levels 2 and 3 affirmation is required after every assessment and annually thereafter.

Vincent Scott, founder and CEO of Defense Cybersecurity Group, said making the "assertion that we are completely 100 percent compliant, and that we will remain 100 percent compliant going forward" is an "impossible task."

"Things happen, stuff breaks, people do stuff they shouldn't have done, the controls break down, we end up with control failures. Those things happen," he said. "I can attest to a point in time ... 'Hey, we did a self-assessment on this day, [these are] the results, we went through the process, we say we're 110 out of 110.' But I can't promise tomorrow that we won't be 109 out of 110, because stuff happens.

"The language in the rule that they put in there is very strong," he continued. "An assertion [from a] legal perspective is the equivalent of an oath. So, I have to swear an oath that we're always going to be compliant going forward. ... Nobody can do that."

In a statement, the Defense Department said it "estimates overall program costs will be reduced by allowing for self-assessments for Level 1 and some Level 2 assessments and minimizing cost to industry for Level 3 assessments by having government assessors ... conduct these assessments."

Trey Hodgkins, president and CEO of Hodgkins Consulting LLC and the chair of the National Defense Industrial Association's Cybersecurity Division, said the department is not adequately taking into consideration the costs for companies to not only reach the required level of cybersecurity but to sustain that level long term.

"From a regulatory perspective, [it's] going to be challenging for a sophisticated company to understand all their risks and liabilities, much less a smaller business — which probably doesn't have access to those kinds of resources another company would — to understand what they need to do and not do," Hodgkins said in an interview. "It's costly. I think the department underestimated their expenses."

While the government can assert that many of the cybersecurity requirements are in place in contracts already, "the reality ... is that I think a lot of companies have been waiting for this rule to come out to understand what is the level of the investment?" he said. "Am I supposed to be a Level 1 self-assessment, or am I going to need to do a Level 2 audit, which is done by a third party? Where does the work that I do for the department — or as a subcontractor to some of the primes — where does this fall into that environment, and what do I need to then invest in to meet that requirement?

"I think some people have perhaps postponed or delayed those investments, waiting to see what this looks like and trying to get a better sense of it," he said. "So, they do have an existing obligation, [but] I don't think the department has the kind of universal adoption that they think the contract clauses require."

Another potential cost driver is the expansion of scope in the proposed rule requiring companies to assess not only assets that process, store or transmit CUI but also those that provide security for CUI assets, Scott said.

"From my perspective, that means we are eliminating a huge swath of the available security tools ... that are out there for purchase by the defense industrial base," he said. In the last decade, "nearly all security tools have a cloud component now," and the CMMC 2.0 proposed rule requires cloud service providers to meet the Federal Risk and Authorization Management Program, or FedRAMP, Baseline Moderate or Equivalent standard.

"There are only 300 or so FedRAMP offerings out there, and they are all tooled for big government, ... and if you're a small or medium-sized business, there continues to be challenges in even getting someone to sell those offerings to you, if they exist," Scott said. And switching to a FedRAMP product will incur a "significantly" higher licensing cost, as "it's very expensive to get something FedRAMP certified and very challenging.

"It is a very, very expensive prospect for a company to get their tool FedRAMP certified. ... I don't think there's going to be a lot of drive in the commercial security space to accommodate this because the small- and medium-sized defense contractors" aren't a large enough market, he said. "The DoD isn't driving the marketplace — the rest of the commercial world is, and the rest of the commercial world doesn't care about FedRAMP."

After taking industry's comments on the CMMC 2.0 proposed rule under consideration, the Defense Department is expected to publish the permanent rule later in 2024.

Scott offered a grim outlook if there aren't significant changes to the proposed rule. "You have a pretty fair size of DoD companies that live below

iStock illustration

what I call the cybersecurity poverty line," he said. "The DoD has said [it was] prepared to accept some shrinkage in the [defense industrial base] in order to meet these requirements because it was important. Potentially, I think the shrinkage could be quite large, [and] I don't think the DoD is going to allow that to happen, because [it needs] those companies."

Scott said he thinks of CMMC as the "unstoppable force meeting the immovable object" or a "high-speed SUV sliding into the intersection against the light — there's going to be a wreck, but I don't know where all the cars are going to end up.

"I suspect that the DoD will probably be forced to modify and lower some of this, because ... they really would just crush a significant portion of the defense industrial base if they roll forward with it as is," he said.

Hodgkins said he believes CMMC "will deliver better security at the end of the day" and have a "rising tide floats all boats effect, but it's going to come at a cost.

"I don't know that the government has fully understood what those costs are, and I don't think there's a clear understanding of how government requirements need to be part of the cost of the end product," he said.

Noonan said the "silver lining" for defense companies is that "despite ... some of the noise around these requirements, they're largely the same requirements, and it's kind of like getting in shape.

"There's no better time to start than now, and the sooner you start, the sooner you'll get to the finish line," he said. "Certainly, read the rule, make comments, do all those things, but more importantly, get to work on implementing the requirements, because that's really where all the gains are." ***ND***

VIEWPOINT

Proposed CMMC Rule Spells Out Liability Risks For Noncompliance

BY ROGER ABBOTT AND ADAM BARTOLANZO

The Defense Department on Dec. 26 published for public comment a proposed rule implementing the Cybersecurity Maturity Model Certification 2.0 program — more than two years after it scrapped the initial version of this highly publicized program.

Although the proposed rule does not deviate too significantly from guidance the department has already released, it formalizes implementation and provides contractors with additional information about the program.

However, this rulemaking is limited to Title 32 National Defense regulations; the actual contract clauses that will apply to defense contractors are still being developed under a separate rulemaking process.

Additionally, given the repeated delays in rolling out CMMC, it remains to be seen whether the department will be able to keep up with its aggressive timetable. Nonetheless, contractors should be mindful that the program largely enforces existing cybersecurity requirements and focus their efforts on fully complying with those requirements before the final rule takes effect.

According to the proposed rule, the purpose of the CMMC program is to "establish requirements for a comprehensive and scalable assessment mechanism to ensure defense contractors and subcontractors have ... implemented required security measures," which, for the most part, have already been in place for several years.

The proposed rule also establishes new cybersecurity requirements that apply to a select number of "priority" programs.

To this end, the proposed rule establishes a tiered framework, including the three levels defined by the Defense Department when it first announced CMMC 2.0 in November 2021 and developed in guidance documents that have been published in the interim. Each of these levels aligns with existing cybersecurity requirements. Level 1 is aligned with Federal Acquisition Regulation 52.204-21, "Basic Safeguarding of Covered Contractor Information Systems," which requires contractors that handle "Federal Contract Information" on their information systems to comply with 15 security requirements that are "elementary for any entity wishing to achieve basic cybersecurity."

Although this contract clause technically applies only to contractors that handle such information, the proposed rule indicates that the department expects all defense contractors to comply with FAR 52.204-21.

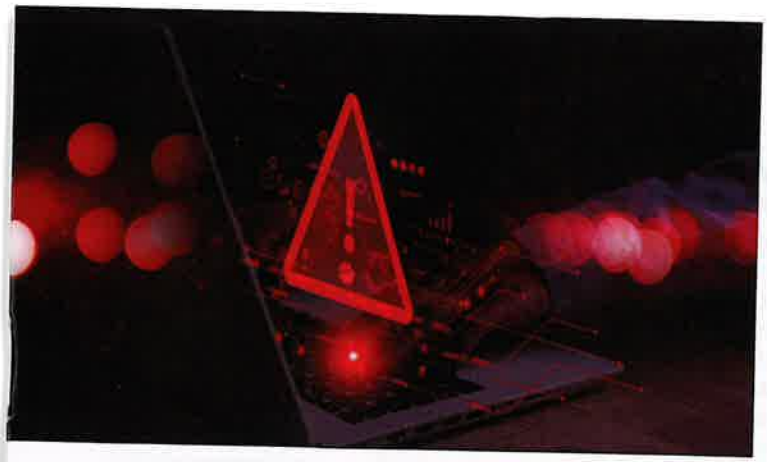
Level 2 is aligned with Defense Federal Acquisition Regulation Supplement 252.204-7012, which applies to contractors that transmit, store or process Controlled Unclassified Information on their information systems. Those contractors must comply with 110 requirements from the National Institute of Standards and Technology Special Publication 800-171.

Finally, Level 3 incorporates 24 new security requirements from NIST SP 800-172, which will apply to a select number of "priority" programs. The proposed rule estimates that only 1,487 contractors will be subject to these new requirements.

The proposed rule enforces these security standards by establishing a scaled assessment mechanism. Assessments will be made conditions of contract award and must be submitted at the time of award for a contractor to be eligible. Level 1 assessments, which will apply to most defense contractors, must be conducted on an annual basis, whereas Level 2 and Level 3 assessments will need to be performed triennially for contractors to remain compliant.

Level 1 requires self-assessments by contractors to verify their compliance and submit their assessment scores to the department's Supplier Performance Risk System before

iStock illustrations



award and annually thereafter. Vague self-assessments, however, are out. The assessment guides — released concurrently with the proposed rule — define concrete self-assessment procedures companies need to satisfy, even if a formal System Security Plan is not required at Level 1.

Level 2 requires contractors to submit either a self-assessment or a certification assessment to be performed by a certified third-party assessment organization "as determined by DoD."

It remains unclear how many Level 2 requirements will be "determined by DoD" to require self-assessments versus certification assessments. The tables included with the proposed rule evaluating its impact estimate that about 95 percent of entities that will be required to certify at Level 2 will need to be certified by a third party. But how reliable an indicator is that? The Defense Department faces a huge backlog of third-party assessors seeking accreditation. Given its estimate that 76,598 companies will need such a third-party certification, it seems likely that many companies will not be able to obtain third-party certification within the three-year timetable for implementation specified in the proposed rule.

Level 3 requires a certification assessment by the Defense Industrial Base Cybersecurity Assessment Center. The center is also responsible for performing the Level 2 certification assessment of the accreditation body responsible for accrediting third-party assessors as well as performing Level 2 certification assessments of third-party assessors. As a result, contractors handling Level 3 information are likely not to be immune from expected delays due to the backlog of third-party assessors waiting for their accreditation to go through.

Under certain circumstances, the proposed rule permits contactors that are not yet fully compliant with existing requirements to submit a "Plan of Action and Milestones." But contractors be warned: such a plan is not permitted for Level 1 self-assessments, and even at Levels 2 and 3, a minimum overall assessment score must be reached before a plan is allowed.

Nor can contractors rely upon a plan indefinitely, as the proposed rule requires it to be closed out within 180 days of the initial assessment. And so, contractors handling Level 2 or 3 information that are not in full compliance at the time of contract award will need to act quickly to address their security gaps, lest they find themselves in breach.

The proposed rule also includes additional information about the use of external service providers, including cloud service providers. Contractors may use non-CMMC certified cloud service providers

to handle Controlled Unclassified Information in a cloud environment, provided the environment satisfies at least FedRAMP Moderate or equivalent requirements.

However, other external service providers must hold a CMMC certification equal to or greater than that of the contractor. Given that the proposed rule will include a mandatory flow-down provision, the restrictions on the use of external service providers will present supply chain management challenges.

The significance of these challenges cannot be overstated because the proposed rule requires a "senior official" of each company subject to the CMMC program to annually affirm compliance. For Levels 2 and 3, affirmation is further required after every assessment, as well as at close-out of a plan of action and milestones. Every affirmation will carry with it a degree of risk under the False Claims Act, with that statute's treble damages constantly hovering over every defense contractor subject to a CMMC assessment as a condition for award.

Will the Department of Justice treat CMMC affirmations as "material" to payments made on a contract subject to the program? Possibly, and certainly an enterprising whistleblower may think so.

Consequently, the requirement to flow down Defense Department cybersecurity provisions to subcontractors, and possibly suppliers, presents risk under the False Claims Act. To fully protect themselves, contractors may need to spend significant resources vetting and monitoring subcontractors and suppliers.

One can imagine the price premium subcontractors and suppliers would include in their quotes if that were the case. Some contractors may require prospective subcontractors to obtain third-party certification even if such independent certification is not, strictly speaking, required.

Liability can also arise under the False Claims Act even when the "senior official" holds a good faith — but incorrect — belief that their company is compliant. This is because liability — and treble damages — can attach if a company acts with "reckless disregard of the truth or falsity" of the matter asserted. Affirming a self-assessment by deliberately ignoring deficiencies in a company's cybersecurity system certainly could land that company in hot water, so care must be taken each time an affirmation is made.

Obtaining a third-party certification of compliance may not necessarily provide a "safe harbor" because companies must continually remain compliant with the required cybersecurity standards. Companies that are subject to the DFARS cyber rule, then, should consider engaging a consultant to develop the System Security Plan they use to perform their NIST SP 800-171 self-assessment, even if it is unclear whether they will eventually be required to obtain a third-party certification.

Having a robust System Security Plan in place may not only help companies that require third-party certification do so expeditiously but could also reduce the risk of liability under the False Claims Act by demonstrating appropriate steps were taken to support a good faith belief in the accuracy of an affirmation of compliance.

CMMC 2.0 applies to virtually all defense contractors regardless of size; only companies whose military business is limited to supplying commercial off-the-shelf products and services or falls under the micro-purchase threshold are exempt.

The program is likely to have a disproportionate impact on small businesses, particularly those required to obtain third-party certification. The proposed rule estimates the cost per Level 2 certification assessment to be upward of $100,000 for small entities. Some companies may be able to minimize costs by limiting Controlled Unclassified Information to an isolated "enclave" within their information system. But companies with only a small number of defense contracts in their federal contracting portfolio may conclude that the cost of complying is not worth it.

Only time will tell what the full impact of CMMC 2.0 will be. Some questions about the program may be answered during the rule-making process, with comments currently due Feb. 26. Others, however, likely will be answered only when the final rule takes effect.

To that end, the department has proposed an aggressive, four-phase rollout that will take place over a three-year period. Under Phase 1, requirements for Level 1 and Level 2 self-assessments will be included in solicitations and contracts immediately upon the effective date of the rule.

Phase 2 will follow six months later, when the Defense Department intends to include requirements for Level 2 certification assessments in solicitations and contracts, meaning contractors will only have half a year to prepare for third-party assessor certifications once the final rule takes effect.

Level 3 certification assessment requirements will start to be included during Phase 3, one year after the rule's effective date. Phase 4, full implementation, will begin one calendar year after the start of Phase 3 and is expected to occur on or after Oct. 1, 2026.

Of course, past projections of CMMC's rollout have been optimistic to say the least. Both iterations of the program have experienced significant delays. Nonetheless, contractors that handle Federal Contract Information and Controlled Unclassified Information should be mindful that they are already subject to cybersecurity requirements, and that now is always the best time to confirm their cybersecurity measures are up to code.

Otherwise, contractors may find themselves suffering the consequences of noncompliance, including the potential for those pesky treble damages hanging ever so delicately each time an affirmation of CMMC compliance is made. **ND**

Roger Abbott is a principal and Adam Bartolanzo is a counsel in the Government Contracts and White Collar Practice Group at Miles & Stockbridge P.C. They can be reached at: abartolanzo@milesstockbridge.com and rabbott@milesstockbridge.com.

Disclaimer: This is for general information and is not intended to be and should not be taken as legal advice for any particular matter. It is not intended to and does not create any attorney-client relationship. The opinions and legal positions asserted in the article are those of the authors and do not necessarily reflect the opinions of Miles & Stockbridge firm.

iStock illustration

NDIA POLICY POINTS

The Costs and Scope of CMMC 2.0

BY RACHEL MCCAFFREY AND MICHAEL SEEDS

While yet to be fully implemented, the Defense Department first proposed the Cybersecurity Maturity Model Certification program in 2019, and the concept seems simple.

CMMC will ensure defense contractors comply with their contractual obligations to protect controlled unclassified information, or CUI, by requiring companies to hire third-party assessors to certify compliance, moving away from the "self-attestation" model.

However, nothing is ever as simple as it seems, and since the CMMC framework was first announced in 2019, "uncertainty" is a word that has been closely associated with the program.

The Defense Department released a proposed rule to implement the second iteration of CMMC, dubbed CMMC 2.0, on Dec. 26. The rule makes several changes, including reducing the number of compliance levels from five to three, aligning Level 2 compliance with National Institute of Standards and Technology Special Publication 800-171, and aligning Level 3 compliance with NIST SP 800-171 and 800-172.

While the streamlined CMMC 2.0 makes some positive improvements, as the short timeline for comments approaches rapidly, we find "uncertainty" remains with some elements, especially around the cost and scope of the program.

The costs surrounding CMMC have been a hotly debated topic since its inception. According to department estimates, the private sector will face an annualized cost of $4 billion to implement CMMC 2.0, which includes nonrecurring engineering costs, recurring engineering costs, assessment costs and affirmation costs.

The proposed rule acknowledges public feedback indicating the cost estimates for CMMC 1.0 were too low, and as a result of several changes, "some CMMC 2.0 costs may be higher than those included in CMMC 1.0."

The proposed rule, however, still does not include the costs associated with implementing the actual underlying cybersecurity controls, such as the security requirements outlined in Federal Acquisition Regulation clause 52.204-21 for CMMC Level 1 and the security requirements outlined in NIST SP 800-171 Rev. 2 for CMMC Level 2. When the department implemented the requirement for defense contractors to protect controlled unclassified information in accordance with NIST SP 800-171 in 2017 under DFARS 252.204-7012, the department did not release a cost estimate to assess the impact on the defense industrial base.

Although the department knew the implementation would increase costs, it answered questions surrounding costs by stating they were "unknown" but "deemed necessary."

Currently, the Pentagon believes it does not need to consider the cost of the underlying requirements for CMMC Levels 1 and 2 since they "should already have been incurred." While this may be true for existing companies within the defense industrial base, it may be helpful for new entrants such as startups and nontraditional defense companies to understand the requirements and costs associated with military partnerships.

Another source of uncertainty is the scope of CMMC 2.0, which goes beyond companies simply complying with existing requirements. As expected, the proposed rule expands CMMC requirements to the application of all NIST SP 800-171 controls and certification assessments to the new category of organization, "external service provider." This means all managed service providers and managed security service providers — companies that provide info-tech and cybersecurity services to defense firms — must certify before the companies they support, the "organization seeking certification," can seek an assessment.

The rule seemingly fails to recognize that expanding the scope of where CMMC requirements are applied also drives a significant cost increase. It no longer simply assesses existing security requirements.

The proposed rule also expands the application of the requirements.

Further expanding the scope, the department creates a new category of information, "security protection data," but does not clearly define the data.

The rule also effectively mandates that every security tool delivered as a cloud service must be FedRAMP authorized or equivalent. Defense companies will need to consider what security tools they have now and what they will need to buy in the future and decide whether to purchase the more expensive FedRAMP options wherever possible.

Another area is the affirmation requirements for Levels 1, 2 and 3. A senior company official must affirm continuing compliance with the requirements in all systems in scope. Still, it is not clear whether an affirmation covers a specific point in time or is continuous. While a company can undoubtedly certify at a point in time that all controls are in place and working, company officials will face new potential liability and an almost impossible task if they must affirm after a set point in time continuing compliance that systems will not break, controls will not fail and the threat will not change.

Finally, in addition to continued uncertainty related to costs and scope, NIST SP 800-171, the primary underlying security requirement for CMMC 2.0, is also undergoing a separate regulatory process to update from Revision 2 to Revision 3.

The Defense Department should partner with industry to develop and implement a plan to transition between revisions to ensure industry can make decisions to allow companies to meet contractual obligations under the Defense Federal Acquisition Regulation Supplement.

The department must prioritize partnering with industry on cybersecurity requirements and implementation. The National Defense Industrial Association strongly believes that more effective cybersecurity requirements will benefit warfighters by protecting our best ideas and technology.

However, the proposed rule requires significant adjustments to balance security requirements with implementation costs. **ND**

Rachel A. McCaffrey is senior vice president of membership and chapters, and Michael Seeds is senior director of strategy and policy at the National Defense Industrial Association.

NDIA PERSPECTIVE BY MICHAEL J. BAYER

Association to Focus on Proposed Cybersecurity Rule

The cyber threat is long past the emergent or developing stage. It has been maturing for some time. While its "guns" go unheard, it is real, and it often comes with more devastating consequences.

It is also a contested domain with a multi-decade struggle for influence that will have a direct impact on our national destiny.

There are many bad actors, but China and Russia have focused their efforts on strategic ways to achieve their objectives. Both are executing well-developed cyber-enabled regional and global "gray zone" strategies at scale against the United States and its allies. These threats are real and are not "unknown unknowns."

From an economic and security perspective, it is vital we protect our nation's critical data and networks. We cannot afford to allow a pacing adversary or near-peer competitors to steal intellectual property, personal health and financial information, or undercut our military's competitive advantage on the battlefield. For these reasons, the National Defense Industrial Association and its members long ago committed to the necessity of securing the data and systems that power the defense industrial base, as well as the platforms, infrastructure and services that support warfighters.

Simultaneously, to avoid extraneous costs and burdens on industry, we have also been vigilant to focus our resources and efforts to prioritize protecting the critical information and systems that truly matter.

Our member companies understand that they are being targeted every day in cyberspace. They take an enterprise approach toward cybersecurity, are personally engaged and consistently communicate expectations. They select leaders who understand the threat and set priorities and incentives that reflect the centrality of information to the success of their operations. They hold everyone accountable for cybersecurity and demand education, training and constant testing of their workforce at every level.

They establish clear and enforceable standards and set priorities for what information must be protected. They establish organizational structures and processes that optimize alignment of responsibility, authority and accountability. They maintain good situational awareness of their organizations' cyber-health and factor cybersecurity into every decision they make.

They also know that information security is furthered through authentic public-private collaboration, and it can fall short when industry is not allowed to be a strategic partner.

The process of implementing the long-anticipated Cybersecurity Maturity Model Certification, or CMMC, program is a perfect example of the need for industry and the government to collaborate and do so in a way that is both supportive and inclusive of the economic realities of all strategic industry partners within the defense industrial base, including small businesses.

In December, the Defense Department released the proposed rule to implement CMMC 2.0. The CMMC program is intended to verify that contractors are meeting cybersecurity requirements. This is a high-priority focus for the association because the verification program adds costs and requirements to member companies.

According to the department's estimates, the defense industry will face an annualized cost of around $4 billion to implement CMMC 2.0. This cost estimate does not include the compliance costs associated with the underlying cybersecurity requirements already spelled out in federal regulations.

And unfortunately, despite this significant financial impact, the rule allowed industry just 60 days to review and comment on the newly proposed rule, eight CMMC guidance documents and requested additional information collection from industry.

The continued flux and uncertainty in the scope and application of cybersecurity requirements and the lack of a well-understood implementation plan continue to drive significant uncertainty for U.S. defense companies. The department and industry must partner to fully identify, understand and prioritize both the data government and industry need to protect and how that data should be protected.

Collaborating with industry as true strategic partners will help ensure we secure the necessary data and systems to maintain national deterrence and warfighting technological advantages while avoiding unnecessary burdens that will regulate innovative companies — especially small businesses and startups — out of their ability to support the Defense Department and its mission.

This is vital work, and we hope you will join our experts who will spend much of this year working on this issue. *(For more on CMMC, see page 20.)*

At the same time, we have another high impact series of conferences underway. Plan on joining us in Charlotte, North Carolina, Feb. 26-28 for the 2024 Tactical Wheeled Vehicles Conference. This extraordinary event brings together leaders from the Pentagon, the military services, industry, suppliers and academia to discuss present and future tactical wheeled vehicle requirements.

In addition, do not miss out on joining NDIA and U.S. Indo-Pacific Command for the 2024 Pacific Operational Science & Technology (POST) Conference held March 4-7, in Honolulu, Hawaii. This annual conference promises to deliver an unparalleled platform for collaboration, innovation and exploration of opportunities for joint research, development and experimentation.

In addition to panels and breakout sessions, POST includes a one-of-a-kind mobile classified reading room for authorized attendees to gain insights into the capability priorities and requirements of the combatant command.

Also, POST Field Experimentation (POST FX) provides industry and academia guests with a unique opportunity to focus on accelerating innovation, including in areas such as biotechnology, quantum science, future generation wireless technology, trusted artificial intelligence and autonomy.

Your NDIA is off to a fast start in 2024. Please join in with us! **ND**

Michael Bayer is NDIA board director and president and CEO of Dumbarton Strategies.

iStock photo-illustration