November 5, 2021

President Joseph Biden
The White House
1600 Pennsylvania Avenue
Washington, DC 20500

CC: Sen. Jack Reed, Chair, Senate Armed Services Committee
Sen. James Inhofe, Ranking Member, Senate Armed Services Committee
Sen. Ben Cardin, Chair, Senate Committee on Small Business and Entrepreneurship
Cong. Adam Smith, Chair, House Armed Services Committee
Cong. Mike Rogers, Ranking Member, House Armed Services Committee
Hon. Lloyd J. Austin III, Secretary of Defense

Re: CMMC 2.0 is Wrong for our Nation

Dear Mr. President,

In the "Executive Order on Improving the Nation's Cybersecurity" (EO 14028), you make the case that "[t]he United Sates faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. … Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life."

Yesterday, the Department of Defense ("DoD") chose not to take a bold step forward but rather several steps backward with the release of CMMC 2.0. These steps are in direct contradiction of your goals set forth in EO 14028 and will harm our nation and the security of our supply chain.

CMMC Background

The Cybersecurity Maturity Model Certification ("CMMC") program was designed to better protect the unclassified intellectual property and other information our adversaries desperately seek by kick-starting government contractors' efforts to improve their own cybersecurity programs. DoD had previously watched for years as contractors paid lip service to, yet self-certified their compliance with, the requirements published in FAR 52.204-21 and DFARS 252.204-7012. As a result, our nation's secrets slipped into the hands of our adversaries, threatening our technological superiority and putting our servicemembers at risk.

That is why, in 2019, DoD launched the CMMC program. Rather than allow contractors to self-assess their cybersecurity programs, under CMMC 1.x contractors' cybersecurity programs would be assessed and certified by independent third-party assessors. This approach allowed our nation to feel confident that the supply chain was properly addressing cybersecurity, permitted industry to scale to meet

certification demand, fostered competition and cost reduction, and created a program that was replicable across the entire government and even to other nations where DoD conducts business. CMMC 1.x allowed attainment of these objectives in a timeline that would help keep our adversaries at bay and staunch the loss of our nation's critical information. CMMC 2.0 negates the value brought by the CMMC program and weakens our national security.

Self-Assessments Do Not Work

Instead of requiring independent assessments, CMMC 2.0 takes us back to the scenario where most contractors can self-assess and certify their programs' compliance with certain standards. This is the same approach that existed prior to establishing CMMC 1.x, and clearly did not work! CMMC 2.0 creates slightly more jeopardy for contractors since the head of the organization must sign an attestation of the contractors' compliance with the regulations. However, contractors are also aware that the Department of Justice ("DoJ") can only pursue a handful of False Claims Act cases each year, and the contractor must be caught, or a whistleblower needs to come forward, before DoJ will initiate a claim. Accordingly, the likelihood is low that DoJ will target any one of the 200,000+ contractors in the DiB. Self-assessments effectively remove any incentive contractors had to bring their programs into compliance.

Creating the Wrong Incentives

The one exception to this argument is with respect to data breaches. As you noted in Executive Order 14028, "[i]t is the policy of my Administration that the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security." Self-assessments create an incentive for the contractors to not report any data breaches or other cybersecurity incidents because this will subject the contractor to review by DoD and could lead to False Claims Act liability. Therefore, CMMC 2.0 will push our nation in precisely the opposite direction intended by your Executive Order.

Making CMMC Compliance Affordable

To be clear, although we believe CMMC 1.x represents a great starting point for improving our nation's cybersecurity, there has always been room for improvement. In the press release accompanying the CMMC 2.0 roll-out, DoD claims that these changes are being made in an effort to make compliance more economical for small businesses. Contractors have been attesting that their cybersecurity programs are in compliance with the FAR and DFARS requirements for years. Thus, unless they have been misrepresenting their programs' compliance to the government, the only additional costs the contractors would face that are associated with a CMMC 1.x program are those associated with the assessments themselves.

Taking the Wrong Approach

While reverting to self-assessments may reduce the compliance cost for some small businesses, given the issues outlined above, cost is not the basis upon which DoD should choose to revert to a self-assessment compliance model. If DoD wanted to reduce the cost for small businesses, there are many alternative avenues available. These include grants through DoD's Office of Small Business Policy and increasing funding to Manufacturing Extension Partnerships and other organizations that would allow small businesses to be assessed at discounted rates. Still further, nonprofit organizations such as the CMMC Information Institute are providing a variety of free and low-cost resources that help small

businesses with their cybersecurity programs. Reverting back to self-assessments and adding government assessors into the mix is simply the wrong approach to "fixing" CMMC 1.x's problems.

Sending the Wrong Message

Another benefit of CMMC 2.0, the DoD asserts, is that it reduces the burden on small businesses by removing CMMC's "process" requirements. While it is true that policies, procedures, and plans (CMMC 1.x referred to these as "processes") will not guarantee a cybersecurity program's success, as illustrated by Equifax, SolarWinds, and numerous other high-profile examples, the absence of well-defined processes, combined with mature, effective governance and oversight, leads to ineffective cybersecurity. Focusing on simply implementing certain technologies, without ensuring they are properly configured and monitored, sends the wrong message to contractors.

History has shown that many contractors will only do, at most, the minimum required under their contracts. If the cost of creating processes was a concern, rather than removing the process requirements, DoD could sponsor the creation of opensource processes which would benefit the entire community and nation. Removing the process requirements from CMMC 2.0 will discourage organizations from taking the steps necessary to mature their cybersecurity programs and will ultimately harm our nation. Again, this is the wrong message to send to contractors.

CMMC 2.0 Cannot Operate at Scale

CMMC 1.x was designed to be agile and used consistently across the entire Executive Branch, and to ensure scalability. According to DoD's own research, there are over 220,000 organizations in the Defense Supply Chain. To its credit, with CMMC 1.x DoD recognized that it currently lacks the capacity to assess that number of contractors and that recruiting the needed number of assessors would be extremely difficult for the government. That is why DoD asked industry to create the CMMC Accreditation Body ("CMMC-AB"), a nonprofit organization that was tasked with overseeing implementation of the CMMC program. The CMMC-AB worked diligently to create a program that fostered competition within the independent assessment organizations, and which allowed organizations seeking CMMC certification to contract with Certified 3rd Party Assessment Organizations ("C3PAOs") to obtain their certification. The CMMC-AB has reviewed and approved the application of over 180 candidate C3PAOs.

The Government Cannot Meet Demand

In 2020, DoD added a new requirement that candidate C3PAOs' own cybersecurity programs must be successfully CMMC certified before the C3PAO will be authorized to conduct assessments. DoD appointed DoD representatives as responsible for conducting those assessments. These DoD representatives already had a significant backlog of work and thus have been slow to assess candidate C3PAOs. To date, only five organizations are now authorized to conduct CMMC 1.x assessments.

Industry is Agile and Ready

The CMMC-AB has trained a cadre of over 120 "Provisional Assessors" who are certified and ready to go to work for the authorized C3PAOs and to begin assessing contractors. Still further, dozens of students have taken training through the CMMC-AB's licensed training providers using DoD-approved curricula, and many more have signed up for future classes. The CMMC ecosystem is poised to jump into action to support our nation, but DoD is not allowing the authorized C3PAOs to begin conducting assessments. Instead, DoD continues to put in place additional roadblocks and policy changes that hurt those

companies that rose to the cause and invested their energy in becoming certified to support this mission. This further hurts our nation.

CMMC 2.0 Does not Scale

CMMC 2.0 introduces the concept of DoD representatives performing the assessments and certification of certain contractors based on the sensitivity of the information they handle. Given that these same DoD staff have only been able to certify less than a dozen candidate C3PAOs in nearly a year, it is hard to see how they will be able to conduct the necessary number of assessments to support the needs of DoD's contractors. This, in turn, means contractors will be shut out of contracts due to DoD's inability to assess them in a timely manner. CMMC 2.0 simply cannot scale to meet the realities of the way DoD and its industry partners function.

CMMC 2.0 Relegates CMMC to a DoD-only Standard

Contractors face an ever-increasing set of government regulations and red tape, with different agencies applying often inconsistent requirements. As you suggested in Section 6 of EO 14028, standardization is critical for ensuring a more agile response to any threat. CMMC 1.x was intended to be useful not only by DoD, but by the broader government and even worldwide. CMMC 2.0 will relegate CMMC to a DoD-only standard.

As noted above, CMMC 2.0 requires government employees to assess and certify the cybersecurity programs of some contractors. While this may sound reasonable in theory, many foreign governments are likely to see this as a red flag and prohibit their nations' companies from participating in the CMMC program and obtaining CMMC certification. In fact, the United Kingdom's Ministry of Defense (their equivalent of our DoD) issued an Industry Security Notice in March 2021 advising MOD contractors who also perform work for DoD that the assessment of their cybersecurity programs, including site visits, could subject those contractors to conflicts of interest and create sovereignty issues with respect to at least some of MOD's information. If one of our nation's closest allies is concerned about independent third parties conducting assessments, imagine other nations' consternation when official US government representatives are the ones conducting the assessments. CMMC 2.0 pushes us farther away from standardization which would benefit both our nation and contractors.

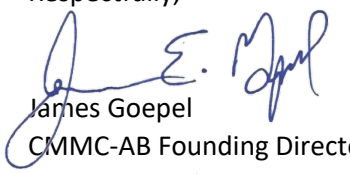
Time is Not on our Side

Somehow, despite taking many steps backward, DoD is also claiming that it will take 9 to 24 months before CMMC 2.0 will be finalized and take effect. This will rob the CMMC program of its momentum and give our adversaries many additional years to even more firmly embed themselves in our nation's supply chain. Again, this is antithetical to the goals you expressed in EO 14028 and harmful to our national security.

Conclusion

CMMC 2.0 is in direct opposition to EO 14028, represents multiple steps backward in protecting our nation, and will only serve to strengthen our adversaries. The undersigned individuals therefore implore you to immediately call on DoD to cease the roll-out of, and cease funding for, CMMC 2.0 and to require DoD to realign the CMMC program in a manner that better protects our nation and is consistent with EO 14028. Our servicemembers', and our nation's, security depends on it.

Respectfully,



James Goepel
CMMC-AB Founding Director
and CMMC Information
Institute Co-Founder

Mark Berman

Mark Berman
CMMC-AB Founding Director

Ben Tchoubineh (Nov 5, 2021 18:03 EDT)

Ben Tchoubineh
Former CMMC-AB Director