CyberNINES
COMPLIANCE WITHOUT COMPLEXITY™

Statement of Scott Singer

President, CyberNINES

before the

House Committee on Small Business

Subcommittee on Investigations, Oversight, and Regulations

Hearing on "CMMC: What It Means for Small Business"

June 24, 2021

Statement of Scott Singer
President of CyberNINES

Thank you Representative Phillips, Ranking Member Representative Van Duyne and members of the subcommittee for inviting me to testify this morning. I look forward to providing information that will help ensure we have a secure Defense Industrial Base and find cost effective solutions to allow small businesses to fully comply with the CMMC Framework and the Department of Defense Federal Acquisition Regulation Supplements.

The SolarWinds hack, Colonial Pipeline cyberattack and the JBS cyberattack have all been in the news lately. There has been some discussion on whether or not implementing NIST SP 800-171 and/or the CMMC practices would have prevented the attack, but in my opinion, it could have prevented having to pay the ransoms and the lost data would have been encrypted and of no use to the perpetrators.

While I will discuss some areas where we will need to relax some requirements, this is done with the suggestion of using a risk-based approach. The faster we can make progress towards getting the DOD supply chain secured the safer it will be.

My name is Scott Singer and I am an owner and President of CyberNINES, a Service-Disabled Veteran-Owned Small Business. CyberNINES has embraced the CMMC ecosystem and is both a Registered Provider Organization (RPO) and a candidate for becoming a Certified Third-Party Assessor Organization (C3PAO).

I am also a retired Navy CAPT and spent over 30 years in active and reserve rolls. My last active-duty role was at the FEMA NRCC (National Response Coordination Center) as the DOD Liaison at the end of 2017, post Hurricanes Irma and Maria. I have over 26 years of experience in information technology leadership roles at Fortune 500 companies and smaller. I tell you this to give the committee some background on myself and the fact that I have worked in both large and small organizations.

CyberNINES formed in June of 2020, an interesting time to start a new business. Thanks to the Interim Final Rule released on Nov 30, 2020, we have been busy. Small businesses are now getting the word they need to comply with NIST SP 800-171. This has come about through the requirement for all DOD contractors in the supply chain to post a cybersecurity compliance score in the Supplier Performance Risk System (SPRS). This requirement is the same no matter whether you are a Prime Contractor or a sub of a sub of a sub. Primes are responsible for ensuring their supply chain is compliant and I have been seeing more of that happen as of late.

CyberNINES has partnered with MEPs (Manufacturing Extension Partnership) in Minnesota (Enterprise Minnesota) and Wisconsin (WMEP). MEPs are public-private partnerships located in all 50 states and Puerto Rico. They focus on supporting small and medium-sized manufacturers. MEPs are an initiative of NIST, a major component of the Department of Commerce.

I suspect I have done assessments in the districts of a number of the members of this subcommittee.

COMPLIANCE COMPLEXITY

Small businesses do not have purchasing departments. They do not have compliance or regulatory departments. In most cases they have not gone to any classes on government contracting and barely know what a flow-down (requirements passed down to subcontractors on purchase orders) is let alone how to protect ITAR (International Traffic in Arms Regulations), EAR 600 Series (Commerce controlled items that used to be controlled as ITAR) or CUI (Controlled Unclassified Information). Those of us that work with NIST SP 800-171 and CMMC all day may start feeling like we know it but for those that don't it is a daunting set of Acquisition Regulations, Export Control Regulations and cybersecurity contract clauses. I have seen Primes flow-down pages of requirements to a small business along with pointing them to their website for more. We need to make this process easier for them. Primes, C3PAOs and RPOs can assist these small businesses get compliant and reduce the complexity for them. **However, the small businesses need help funding this journey or they will drop out of the Defense Industrial Base.**

COSTS ASSOCIATED WITH MEETING CMMC AND MAINTAINING COMPLIANCE

Cybersecurity compliance scores required to be posted in SPRS range from a low of -203 to a perfect score of +110. Of the last 33 Basic Assessments we have conducted for small businesses, the average compliance score was -105. The median score was -110 (where most companies fell). The low was -197 and the high was -13. I would like to think of us as experts and we are only at +81. My business needs to be fully compliant at +110 and complete 20 more CMMC Practices before we are able to be assessed by DCMA DIBCAC (Defense Contract Management Agency Defense Industrial Base Cybersecurity Assessment Center) and get authorized by the CMMC Accreditation Body to conduct assessments for the DOD. So, for our 33 small businesses in WI and MN, where we have recently conducted a Basic Assessment, we have found that on average they are only about 34% of the way toward meeting all the NIST Controls. Cost models put forth by the government assume that companies are much further along on this journey and have completed the 110 NIST Controls and only have to complete the 20 new CMMC Practices, get assessed by a C3PAO and they will be compliant. Assuming fully compliant to the 110 NIST Controls, the DOD has put out that this will cost an additional $26,214 to complete the 20 Practices and 3 Processes followed by an additional $28,616.24 to be assessed by a C3PAO. Reality paints a different picture. As discussed above small businesses that we have assessed are only part way there and the costs will be much higher. Our estimates indicate that they will be more to the tune of $130,000 from my cost models (for micro companies).

Last week I conducted a Basic Assessment of a small manufacturer in MN. They had only 6 employees (including the owner and his wife), one small manufacturing space with three machines and they do excellent, innovative work. I spent a good majority of my time doing the assessment from the owner's house. This year he expects to make $875,000 in revenue. My estimate is that if he wants to stay a DOD contractor and meet CMMC by 01 OCT 2025, he will have to spend 10% of his revenue over the next three years alone on getting compliant. Obviously, his company will not be able to absorb this and we could lose a highly innovative parts supplier to the DOD.

Small businesses lack expertise in regulatory, DOD contracting, quality systems and information technology requiring an excessive amount of opportunity costs for a small business that tries to forge their own path to compliance. There are tools that can help small businesses comply but we need to help connect them with resources that will guide them toward cost effective solutions instead of selling them expensive tools. **Having a program where the Primes take a strong guiding hand of their supply chain is critical to maintaining these small businesses as DOD suppliers.**

There are a lot of discussions around the costs associated with being CMMC compliant as an allowable expense. To the best of my knowledge, Maturity Level 5 (ML5) contracts will be able to direct charge their allowable cybersecurity expenses. For ML3 and Maturity Level 1 (ML1) (which will be the requirement for the vast majority of the DIB) they are directed to add the costs to their indirect rates and spread the costs across the business. I contend for the small manufacturers that this only works if they are the Prime. Most don't have established indirect rates and most don't do cost-reimbursement contracting for DoD. Moreover, market factors around competition for orders will require them to compete and lower prices. Established contractors will be more likely to be able to provide a lower bid and win the order from the Prime. **There should be a process separate from the competitive market place to allow small**

businesses to get paid for the reasonable, necessary and allowable cyber compliance expenses. Companies further ahead should not be penalized and be able to recoup their past expenses too.

OPERATIONAL TECHNOLOGY REALITIES

One of the basic premises of both NIST SP 800-171 and CMMC is that CUI should be encrypted. In the last 33 assessments CyberNINES has done, none of the CNC (Computerized Numerically Controlled) machines being used by our clients would be able to support this requirement. NIST SP 800-171 does have some leeway for what is called Enduring Exceptions using compensating controls as outlined in the NIST SP 800-171 Assessment Methodology. CNC machines are used for generating parts through a reductive process from stock material in an automated fashion from a parts program. The vast majority of CNC machines do not allow for encrypted parts programs. The parts programs must be entered in the machine unencrypted and normally via a USB thumb drive.

To date and to the best of my knowledge, there are no pieces of CNC equipment utilizing encryption. And there are no plans of adding this option to CNC equipment that I am aware off.

CNC's are being used as an example here today, but most of the manufacturing machinery in industry faces the same challenge. Currently there are limited options for equipment that utilizes encryption. Those products utilizing encryption are very new to the market and not in mass use.

CMMC doesn't really address operational technology such as manufacturing equipment. I would propose that the CMMC standard expressly allow for compensating controls. We have been counseling our clients to protect the USB drives by locking them away when not in use, labeling the drives as CUI and protecting the parts program using a FIPS 140-2 compliant encrypted location such as a FedRAMP High GovCloud. And, our first choice is to air gap the equipment, but, when it needs to be connected to the Internet or Intranet, we recommend a defense in depth strategy of segmenting these manufacturing machines from the rest of the network. This can take time and cost money so some flexibility in implementation is essential.

BOTTLENECKS FOR C3PAOS

C3PAOS NEED TO GET ASSESSED SO THEY CAN DO ASSESSMENTS

As of the writing of this testimony only two companies have passed the DIBCAC assessment to be Authorized C3PAOs to conduct assessments. To the best of my knowledge, less than 10 C3PAOs will have been assessed by DIBCAC this year. According to the April 2021, CMMC Town

Hall, the Accreditation Body (AB) has recognized 171 Candidate C3PAOs and 278 pending C3PAOs: more than 400 total. In addition, there needs to be enough CMMC Assessors (CCAs) to conduct the number of assessments which the AB requires of C3PAOs. At this time there are only 100 Provisional Assessors (PAs) available to do assessments for C3PAOs. Doing the math, I don't see how we can get anywhere near enough C3PAOs through the process to assess 300,000 DIB companies by 01 OCT 2025. I saw one estimate that we would need over 8,000 assessment team members working full time from today until 01 OCT 2025.

C3PAOs must meet FedRAMP High in order to pass DIBCAC assessments. Requiring FedRAMP Moderate as is the current requirement for NIST 7010 would improve throughput of C3PAO assessments.

C3PAOs may only be holding System Security Plans (SSP) from consulting arrangements, and there is an argument to be made that they don't need to have client documentation in their environments related to assessments (Note: A C3PAO can't do an ML1 or ML3 Assessment and provide consulting to the same company). It is more likely the general consultants like RPOs will hold documentation such as System Security Plans and Plans of Actions and Milestones as they prepare organizations to be compliant. Thus, there is more risk, I contend, with RPOs than C3PAOs as C3PAOs should leave their work at the client's office. I believe a more appropriate level for C3PAOs is Maturity Level 1 (ML1) which is required for handling Federal Contract Information (FCI). However, in the interest of compromise, ML2, while a transition step, may be a good interim step to get more C3PAOs authorized if the DOD is set on ML3. That said, it has been helpful for my company to go through the same process as our customers. C3PAOs will be required to hold and submit assessment reports to eMASS. These assessment reports are being considered at this time as CUI which is also driving the ML3 requirement. A group of C3PAO candidate companies believe that this decision to treat these reports as CUI should be reviewed given the lack of CUI in these reports. (Over-classifying private information as CUI can create many problems disproportionate to value.) Doing so will permit a more appropriate and immediate number of C3PAOs to launch the CMMC program while still meeting the intent of handling CUI. **A compromise would be to assess Candidate C3PAOs to ML1 or ML2 now and require ML3 in the future, if needed, after more DIB companies get assessed. Recommend the DOD look at creating an eMASS Enclave to allow C3PAOs to use the tool without having to meet cleared industry requirements.**

C3PAOS STAFF MUST HAVE TIER 3 INVESTIGATION

C3PAOs have been instructed that the following staff need Tier 3 Background investigations. These investigations are equivalent to a DOD SECRET clearance investigation, but do not convey a clearance.

- All assessors

- Quality leads and technical managers responsible for assessment quality and review
- IT staff

This background check requirement is far above the standard for the assessment industry as well as the defense contractors being assessed. Even companies that develop ITAR products do not need Tier 3 background investigations of their staff.

The ability to submit staff for Tier 3 Background investigations is extremely limited at this time. C3PAOs have been advised to hire staff with active clearances as a workaround. This could negatively impact resources that could be used on cleared contracts.

This requirement for Tier 3 background investigations for assessment and support staff creates a bottleneck for C3PAOs. **I would recommend this requirement be reduced to the level of a typical government Suitability Determination. This would greatly increase the time to get people checked and I believe does not impact national security due to the level of information (CUI, ITAR, 600 Series) that is being reviewed. Another option is to allow interim clearance as done with DOD clearances.**

POSSIBLE SOLUTIONS

ALLOW RISK ACCEPTANCE

Right now, companies can't get a CMMC certification, when it is required, without a 100% score on all assessed criteria. Forcing a framework that requires such "perfect" compliance will result in DOD supply chain interruptions. In my experience with AS9100, ISO 13485 and ISO 9001, auditors are given some freedom to give major and minor findings. Failing only happened after multiple major findings and a failure of the company to address them. To my knowledge, the DOD has not been able to fully implement their own cybersecurity requirements for internal Federal Systems. 100% compliance is not a realistic goal.

I would suggest allowing companies to fall short on low risk cybersecurity requirements with provisional certification. In addition, I would recommend developing a scoring model for CMMC and a criterion for provisional certification, adjudicated by the DCMA DIBCAC. Rate suppliers as High, Moderate and Low and set a score for that level. As the process matures, the criteria for a pass should get harder. I think the idea of a provisional certification that allows companies to process CUI is best for balancing risk with the need to maintain the DIB supply chain in the short term.

ALLOW FOR REIMBURSEMENT OF SOME EXPENSES TO MEET CMMC

As discussed earlier in my testimony, non-COTS (Common off the Shelf) manufacturers are going to need to meet CMMC ML3, and small businesses are going to have a difficult time. While large Primes at CMMC ML5 are allowed to claim the allowable cybersecurity expense, ML3 and ML1 will need to absorb the cost in their indirect rate. Leaving it to market conditions for non-Primes will lead to an unfair playing field for competition. Those that want to take a risk or those that are further along with their own journey toward full compliance will be able to set lower prices and win orders. Those that decide to increase their internal indirect overhead costs and thus increase their direct rates will risk losing orders. While on the surface this may seem like fair competition, it is not in the best interest of the government in getting the best manufactured parts. There should be a system for reimbursement that is outside the competitive market process. For small manufacturers, use the MEP network as a way to equitably distribute funds. They are already setup to work in this fashion through NIST.

ALLOW HOSTING OF UNAFILLATED ORGANIZATIONS

There needs to be the allowance to support hosting of micro-small businesses on shared or higher lever suppliers in the supply chain without them needing to be ML3 Certified. As long as their host is certified. Using an MSSP (Managed Security Service Provider) model will allow sharing of costs of being compliant over a number of companies.

Another area of CMMC focus has been on using CUI Enclaves to wall of CUI from the rest of the company and reducing risk of a CUI breach. This is important for protecting CUI and can reduce costs for small businesses, but I believe there are some unintended consequences. Too much focus on CUI Enclaves could impact overall security. While encrypting CUI will ensure that it does not fall into bad actors, ransomware can take down the whole company and interrupt the DOD supply chain. Money may be better spent on general cybersecurity hygiene for small businesses and utilizing a hosting model from Primes. Create the hosting/ransomware protection framework for small to micro-DOD subcontractors.

GRADUATE THE ROLL OUT OF CMMC

Start the roll out based on risk. Develop a risk level for orders similar to Rated Orders. Require higher risk orders to have to meet the CMMC requirement along with the Prime’s supply chain. The risk should be based on the impact to national security due to a breach of CUI or impact to a project due to ransomware. I would recommend this going into place at the same time that CMMC goes into effect on 01 OCT 2025. Before then, the CMMC process should be tested thoroughly. Gradually increase the number of required Primes and their supply chains that must meet the requirement based on the ability for the C3PAO and CMMC ecosystems ability to handle the demand.

Small businesses further down the supply chain generally are dealing with single parts and special processing (painting, coatings) whereas larger suppliers are dealing more with sub-assemblies. In addition to risk rating awards, I recommend that CUI at the part level should be viewed as less of a national security risk than assemblies (this will not always be the case).

CONCLUSION

The Defense Industrial Base is critical to our national security. The majority of the 300,000 contractors in the DIB are small businesses. Without monetary support and clear regulatory guidance, the DOD will lose small businesses as they will make the tough business decisions to find business in the commercial sector.

A balance must be struck between risk and cost. Too much cost and we lose suppliers. Too much risk and we hurt our National Security.

Thank you for allowing me to testify today. And, especially, thank you for supporting all the small businesses that are the backbone of our National Security.