TESTIMONY OF DR. WILLIAM LAPLANTE

SENIOR VICE PRESIDENT, MITRE NATIONAL SECURITY SECTOR

BEFORE THE

CYBERSECURITY SUBCOMMITTEE

OF THE

SENATE ARMED SERVICES COMMITTEE

MARCH 26, 2019

Chairman Rounds, Ranking Member Manchin, and distinguished Members of the Subcommittee on Cybersecurity, thank you for the opportunity to testify before you today on matters relating to the cybersecurity of America's defense industrial base. This is a critically important issue and one about which I very much appreciate being asked to offer some thoughts.

For those who don't know MITRE, we are a not-for-profit corporation that operates seven federally-funded research and development centers, or FFRDCs, for eight primary government sponsors. The largest of the FFRDCs we operate, the National Security Engineering Center, is sponsored by the Department of Defense. We also operate the National Cybersecurity FFRDC on behalf of the National Cybersecurity Center of Excellence, which is a component of the National Institute of Standards and Technology, or NIST. Of MITRE's roughly 8,500 employees, some 1,000 are cybersecurity experts who support a very broad range of work on behalf of federal requirements. Our vantage point, which gives us the benefit of being able to look across multiple agencies at a wide array of threat vectors and challenges, is critical to our understanding of this problem set and greatly informs the advice we are able to provide to our sponsors.

If I may, I would like to take a moment to congratulate the leadership of this Committee for having the foresight to establish this panel in the 115th Congress and for continuing it into the current Congress. There is no question but that the cyber domain is a critical warfighting domain today. This is unequivocally true, as you are all aware, for those who wear the uniform of our military and who are charged with defending against hostile cyber operations directed against our forces literally every day. But it is no less true for the thousands of companies that make up the nation's defense industrial base – companies that support our national security through the delivery of vital goods and services under contract to the Department of Defense and its components, and without whose support our forces would be all but ineffective. The men and women of our defense industrial base do not wear the uniform, but they are no less a target in this age of cyber warfare.

Indeed, as the Members of this Committee well know, both from the near endless stream of media reporting we all see and the information you receive from both the Department and the many companies that comprise the managed cybersecurity services industry, our defense industrial base has been and remains under siege from hostile actors. The loss of intellectual property in recent years has been enormous, and it has allowed our adversaries to rapidly and dramatically advance the state of their warfighting and enabling technologies by leveraging our substantial investments in research and development. Our technological edge – which along with the quality of our men and women who serve, and the strength of our alliances with key partners, has for decades given us a vital advantage – has in many areas been compromised.

While even the largest defense contractors have been victimized by the predatory cyber operations of our adversaries, the problem has been most acutely realized at the lower tiers of the defense industrial base, typically comprised of small- to medium-sized companies. These companies often serve as the sub-contractors and sub-sub-contractors to the primes. In many instances, they are start-ups or just barely removed from such status. They are often where some of the greatest innovations occur – the kinds of innovation that are, rightly, being pursued by the Department for integration into our most advanced warfighting capabilities.

As the 2018 National Defense Strategy (NDS) noted," the Department's technological advantage depends on a healthy and **secure** national security innovation base." It also observed that the Department must streamline processes so more "small-scale vendors" can provide the Joint Force with those cutting-edge technologies needed to maintain our military advantage. I believe we can, and in fact we must, do both of these things – maintain a secure innovation base, and yet not overly burden smaller companies with such onerous and costly compliance mandates that it drives them away from doing business with DoD.

The fact of the matter is, this is an extraordinarily difficult problem set. Many have decried the insufficiency of efforts to protect the defense industrial base, blame for which often falls on the Department of Defense. I have heard many who have suggested that the Department "hasn't done enough" to address this major challenge.

From my perspective, I think the Department has actually done quite a lot. Most recently, it has adopted the NIST 800-171 standards for cybersecurity and integrated related requirements into the Defense Federal Acquisition Regulation Supplement (DFARS), with additional work underway on revisions to these standards. One of the questions that the Subcommittee posed in inviting me to testify today asked about my thoughts on the potential need for contractors to meet security standards beyond the NIST 800-171. The 800-171 specifies that defense contractors handling controlled unclassified information execute over a hundred separate controls on their systems. Achieving full

compliance requires implementing all of the controls or equivalents. I will tell you that MITRE, with some 1,000 of what I would consider some of the world's best experts on cybersecurity, had an enormous challenge meeting the requirements of the 800-171. For companies that are much smaller than MITRE, with far fewer resources and far less cybersecurity expertise available, one can only imagine that additional requirements beyond the 800-171 will be incredibly burdensome. Complicating this is the fact that while DoD requires compliance with 800-171, other federal agencies utilize a different security standard. So if a contractor wants to do business with both DoD and, say, the Department of Homeland Security, it has to either operate under two different sets of requirements, or ratchet controls up to the highest instance.

I would further make the observation that there is no measure or target for outcomes associated with implementation of the 800-171 standard – for instance, was less data lost? While standards may have the potential to improve performance above a baseline level, they quickly lag behind evolving operating environments and emerging technologies. Most importantly, they quickly become the target of our adversaries, who familiarize themselves with our standards and look for seams they can compromise. We cannot lose sight of the fact that this threat is extremely dynamic.

My point in highlighting this is to caution against an urge to levy even more security standards on contractors beyond those already being contemplated in the update of the 800-171 when the Committee sits down to draft this year's authorization bill. The danger is that you will either put contractors in a situation in which they will continue their efforts to support DoD but will ignore these requirements, or they will simply reject the idea of doing business with the Department or the Tier 1 contractors because the burdens are too great.

On this score, I would suggest there is a real need to encourage the contractor community to consider implementing threat-informed defenses. Clearly, there are basic security standards – essentially, compliance-oriented requirements – that need to be met. But there is no substitute for understanding the nature of the threat vectors most commonly used by our adversaries – their specific tactics, techniques, and procedures, or TTPs – and using that awareness to inform where network defenses need to be beefed up to thwart the most likely or consequential cyber threats. MITRE has done a considerable amount of work in this area, and we make our ATT&CK framework – basically, an encyclopedia of adversary cyber TTPs that can assist security practitioners to best determine how to position their defenses, and where to invest limited resources to get the biggest bang for the buck – available at no cost, in keeping with MITRE's service in the public interest.

With that said, let me offer some thoughts about some areas in which there might be some useful progress in this area, recognizing that there is no silver bullet and that none of these is going to be a panacea.

Critical to a successful path forward, I believe, is the need to bend the cost curve on cybersecurity. We need to find ways to make cybersecurity architectures less expensive for the defense industrial base to implement.

For example, I think there could be some value in encouraging DoD to work with the National Institute of Standards and Technology to recognize the defense industrial base as a key industry vertical. Such recognition would result in the development of practice guides and reference architectures tailored to the requirements of this community of interest. Again, I am not going to tell you this is a panacea. But such products could be used by some contractors – probably some of the medium-sized ones, at least – to model enhanced security postures. Clearly, there will be some who will find themselves unable to leverage such products or who have specialized requirements that may not be met by them. But NIST has generated other guidance – for example for use by the health care and energy sectors – that have certainly had utility.

Another option that has been discussed – and was among the questions posed by the Subcommittee in its invitation – relates to making the kinds of Continuous Diagnostic and Mitigation (CDM) products that the "Dot Gov" agencies are required by DHS to employ, also available to the defense industrial base. CDM is essentially a suite of commercial products that help federal agencies understand the details of their networks and systems and better monitor activities occurring on them. These tools can aid in identifying the inventory of connected devices on a network and help identify patching deficiencies or other security problems. Again, I would say there could be value in such an offering, but this, too, is no silver bullet. Performing timely patching and assuring basic network and system hygiene are a necessity, but this approach alone is insufficient to assure security. In today's computing environments, there is too often just no way to have full knowledge of what's on a network or a perfect ability to patch. A vulnerability scan one day may reveal a range of unknowns that may differ just a few days later. So again, not an end-all, be-all, by any means, but one potential set of tools that could help.

One concept that I think has particular promise, which Under Secretary of Defense for Acquisition and Sustainment Ellen Lord in fact has advocated exploring, is the idea of one or more cloud environments, operated under auspices of DoD, that would be specifically tailored to the needs of the defense industrial base. Such DoD-sponsored cloud offerings would be fully compliant with the latest 800-171 or successor security standards, potentially relieving the contractor community of many of the burdens of managing their own architecture and security requirements. Such an infrastructure would allow the contractor community to access compute, storage, managed security, software development, and other services from one or more DoD-sponsored service providers. There are a lot of unanswered questions about this approach, not the least of which relates to the ultimate cost a contractor would have to bear to leverage these services. Presumably there are economies of scale that would be realized in such an instantiation that could be passed on to contractors. Moreover, if more than one such offering were

made available, such an arrangement could generate additional competitive pressures that could help drive costs down. Certainly, there are other important questions that would need to be asked – for instance, would such an arrangement also address back office requirements like finance, human resources, and the like? What about specialized capabilities, like the computing requirements associated with, say, a laser cutting machine? Another important question: What would compel or incentivize contractors to avail themselves of such an offering? My own view on this is that an award from the government would be contingent on contractors – including any lower tier sub-contractors who wish to be involved – meeting all specified security requirements.

One additional thing I would emphasize here is the need for the Committee to look beyond just cybersecurity to also consider the broader challenges associated with the nation's supply chain. I realize this may extend the discussion beyond the writ of this Subcommittee.

MITRE has developed a strategy we have called "Deliver Uncompromised," designed to help DoD address the broader question of critical dependencies and other weaknesses in our supply chain. There are many aspects to this strategy, but one important recommendation calls for the formation of a whole of government National Supply Chain Intelligence Center (NSIC) to aggregate all-source data, both classified and unclassified, to share with at-risk operators and industry partners. The NSIC would operate as a shared national resource to develop and operate technologies for threat detection, artificial intelligence, and data analytics, enabling analysts to "connect the dots" among disparate data from a multitude of sources. While not nearly as large, it would be modeled on the National Counterterrorism Center, and would be populated with representatives from the intelligence, program, and systems engineering communities and have a broad range of authorities. It would serve as the center of excellence for supply chain strategic warning and risk assessment, including responsibility, for example, for determining the provenance of software destined for DoD, which often includes elements that originated overseas.

Today, threat warnings to industry – if they occur at all – are too slow and cumbersome, leaving the majority of companies in the innovation base uninformed and exposed. Methods must be established to share threat information and recommendations with companies that are not cleared contractors. It is difficult to translate from classified threat data into unclassified warning, but this is a responsibility that should be assigned to the NSIC.

With that, let me conclude by thanking the Subcommittee once again for offering me the opportunity to testify today. I will be pleased to respond to your questions.