Stenographic Transcript
Before the

Subcommittee on Cybersecurity

COMMITTEE ON
ARMED SERVICES

UNITED STATES SENATE

HEARING TO RECEIVE TESTIMONY ON
THE CYBERSECURITY RESPONSIBILITIES OF
THE DEFENSE INDUSTRIAL BASE

Tuesday, March 26, 2019

Washington, D.C.

ALDERSON COURT REPORTING
1111 14TH STREET NW
SUITE 1050
WASHINGTON, D.C. 20005
(202) 289-2260
www.aldersonreporting.com

HEARING TO RECEIVE TESTIMONY ON
THE CYBERSECURITY RESPONSIBILITIES OF
THE DEFENSE INDUSTRIAL BASE

Tuesday, March 26, 2019

U.S. Senate
Subcommittee on Cybersecurity
Committee on Armed Services
Washington, D.C.

The subcommittee met, pursuant to notice, at 2:31 p.m. in Room SR-232A, Russell Senate Office Building, Hon. Mike Rounds, chairman of the subcommittee, presiding.

Subcommittee Members Present: Senators Rounds [presiding], Scott, Manchin, and Gillibrand.

OPENING STATEMENT OF HON. MIKE ROUNDS, U.S. SENATOR FROM NORTH DAKOTA

Senator Rounds: The Cybersecurity Subcommittee meets this afternoon to discuss an issue of great concern to me and the Department of Defense: the cybersecurity of the defense industrial base.

Since the reporting of the breach of a contractor for the Naval Undersea Warfare Center last June, the Department has been shocked into action. The truth is, however, that adversaries have been breaching our contractors for a much longer time, stealing our design information and intellectual property not by targeting the Department itself, but through its vulnerable contractor base.

This espionage will never be stopped in its entirety, and it is unlikely that it can be negotiated away or deterred. It must, however, be made more difficult. The Department cannot afford to continue leaking critical design secrets to China and Russia effectively subsidizing their own defense developments.

It is incredibly clear that the status quo is not working. So far, the Department’s efforts in this space have been disjointed and have mostly been a reemphasis of the current policies.

The Navy has taken additional steps to start to audit its contractors for compliance with their cybersecurity requirements. This month, the Navy released their cybersecurity readiness review, which includes several recommendations for improved collaboration and communication between the Navy and their contractors to mitigate cyber threats. I am encouraged that the Secretary of the Navy has taken the first step to improving their cybersecurity by completing this detailed review, and I look forward to understanding how they plan to implement the recommendations.

The Office of the Secretary of Defense has also reemphasized the importance of the current National Institute of Standards and Technology, or NIST, cybersecurity standard.

The Department has also stood up the Protecting Critical Technologies Task Force headed by Major General Murphy. The task force is taking a wide-reaching approach to the problem, contemplating the policy, technological and operational changes that could improve contractors' cybersecurity.

While I expect the Department will come up with measured policies to make improvements in this area, I hope that it takes seriously the concerns of the defense industrial base. The Department cannot simply apply increasingly stringent cybersecurity requirements on its contractors. Doing so without subsidy or assistance is unlikely to particularly improve the cybersecurity to the defense industrial base and will likely drive the most innovative small businesses out of its supply chain.

I am also somewhat apprehensive about an approach centered on cybersecurity checklists. While there are benefits to the NIST-based framework, I am concerned that approaches based on compliance to that framework do little to help businesses meet these standards, do not account for the particulars of the threat, and do not help businesses prioritize investments or personnel. Instead, these approaches establish baseline for capability which may or may not form the basis for an effective cybersecurity architecture.

I hope the Department can formulate policies that prioritize the lowest-hanging fruit and emphasize the best return on investment for contractors that often struggle within thin margins.

I also hope that the Department’s policies take a considered approach to partitioning cybersecurity responsibility among itself, its prime contractors, and their subcontractors. No one entity can shoulder the entire burden of this effort.

We have invited witnesses from the defense industrial base to assess how the Department’s policies and regulations have affected their cybersecurity, which is a viewpoint that we cannot afford to ignore in these conversations.

Today, we will hear from: the Honorable William A. LaPlante, Senior Vice President and General Manager, MITRE National Security Sector, heavily involved in the MITRE strategy entitled “Deliver Uncompromised;” Mr. John Luddy, Vice President for National Security Policy, Aerospace Industries Association; Mr. Christopher Peters, Chief Executive Officer of The Lucrum Group, heavily involved with the National Defense Industrial Association’s work on defense industrial base cybersecurity; and Mr. Michael P. MacKay, Chief Technology Officer, Progeny Systems Corporation, a small defense contractor based in Manassas, Virginia. Thank you for your willingness to testify today. I look forward to our conversation this afternoon.

Senator Manchin?

STATEMENT OF HON. JOE MANCHIN III, U.S. SENATOR FROM WEST VIRGINIA

Senator Manchin: Mr. Chairman, thank you so much.

I want to thank each and every one of you all for being our witnesses today testifying on a critical national security problem, namely the hemorrhaging of technology and know-how from the U.S. industry and academia to adversaries, chiefly China, which enables the rapid progression of their military capabilities. I have had the opportunity of both serving on Armed Services and Intel. So I know exactly where you all hopefully will be coming from.

We know that China is using cyber hacking and coercing technology transfers from U.S. companies to acquire U.S. intellectual property, which undermines our economy and ultimately erodes national security because it remains easier for cyber hackers to penetrate networks than for defenders to stop them. There are no simple solutions to these problems.

But I am encouraged to see Congress, DOD, and the private sector finally addressing the fundamental issues that we all face.

One of these pressing issues is the imperative of improving security in the smaller defense industrial base companies. These companies are vital components of our supply chains and sources of our innovation. But many of these small companies currently lack the resources and expertise to defend themselves and the DOD data and technology that they hold against national state attacks.

We must find ways to correct this situation. Our witnesses today -- you all come from and you represent or you have studied these industrial base partners who are threatened every day with cyber attacks from our principal adversaries. So I look forward to your insights and advice on how we correct this.

Thank you, Mr. Chairman.

Senator Rounds: Thanks, Senator Manchin.

Let us just begin with opening statements, if you would like, and Dr. LaPlante, I will start with you.

STATEMENT OF HON. WILLIAM A. LaPLANTE, SENIOR VICE PRESIDENT AND GENERAL MANAGER, MITRE NATIONAL SECURITY SECTOR

Dr. LaPlante: Yes, thank you, Chairman Rounds. Thank you, Ranking Member Manchin. Thank you, Senator Scott and the other members of this committee.

Of course, having this hearing and your opening statements both identified the challenge on the threat side, but also making sure that every solution we put in will not be actually worse than the problem we are trying to solve. So you understand that.

As you said, I am Senior VP at MITRE. We operate seven -- it is a not-for-profit -- FFRDCs, one for the DOD and the IC, but another one, importantly, is the standards of cybersecurity for NIST. So I have a few things to say about that.

Before that, I was the Secretary of the Air Force for Acquisition.

As you all know, just like our warfighters are under attack or threatened under attack, we now pretty well know that our defense industrial base has been under attack for 10-15 years. Most of us who have worked in the industrial base have known this. It has been a while. For a while, we could not talk much about it, which has been part of the problem.

And, yes, we still have an education issue, as I think some of my colleagues are going to say.

It is not just the loss of IP. We have all had this experience. My experience while Assistant Secretary I think was at the Dubai air show walking over to the China part of the air show and looking at the J-31 and saying other than that second engine, that is the F-35, and then going over and getting the brochure for what was a dead-on copy of the MQ-9, which is our Reaper unmanned aerial vehicle.

Now, am I saying the insides are the same and they operate the same? No, maybe not, but they will get there. And so, yes, it is real.

But it is not just the IP. It is also how we train. It is our manuals. People in my business -- we write lots of stuff. We write lots of technical memos. And a lot of that stuff has not been classified. So you can understand how we train. You can understand what they call -- you understand tactics, techniques and procedures, CONOPs. So it is all together.

Now, does that mean that they are going to be just as good as us by having it? Not necessarily so, but it sure helps. It sure helps them.

So this is about our tech superiority.

Now, inclusion is needed. At the same time we are saying all this, of course, we do not want to scare away our friends in industry. We want the small businesses. We want the innovative firms. We get that.

So this is complex, but we can solve it. We have to educate.

Now, the Department gets knocked for this a lot, and I think we have all kept pressure on the Department. And I have been on the other side of this boat too. But they have done a bit. You referred to the Navy. The Navy has been really active over the last year and a half partially out of real reason. I would also say that putting the standard out there, 800-171, is not a panacea. You are exactly right, Mr. Chairman. Compliance by itself is limited in what it can do. It can do things. What we used to call it on the Defense Science Board is can raise cyber hygiene. That is good. It is like the broken window theory of crime. It does make the neighborhood a little better, but it is not going to solve it because you have an adversary. It is not just quality that you are trying to build a better airplane. You have an adversary.

But it has over 100 controls. We still have multiple standards.

But here is what we are missing, and we are all trying to work this. And the insurance industry is going in this direction. The Deliver Uncompromised paper you referenced was trying to go there trying to figure out how to monetize, how to turn security of cyber into something real that you can actually measure as an outcome. Compliance is an input. It is not an output. You really want to know if I did this, what percentage more secure am I. I can measure costs. If I have a radar, I can measure its performance. I can measure its schedule. I may not like the schedule, but I can measure it. I do not know how to measure cybersecurity. We have got to figure that out. Once we figure that out -- and the insurance business is going there because that is what they are in -- where we can start putting real objective metrics against this, then we will get there. And so I am actually optimistic. In the next couple years, I think we will get there as a community. That is where we need to go.

So there are other things we can do. We need a threat sharing center, not unlike the NCTC, the National Counterterrorism Center, where you got FBI sitting next to intel, sitting next to industry that can rapidly see what is happening. A company gets bought overnight. It was good. Now it is bad. We got to get that information out. Oh, by the way, the people that you got to get the information to do not have clearances. So we got to figure that out. But we got to go into a much more of an active model like that.

And there is experimentation going on, great ideas, of bringing secure cloud environments and making them available to the industrial base so they can develop inside a secure cloud. It is already being done in parts of the government right now. That is a great idea.

There are other ideas we will talk about later.

Again, thank you for having the hearing. I look forward to your questions.

[The prepared statement of Dr. LaPlante follows:]

Senator Rounds: Thank you, Dr. LaPlante.

Mr. Luddy?

STATEMENT OF JOHN LUDDY, VICE PRESIDENT FOR NATIONAL SECURITY POLICY, AEROSPACE INDUSTRIES ASSOCIATION

Mr. Luddy: Chairman Rounds, Ranking Member Manchin, Senator Scott, members of the subcommittee, thank you for your efforts to highlight the importance of a secure supply chain and for inviting me to contribute to today's discussion.

The Aerospace Industries Association represents nearly 340 manufacturers, suppliers, and service providers across every sector and tier of the aerospace and defense industry. Our 2.4 million people are the backbone of the American economy and are crucial partners in protecting our national security.

Our industry is fully committed to partnering with the U.S. Government to stay ahead of cyber threats and ensure resilience throughout the industrial base. AIA has just issued a report called "What's Next for Aerospace and Defense: A Vision for 2050." The report paints a picture of the technologies and innovations that experts in our industry believe will be driving the way we move, connect, explore, and defend our interests 30 years from now. The future we envision is exciting, and it depends entirely on robust and reliable cybersecurity. So we share concerns raised by senior Department of Defense leaders about the cybersecurity of U.S. military systems and of our entire acquisition process.

I also want to emphasize that we at AIA are pleased with the level and quality of dialogue we are having on this topic with DOD. Cybersecurity is discussed prominently at quarterly meetings of our CEOs with Under Secretary of Defense for Acquisition and Sustainment Ellen Lord and her senior staff. I also convene quarterly engagements with Vice Admiral David Lewis, Director of the Defense Contract Management Agency, and other DOD officials. We held the fourth of these meetings last week and have now institutionalized them as a forum to iron out the specifics of cybersecurity policy and implementation.

This afternoon, I will focus on three areas: first, on the way DOD defines the information that contractors must protect; second, on the need for cybersecurity policy to be clear, consistent, adaptive, and scalable, both across DOD and with industry; and finally, I will highlight AIA‘s National Aerospace Standard 9933, “Critical Security Controls for Effective Capability in Cyber Defense,” which we are now seeking to improve and bring into wider industry use in collaboration with DOD.

My first point is fundamental: the initial step in gauging appropriate cybersecurity is understanding what information needs to be secured. Obviously, classified information is clearly marked and handled through separate and secure channels. But DOD and industry also handle an enormous amount of controlled unclassified information, or CUI, some of which is further designated as covered defense information, or CDI. This CDI is the focus of our ongoing shared cybersecurity efforts.

In August of 2015, DOD implemented a DFARS cybersecurity clause that significantly increased the range of information that could be defined as CDI and thus needing protection to nearly everything that a major defense contractor uses to perform contracts for DOD. As a result, as specific DOD customers, the Army or Air Force, for example, determine and identify which unclassified information must be protected on contractor networks and in communications between the DOD and the industry supply chain, there has been a tendency to overprotect mundane or basic information with complicated marking requirements. There are over 100 categories of CUI in the National Archives Records and Administration CUI registry, and the guide to marking CUI is 41 pages long. DOD and industry must work cooperatively to identify the unclassified information that is truly important to our national security interests. The current definition of CDI must be refined so that our limited resources can be applied to the most sensitive elements of our unclassified information. With limited resources, if we try to protect everything that is currently considered CDI, we may under-protect the really important things.

My second concern stems from the absence of a unified DOD approach to cybersecurity policy, which has led to different customers within DOD adding requirements beyond the current baseline requirement embodied in NIST Special Publication 800-171. This too often occurs without any engagement with industry regarding the feasibility and costs associated with enhanced agency-specific measures. This lack of uniformity complicates the landscape and adds significant ambiguity as companies are expected to comply with a burgeoning list of service-unique requirements, resulting in segmented infrastructure, limited visibility, and duplication of resources within contractor networks.

Further, industry strongly believes that the customary regulatory process should be followed for these new requirements, with industry feedback leading to a more coordinated and informed rule instead of the ad hoc service-by-service approach that is occurring now.

It is not practical, affordable, or safe for the government and industry to implement service-unique cybersecurity requirements and evaluation criteria because our adversaries will exploit the gaps this creates. We must have a unified approach to apply mass and strength to our solutions. Recently, to align the efforts of several DOD organizations, Under Secretary Lord issued two memos directing Vice Admiral Lewis to perform specific actions for contracts overseen by DCMA. We commend Ms. Lord for her efforts to bring clarity and urgency to DOD cybersecurity efforts. Her memoranda raise complex and important legal and policy issues, however, and it is essential that these be carefully and collaboratively assessed if we are to promote our shared objective of enhanced cybersecurity for DOD programs and the defense industrial base.

I will close by discussing AIA’s most recent tangible response to the cybersecurity challenge. In an effort to advance industry’s partnership with the DOD, late last year AIA released National Aerospace Standard 9933 to provide a better way for our companies to assess their vulnerability to the dynamic cyber threats we face daily. I provided a copy of the paper describing the standard to the subcommittee. It was developed to address two realities facing our industry.

First, while we support having standards and reporting breaches, we have maintained that the DOD’s implementation of NIST 800-171 constitutes a static solution to a dynamic problem. Adversaries are constantly evolving their tactics and consequently there are no silver bullets or one-time solutions that will address the challenges we face.

Second, the dynamic nature of cybersecurity today makes it extremely difficult for small to mid-sized suppliers to create self-sustaining security programs capable of managing the risk posed by advancing adversaries.

To set a viable cybersecurity baseline for the aerospace and defense industry, AIA developed NAS9933, which is built upon the Exostar Cyber Security Questionnaire and information published by the Center for Internet Security. The standard contains five capability levels. Instead of a one-size-fits-all checklist for compliance, this format establishes capability level 3 as a minimum performance level, with levels 4 and 5 as higher-level objectives.

Let me briefly illustrate the different levels.

A company that achieves capability level 3 has a solid performing cybersecurity risk management program and strong technical network protections in place to protect critical information, which make it harder for an adversary to penetrate the company’s systems. This company has demonstrated that it understands the nature of advanced threats and is taking steps to address these threats.

At level 4, a company can detect, protect against, and respond to advanced threats, for example, by using virtual machines and air-gapped systems to isolate and run applications.

A company at level 5 has optimized network protection based on the changing nature of the threat, for example, by requiring multi-factor authentication for accounts that have access to sensitive data or systems.

We intend for NAS9933 to establish the cybersecurity baseline in the aerospace and defense industry and to support government leaders’ efforts to align with industry and move beyond minimal compliance toward greater risk- or threat-based security. As with all standards, NAS9933 is a starting point, and we look forward to developing it further to best aid our industry partners.

To be clear, our standard is designed to serve as a maturity model of best practices for helping companies improve their cybersecurity programs. It is not intended to replace or supersede the government’s mandated controls, nor should it be used as an evaluation tool to score companies and assign ratings. As I have stated, enduring DOD and industry partnerships need to be established and leveraged to continually evolve our collective approach to this problem. The DOD and industry bring unique perspectives, experiences, and equities to the table to address these challenges. Only by working together will we be successful.

Senator Rounds: Mr. Luddy, I am going to have to ask you to wrap it up.

Mr. Luddy: Yes, sir.

In closing, AIA recognizes the national economic security threats from cybersecurity vulnerabilities and shares DOD’s commitment to strengthening our cyber defenses. This issue is simply too important to be handled in a piecemeal approach without an enterprise-wide coordinated strategy. We also need more clarity on definitions so everyone knows what to protect and how. As we continue to work with DOD, Congress, and other stakeholders to address this threat, I hope that we can continue to progress toward a more unified approach across the Department, while also providing DOD contractors the opportunity to provide inputs on proposed approaches and facilitate the most effective, efficient allocation of resources to accomplish the common goal of greater cybersecurity.

Again, thank you for the opportunity to meet today and discuss these issues, and I look forward to your questions.

[The prepared statement of Mr. Luddy follows:]

Senator Rounds: Thank you, Mr. Luddy.

Mr. Peters?

STATEMENT OF CHRISTOPHER PETERS, CHIEF EXECUTIVE OFFICER, THE LUCRUM GROUP

Mr. Peters: Chairman Rounds, Ranking Member Manchin, Senator Scott, Senator Gillibrand, members of the committee, I appreciate the opportunity to be here today.

Over the last 2 years, I visited more than 200 small to medium-sized manufacturers, or SMMs, in the defense industrial base through work on various DOD-funded projects. I helped develop and analyze cybersecurity surveys that reached hundreds more. I have also been involved in the National Defense Industrial Association projects that looked at cybersecurity in the DOD supply chains.

Before I talk about the findings from some of that research, I want to provide an important distinction between information technology, or IT, and operations technology, or OT.

So IT consists of business applications and equipment, such as financial resource planning or enterprise resource planning software. OT includes industrial control systems and software that run machinery on the shop or plant floor.

IT typically uses modern operating systems and applications that are regularly patched and maintained. OT systems often consist of custom applications running on old operating systems, including Windows NT and even DOS. They cannot be easily patched or upgraded, as they may impact production.

In short, the cybersecurity vulnerabilities are considerably greater in OT than in IT. They are easily exploited portals to steal or alter information or even shut down production. One example is Lubrizol where hackers stole intellectual property through the industrial control systems and caused significant financial damage. Another example is a German steel mill where hackers got access to the industrial control systems and prevented the blast furnace from shutting down, causing significant physical damage.

The distinction between IT and OT is important because it represents a significant risk to the industrial base.

So through my work, there are three key findings I would like to highlight.

Number one, the defense industrial base is at considerable risk. My written testimony has quantitative data that demonstrate the lack of awareness and understanding of the DFARS requirements and implementation of the NIST 800-171.

The research shows that SMMs have a poor understanding of cybersecurity in general. They often do not understand the threats much less what to do about them.

This overall lacks of awareness and preparedness should be alarming. Large manufacturers typically have very robust security measures for both their business and operating systems. That makes the less knowledgeable and poorly defended SMMs in the supply chain a greater target for cyber attacks particularly since they often handled much of the technical data sent from those larger contractors. Whether the attack is to steal intellectual property, introduce defects into weapon systems, or to shut down entire operations, the SMMs are prime targets.

Finding number two is that SMMs have been quitting defense work because of the new cybersecurity requirements. Rather than recognizing that these cybersecurity precautions are something that they should take regardless, they perceive the new DFARS requirements as just one more burden that the DOD is imposing.

And finding number three, manufacturers are increasingly frustrated by uneven enforcement. The lack of established metrics against which to measure the level of compliance is viewed by many manufacturers as a weakness that other suppliers will exploit. That perception of inequality or lack of fairness is often a barrier to adoption of costly cybersecurity practices and solutions.

I will highlight three of the recommendations from my written testimony.

Recommendation number one, increase the emphasis on resilience to withstand attacks. One of the most important aspects of this situation is that the threat vectors are always changing, and attacks will happen. Yet, there has been very little discussion about resiliency. SMMs need help understanding how to design resilient OT systems, detect when an attack does occur, and then respond and recover.

Recommendation number two is fuel the rapid development of OT cybersecurity solutions. The DOD should explore innovative means, such as grand challenges, to quickly raise awareness and spur development of OT-specific cybersecurity solutions.

And recommendation number three is develop a means to measure and certify cybersecurity compliance, similar to what you heard before. Manufacturers have to have confidence that their investments in cybersecurity are going to meet DOD requirements. Large manufacturers also need a means to quickly and cost effectively assess the cybersecurity readiness of each manufacturer in their supply chains. That requires the establishment of meaningful metrics that can be readily certified, whether by a customer, the government, or an independent third party.

In summary, the defense industrial base risks are great and much work is needed to mitigate these risks, particularly for industrial control systems. The SMMs do not have the resources to tackle these issues on their own.

They need help if we are to rely on their capabilities.

Thank you for your time, and I welcome your questions.

[The prepared statement of Mr. Peters follows:]

Senator Rounds: Thank you, Mr. Peters.

Mr. MacKay?

STATEMENT OF MICHAEL P. MacKAY, CHIEF TECHNOLOGY OFFICER, PROGENY SYSTEMS CORPORATION

Mr. MacKay: Chairman Rounds, Ranking Member Manchin, and members of the subcommittee, I would like to thank you for inviting me to testify this afternoon.

Progeny Systems is a privately held defense contractor headquartered in Virginia that has just under 500 employees. Progeny is in the category of small large government contractor or perhaps large small government contractor and is a significant target for cyber attacks due to the highly classified nature of our work, as well as the number and types of our contracts. We know that attempts have been made to penetrate our network defenses, and we are fully dedicated to the implementation of the government's recommended policies, procedures, and controls as detailed in 800-171.

As the Chief Technology Officer of our company, I can tell you that cyber defense is a top corporate priority. It is a priority because of the responsibility we have to our customers, and we fully understand that as a small company, our very survival is at stake. We are not a large prime contractor that is, as they say, too big to fail and too big to punish and that our first breach could be the last one.

Most importantly, though, cyber defense is a priority in my company because all of our employees understand as

Americans the threat that adversaries pose. Our overriding goal as a company is providing our warfighters with a competitive advantage no matter the battlespace. We cannot let our nation’s adversaries steal technology that diminishes this advantage, and we have invested heavily in equipment, tools, and manpower to ensure that the NIST specifications are not only met but exceeded.

Thus far, we have only been reviewed by one program office, Team Sub from the Department of the Navy, for compliance with the NIST requirements. We do not, however, have only one program office as a customer. We work for dozens of programs, each of which may have a slightly different interpretation of the NIST requirements. Smaller companies will find it impossible to be rated favorably if they are pursuing two or more differing interpretations of the controls and what is to be considered adequate or complete.

As the committee considers this issue, I would strongly urge you to have one standard interpretation of the NIST requirements. In other words, set the bar high but set it once and hold everyone accountable to that single standard so that we are spared not only the additional cost, but also the need to adjudicate between differing and potentially conflicting direction.

We view the NIST requirements as essentially putting locks on the doors and windows of your house and installing a security system. It is the baseline. It is what you would normally do. These measures are effective in keeping people out of your house who should not be there and letting you know if someone tries to break in. It is a starting point. They are useless, however, if you open the door to a stranger who wants to rob you. And this is where the private sector really needs a lot of help in the human factors area.

We need to raise awareness and to train our own personnel to think of good cybersecurity hygiene as a natural part of their daily work lives. For technology developers who crave connectivity and collaboration, this is a huge paradigm shift. This is especially the case with the younger technology developers who, unlike us, grew up online and are more susceptible to phishing attacks and the other attacks that come directly from the Web.

The guidance provided to date to us has been to seek out peers and share lessons learned. And although we are doing this and it is quite effective, we need to be more effectively confronting the threat. The Department of Defense must take a leadership role, and we need evidence-based best practices, curriculum, and effective training materials to educate our employees to help us train our employees. Cyber defense requires both tools and training to accomplish the mission.

As a small company with limited resources, we feel there is merit to adapting the requirements based on each contractor’s situation, size, and budget included. However, we must protect the technology according to its importance and find ways to help that industry partner, small or large, to protect it. Often the smaller companies like my own who have limited resources also have significant innovations. So we can have the best of both situations if we help those innovators continue to safely protect and pursue their work.

Now, a major tenet of our development community is that no one has all the answers. That is a Team Sub tenet. Progeny Systems received help from the Navy in the form of a 2-day exercise with industry experts in a mock audit of our practices, and it was not just going through the checklist. It was the practical application reviewing our compliance. And the event was eye-opening and invaluable. A standardized, consistent, and regular consultation with experts and red teams like this would probably be the single most beneficial approach that could be offered by DOD to its contractors.

We wholeheartedly agree that providing approved products to the community by the government based on a best of breed selection would be an excellent way to help the community, especially in the case of small businesses if the companies find themselves unable to acquire or develop the right controls themselves.

And in closing, I would like to thank the subcommittee once again for having the privilege to testify before you today, and I would be happy to answer any questions you might have.

[The prepared statement of Mr. MacKay follows:]

Senator Rounds: Thank you, gentlemen. I most certainly appreciated all of your comments.

Normally our tradition here is that we will work our way around the committee, and we will try to stick to 5 minutes within our assigned times. And I will begin my questioning at this time.

Gentlemen, section 1644 of last year’s NDAA, National Defense Authorization Act, required the Secretary to promote the transfer of appropriate technology, threat information, and cybersecurity techniques developed in the Department of Defense to small manufacturers and universities and then to establish a cyber counseling certification program and to develop a regime of voluntary self-assessments.

I would like to know if each of you -- number one, are you aware of the program. Second of all, how could this program be strengthened if you are aware of it. And finally, how should this program be expanded and shaped if it is successful? Dr. LaPlante, would you like to begin?

Dr. LaPlante: Yes, I have heard of the program. I think it is a great idea.

I think the central thesis here is we really have education to do. It is a lot about education. A lot of us believe the best ideas will come from the small businesses once they understand it.

And so an example of what is happening right now, there is something called an adversarial, for lack of a better word, attack vector. It is not unlike a criminal casing out your house. There is a series of things that an adversary in cyber does to look at you, to do reconnaissance, then to penetrate, get in, and then do whatever they are going to do, either put something in there, do damage, take something. Believe it or not, there are about 150 steps that people have outlined of how this is done, and it changes about every week.

What MITRE has done -- and other companies have done the same thing -- is we made that publicly available. So if you want to know how to prevent the guy from getting in your network, this how he does it. This is what the criminal does next, then that. Oh, now if you plug this, he is going to go over here. And what is good about that is that you start getting the defenders to be very sophisticated.

And people say, well, gee, publishing that is bad. People will learn how to do cyber. Well the people doing it on cyber know how to do it. And our rule of thumb in making it an open source, if it is open source already and published about a threat vector, we will publish it. And so there are things like that that if you go to the programs, Senator, that you described and we can get people to understand this is how the threat thinks, and you want to do things that makes his job hard.

Senator Rounds: Mr. MacKay, same question.

Mr. MacKay: I completely agree with the doctor’s comments.

The first thing that I want point out is we are in a situation where you are not paranoid if somebody is actually out to get you. And we need to start thinking about the fact that we should be paranoid. We should be paranoid in a constructive way.

We have been on the receiving end of a great deal of this kind of information, some of which has been provided in a classified setting, and the more information that can be sanitized out of that kind of a report and put into a format that can be published company-wide as open source, as completely open to our employees so they understand the techniques and the methods, the better for us because we cannot get classified meetings put together that easily or that quickly.

Senator Rounds: Thank you.

Mr. Peters?

Mr. Peters: I am not aware of that program directly, and none of the suppliers that I have talked to have ever mentioned that program. If an element of that program is to promote education, disseminate information to the defense industrial base, that is certainly a positive thing.

My one recommendation would be that it needs to be done directly to the small to medium-sized not just through the OEMs or prime contractors.

Senator Rounds: Thank you.

Mr. Luddy?

Mr. Luddy: I am not familiar with that program by name either, Senator, but I do know that Under Secretary Lord has taken a pretty aggressive look at how, together with the large primes, we can work to support the middle and lower tiers of the industrial supply chain to be secure. We recognized this early on when the NIST standard was initially promulgated that while the big companies were essentially almost entirely compliant immediately, that the middle and lower tiers were going to have a more challenging time. Now, to a large extent, our prime contractors work very hard with their supply chains to do that.

One of the good ideas I think that the Department is looking at is the prospect of actually providing people and cloud-based capability to the middle and lower tier companies to help them understand the threats and meet the requirements of security that are out there. So we support that very much.

Senator Rounds: Great. Well, I think the Achilles heel in this whole process is that we want to use lots of different subcontractors. In many cases, some of our most innovative contractors are those subcontractors that are small. We do not want to lose their capabilities and what they have to offer. And yet, we have to have a program in place that allows them to assure us of the best types of protections that we can possibly get with regard to cybersecurity so that there is a standard of acceptance and a standard of capability that is there regardless of the size, and how we go about getting there is part of our challenge today.

Senator Manchin?

Senator Manchin: Thank you, Mr. Chairman.

Maybe you can break this down to me. Basically most of the contracts that go from DOD are given to larger contractors. Correct? So the smaller subcontractor has to go through -- no matter how great their idea, innovation, creation may be. They usually, very seldom ever get directly a contract from DOD.

Mr. MacKay: If I could offer a differing perspective, Senator. Progeny Systems is a prime contractor to the Navy for a number of very important programs, including the cybersecurity controls for the submarine.

Senator Manchin: So you have a direct contract.

Mr. MacKay: We have a direct contract.

Senator Manchin: So I would say you have to meet certain security guidelines and have people that have been cleared, security clearances. Right?

Mr. MacKay: Yes, sir.

Senator Manchin: Are you having problems getting your clearances?

Mr. MacKay: No, sir, we do not.

Senator Manchin: I understand there is a backlog of security clearances.

Mr. MacKay: There is.

Our biggest effort, though, is we have to do the same controls and we have to be just as careful as the large companies on a small company budget.

Senator Manchin: Well, I am saying that everyone should meet the same standards you are meeting. I do not understand why we let the small contractors get by just because they are small. I do not know why we do not hold the larger contractors, who are responsible for the contract, to make sure the subcontractors they are hiring have protections.

Mr. MacKay: Yes, sir.

Dr. LaPlante: In my experience, Senator, when I was acquisition executive, the knowledge a lot of the primes had of their detailed supply chain was very mixed, surprisingly so. And some of that is on the government.

Senator Manchin: Was very what now?

Dr. LaPlante: Surprisingly uneven, even knowledgeable of who is a sub to who and what contracts they have.

Senator Manchin: Who hires the subs?

Dr. LaPlante: Usually the prime.

Senator Manchin: The prime is hiring people. They do not know who they are?

Dr. LaPlante: No. The primes hire people who they are, but sometimes when you look at the contract between the prime and the subs -- the government may not have access to it -- you find out the contract may not have the requirements in it for quality or something else.

Senator Manchin: Is that the way that the contracts are written?

Dr. LaPlante: They can be. They can be. It depends on the contract.

Senator Manchin: So basically a contract from the Navy or Air Force --

Dr. LaPlante: No. What I am talking about -- I am sorry, Senator. This is a contract between a prime and a subcontractor, not between the Navy and the prime.

Senator Manchin: No. I am saying is, first of all, if I put the criteria that I want every contractor to meet if they bid and they were successful, I do not care who does the work. They have to meet this criteria.

Dr. LaPlante: You absolutely could do that.

Senator Manchin: But we are not doing that now.

Dr. LaPlante: I am saying it is uneven. But I defer to my colleagues. But I was surprised at how uneven the --

Senator Manchin: Just trying to get a handle on this.

Okay, go ahead, Mr. Peters.

Mr. Peters: Senator, so there are two challenges. First of all, there are a lot of companies that I know of, small machine shops, that have multimillion dollar contracts directly with the government that are not cleared, but they are producing things that help keep airplanes flying and tanks --

Senator Manchin: Are those all confidential?

Mr. Peters: No. They are still critical. You still have critical --

Senator Manchin: Yes, but I mean, everybody knows what the part is and who is making it.

Mr. Peters: Right.

But the issue with the contractors -- one of the challenges is that if I have got a supply chain -- there are 23 different contractors that make the primary shaft for the Chinook helicopter. 23 and that is just for the primary shaft.

Senator Manchin: Just the shaft.

Mr. Peters: So the problem is that the prime contractor knows who their immediate supplier is. They do not know who is beyond them, third, fourth, fifth tier and so on. You have flow-down requirements.

Senator Manchin: Why would they not?

Mr. Peters: Because the contractors, especially the prime contractors, consider that to be their private information. If I let you know who my contractors are and who my supply chain is --

Senator Manchin: That is the person you will bid against them the next time.

Mr. Peters: Exactly.

Senator Manchin: I really do not care.

Mr. Peters: I agree.

Dr. LaPlante: Your points are well taken. We are just describing how it is.

Senator Manchin: We can change that.

Dr. LaPlante: You can change it. That is right.

Senator Manchin: We are all on committees that can change contracts.

Dr. LaPlante: That is right. But the knowledge of the primes, to the point, of the sub to the sub to the sub is uneven.

Senator Manchin: That is awful. That is absolutely unbelievable.

Mr. Luddy, do you have anything to add?

Mr. Luddy: I was just going to add, Senator, that I believe the legal concept here is of contract privity. And a contractor has privity with its immediate subcontractors, but not with that subcontractor’s subcontractor.

Senator Manchin: Somebody has to be held accountable.

Mr. Luddy: These are the kinds of things that I think we are trying to work through, and DOD is trying to work through.

Senator Manchin: Would you all be objectionable if we wrote the standard of how contracts are let to the prime?

Mr. Luddy: I think we are concerned about anything that will inhibit good information sharing about the --

Senator Manchin: Right now, there is no information sharing. If you are a prime, you do not know who the subprime or the subprime to the subprime.

Dr. LaPlante: Senator, I think what you are getting at is the following, and I think this would help tremendously. Holding more accountability to their supply chain and knowledge for the primes, however we do it and dealing with the legal issues, that would be greatly helpful.

Senator Manchin: It is mind-boggling.

The private sector does not work this way. Does it? The private sector does not work this way that I know of. I have been in business a long time. I have never seen private contracts working this way. Someone is held accountable and responsible all the way from the top to the bottom. Right here you can pass the buck all day long.

You take a shot at this.

[Laughter.]

Senator Rounds: Okay. Let me offer an alternative once. If anybody who was providing anything to a contractor or a subcontractor or, for that matter, anything down the line, was simply identified as being responsible to a certain standard or who was subject to audit so that it was not necessarily knowledgeable to the other subcontractors or other contractors that this was their supply chain, but rather that they were a licensee to perhaps the Department of Defense to where there was a standard that they had to meet, would something like that be an alternative so that you had an entire base of perhaps thousands of subcontractors who had met a particular criteria that would then be allowed to be within the chain? Is something like that available, or has that been tried to the best of your knowledgeable?

Mr. Luddy: Senator, that is one of the objectives of our standard is to try to have within industry a self-regulating effort to set levels of cybersecurity so that a prime will know going from one subcontractor to another that these companies have met levels of security. In the case of the NIST standard now, which requires system security plans and programs to remediate any security flaws, those can be audited. That presents a resource problem for the Department of Defense, which has a limited number of resources and people to apply to auditing, but that is a possibility.

We are concerned about the prospect of the SSPs and POEMs, as they are called, being automatically provided or provided just on a widespread basis because they contain, frankly, sensitive information about a company’s economic viability, security viability, and so forth. They can have real implications in the business sense for what our companies need.

Obviously, there is always the option of an audit, but it is a resource challenge for the Department.

Dr. LaPlante: Mr. Chairman, I would add to what my colleague said this following concept. Once you have such a list that you described, then it is really important to have this active like counterterrorism center to watch the list, watch what changes. We found in similar things some of the worst problems happened when overnight somebody on the list that had been approved gets bought by somebody else. So you got to be very active in watching it, but it could work.

Senator Rounds: Mr. MacKay, I have a question for you. You are a small contractor.

Mr. MacKay: Yes, sir.

Senator Rounds: Yet, clearly you have been successful. Do you employ other subcontractors to you?

Mr. MacKay: Yes, we do.

Senator Rounds: Can you describe for us the process that you have to work through in order to qualify them so that, within your own guidelines, you are comfortable that they have met certain standards?

Mr. MacKay: Yes, Senator. When we have a particular contract to satisfy, we consider industry partners. One of our approaches is to have specially selected industry partners that we work with almost exclusively so that we have better control over their own security practices. And rather than relying on their resources and their infrastructure for things like security controls, we bring them into our IT infrastructure and our project infrastructure so that they are using our controls when they do development on our projects. So we try to encapsulate their work into our way of doing the NIST controls and keeping things safe.

But to the points of the other gentlemen, we have machine shops that we hand off work to. And, you know, Junior Smith has a laptop that he has used on his lathe since forever and you got to try to explain to him that he has got to be more careful. So what we have to do is flow down help to those people so that we give them information in a form that cannot be or is more difficult to be compromised. And I think that is a model that we can pursue.

We are a contractor, subcontractor of Lockheed Martin, and Lockheed Martin assesses us the same way that we assess the people that work for us. So the flow-down is critically important, and each step of the management process has to take ownership. But the guy at the top who has the prime contract has to take on the responsibility of seeing things all the way down to the bottom, and they have to ask the hard questions.

Senator Rounds: And I think that is the part that Senator Manchin was bringing up was, how far down is that, because as you have indicated, you go down to, even in this case where you have a subcontractor, who may very well be using a separate subcontractor themselves, who is simply machining a particular part -- they will have competencies and capabilities that are at least at risk with regard to that particular product that they are supplying to your subcontractor.

Mr. MacKay: Exactly. Yes, it is a very difficult problem, and we have spent countless hours worrying this issue because it gets very complicated very quickly. If I hand a document over to somebody to create a part, then I have to ask them how they are going to be managing that document and who they are going to give it to. They could lie to me. They could say, yes, we are going to do this and at the last minute, hand it off to somebody who came at a lower bid and not tell me. We have to find a way to go back to them and say, so you just delivered this part. Look me in the eye and tell me that you did not change our approach. We can cancel the contract. We can fire them. But to be absolutely sure they did not --

Senator Rounds: By then, it is too late because that has been entered into the supply chain.

Mr. MacKay: Yes. So it is a very difficult problem. I think we have to do as much as we can to take responsibility for what we can see and the contracts that we let, and we should be held responsible absolutely when things go wrong. We go to the limits I think of what we can reasonably do in the execution of our contracts. But it is not going to be infallible.

Senator Rounds: Thank you.

Senator Manchin, your turn.

Senator Manchin: It is probably best that I do not say a whole lot.

Just call the Chinese and ask them how they did it. It is pretty easy. This is not hard to follow right now. I think a blind person can follow this. We wonder why we have been hacked so much, why they have copied everything. You all just explained it. There is no checks and balances. It looks like to me that we are protecting a business model more than we are the security of our country. That is it in a nutshell I think. You are afraid somebody else is going to come and get somebody else, and if they do, they will go around that person to get them directly and take them out of this chain. I see that.

I mean, I used to write RFP's all the time. An RFP is an RFP, request for proposal, and here is how it is going to be done. If you do not do it, you are not in compliance. You will be held liable, be sued out the ying-yang because you broke it. Do you sign RFPs?

Mr. MacKay: Yes.

Senator Manchin: And you agree to the terms of the RFP?

Mr. MacKay: Yes, we do, Senator.

Senator Manchin: Do you have people sign RFPs to you?

Mr. MacKay: Yes, absolutely.

Senator Manchin: Have you ever gone after someone legally?

Mr. MacKay: To my knowledge, we have not, but the T in my title does not usually give me insight into the business side of --

Senator Manchin: I would say there would be different types of categories. The Defense Department is going to be required to do some things that are not top secret, and some things that we have are top secret and we hold primes responsible in different ways because of what we are working on. But I would think everybody in that food chain is going to be held to the highest standard, but you are telling me it does not work that way as it goes down the food chain. Correct?

Mr. MacKay: Well, Senator, I think that we hold everybody to the highest standard that we physically can control because we know what we know, and if somebody decides to go around our back and go to a different supplier -- they go to China for a part or they go somewhere else that compromises the information -- and they lie to us, we have to be able to have a way to find out that they have done that. That is a difficult proposition.

Senator Manchin: If they have to make all their software and everything applicable to your RFP, they got to turn everything over. It should not be too hard to track it.

Mr. MacKay: That would be great.

Senator Manchin: Tell me what you need. Just tell us. That is why you are here. We are here to fix it and you are here to tell us what is broken.

Mr. Luddy: Senator, I would say two things in response to the very legitimate concern you are raising.

One is that there should be a threshold security that everybody needs to meet. I think our standard is an effort to do that. The DOD made an initial effort to do that with

800-171. And both of those efforts are going to continue and I think strengthen. We all have that objective.

Another thing that I alluded to in my testimony is that right now there is perhaps an over-sharing of information across programs. Somebody working on a bolt does not necessarily need the same level of information from the government as somebody working on a guidance system or a navigation system, for example, to oversimplify it. So the Department I know is looking at that. I think that would be a welcome way to deal with it.

So I think the more that we can control and define the kinds of information that get transferred, the smaller bucket of the problem we will have.

Dr. LaPlante: Senator, just a couple, two points really quick.

One is an idea that sometimes comes up -- and it is not perfect -- is there are some programs where we just do not reveal the suppliers. Period. When I was Assistant Secretary, we ordered the bomber for the Air Force. At the press conference, they said who is building the engines. We said we are not telling you. Now, of course, we do not think the Chinese will at some point figure that out. But there is something about protecting things that you would not think would be protected. So that is one point.

The second point is -- and it is where you are going.

I will draw an analogy. When I was Assistant Secretary, when I had a frustrating problem in a program, a missile, and it was failing, we would find out it was not the prime. It was a sub to a sub of the prime. Well, I still held the prime accountable. I do not think there should be any difference with this.

Senator Rounds: But by then, it is too late. Is it not?

Dr. LaPlante: Oh, it is. But it is well known that the prime knows that if the IMU on the missiles failing made by a mom and pop shop, that is in their incentive contract for the prime. So why is it not the same for cyber? That is the question.

Mr. Peters: So, Senator, there are two points I would make. This situation is much worse than many people realize.

One is that -- you are absolutely right -- the flow-down requirements, while they do flow down, as you get to the smaller to medium-sized manufacturers, they do not always take the time to read them, to conform to them. I have been through flow-down requirements that still have Y2K provisions and anti-segregation provisions in them. So it gets very confusing. They get very long. It is hard to do.

The other challenge we have is that the DOD makes all information, contractual and transactional information, public, 90 days delayed, but it is still public through several databases. There are companies that aggregate all of this data and actually sell it in 37 different countries. So all that data is out there. I can find the suppliers that make parts and pieces for any aircraft, any ship, any land vehicle. It essentially provides a blueprint of if you want to go after a certain weapon system, whether to get information and steal it or to --

Senator Manchin: Do they give you an email account on it too?

Mr. Peters: Pardon me?

Senator Manchin: Email accounts on that too so you can go right to it easily to hack?

Mr. Peters: Maybe not quite that level, but they do have the contract information through SAM, System for Award Management, for all of the contract --

Senator Manchin: Let me just bring up something, if I can, real quickly.

You all are here because you understand the system much better than we do. We know something is wrong. China could not have the success they have had in such a rapid amount if it had not been for us. We all know that, and we know what they do on a daily basis. We know what Russia is doing. We know what all these countries are doing. If you have been on Intel and you have been on Armed Services, you are going to get the flow.

Nobody is willing to step to the plate and fix it. Now, there has to be -- you are shaking your head thinking we have got to be the stupidest people in the world to let this happen. And that is what we are saying. We do not want you to jeopardize your business, your contracts, or anything. But somebody has got to come and we have got to put a stop to it.

Senator Rounds: Let me follow up. It would appear to me that within the Department of Defense not only do we need a consistency from one department to the other, but there has to be a way of communicating so that the challenges that you face and the challenges that we are learning about as we move through and that we are now trying to publicly share with a committee meeting like this in the open -- and as you know, most of our Cyber Subcommittee meetings are in a classified setting because we do not talk about this. We decided intentionally to do this one in the public so that we could draw attention to how serious this was and to also suggest something else, and that is that you need to have a way in which you can communicate with the Department of Defense.

Today, as you work your way through this process, clearly this is not something that you have not thought about before. Clearly it is something that you are aware of and you had concerns or you would not be here.

When you look at these things, is there a way today in the system for you to share with the individuals that you contract through the Department of Defense, through the different branches and so forth, different offices, procurement offices -- is there a way for you to share and express and participate in trying to improve the acquisition process? Is there a process there right now that you are aware of?

Mr. Peters: So, Senator, again, I spend most of my time with small to medium-sized manufacturers in the defense industrial base. When I let them know, though, I was going to be testified, I was overwhelmed with issues they wanted me to raise, and I got a list this long. I had to really boil it down.

The challenge is that there are some venues to do that. However, what we find is that most of the manufacturers -- I focus on manufacturing. Most of them are reluctant to say anything, whether it is directly through the DOD, through procurement technical assistance centers, any of the different kinds of venues they have, because they are afraid of reprisal. I have a number of horror stories of reprisal from the DOD because somebody spoke up, they raised their voice.

So unless there were some way for you to gather this information anonymously -- and that is one of the reasons I get a lot of this insight. When I do my research, I promise the subjects anonymity. They spill the beans. But unless there were some way for you to do that, either through a university that was doing this research or through some independent third party, I think you are always going to have this fear of reprisal.

Senator Rounds: You know, NASA actually has a program for pilots who, when they see something that is unsafe within the system, there is a form that a pilot can fill out. Basically even if they messed up on a federal aviation regulation or if they have done something, as long as they fill that form out and advise through NASA that there is a safety issue involved in a particular place, whether it is going into a particular airport, working under a particular type of airspace, or whatever -- when they fill that out and send it in, this is what is used to actually make the entire system work better long term. What you are saying is that really does not exist right now within the defense acquisition system. But perhaps something along that line may be --

Dr. LaPlante: Yes, Mr. Chairman. I think there is also a program very much like you described called ASIAS with the FAA, that the airlines have gotten together and they have agreed to have a safe sharing environment by pilots. There is something to that.

I draw the analogy. When you have an air incident in the Air Force, they first get the root cause, and the people that are talked to, complete immunity. You say whatever you want. They do not do the punishment thing. They want to get the facts. You separate that later if you say we need to do some discipline, do that later with a different group. But it is to foster that environment that you are talking about.

Senator Rounds: One other item that comes to mind as I listened to the discussion here. The thought that there would be reprisals coming back through DOD for a subcontractor or a business entity to report something which would be a threat to national defense is of real concern. And while we are not naive enough to think that that may not be occurring, it seems to me that some of that has to do with the culture within the different organizations.

I would call to mind most recently the Department of the Navy just put out their current cyber analysis, and they were, in my opinion, very straightforward, and they went into some detail about their own challenges. In a way, it was like going to confession. But they did more than that. They actually recognized that they are an information operation. They may have a goal of getting 355 ships, and it is not the fact that our near-peer competitors are stealing our ships. They are stealing our information. And if we are going to protect our ships with all sorts of systems, what is it that we are doing to protect our information, which clearly is just as valuable, if not more valuable? And I think that openness on the part of the Department of the Navy is something that may very well suggest the changes needed within the culture not just of the Navy but elsewhere within DOD as well.

And I am seeing heads nodding, but I would love to have your thoughts that perhaps that is part of the discussion that we need to participate in.

Mr. MacKay: Senator, I can contribute that our experiences with the Navy, and in particular Team Sub, has been that they have grabbed this problem by the horns. I think there would be repercussions if we did not report issues that we are seeing in cyber defense and in the way that they are conducting their activities and looking at the problem. They are pushing us. They are teaching us. They have really taken the forefront.

But I think the discussion across the board here shows how it depends on each Department of Defense and each program office even, and you do not have a consistent approach across the board. Something that pushes down from the top that sets policy and sets the approach would be very valuable. I would offer the Department of the Navy as a good example of how it should be done because we have had nothing but encouragement and help from our Department of Defense partners.

Dr. LaPlante: I would also say there is a part of the Navy -- and this is a culture thing -- the submarine Navy. And they have a culture maybe because they are nuclear trained of get the facts. Do not just look to shoot somebody. And there is a famous admiral who ran SSP, which is the submarine ballistic missile part of the navy. Malley’s Rules. Rule number one is tell bad news fast. It never gets better with age. You got to have that in the culture. And I think you are seeing some of those glimpses. If we could get that out there more on this topic.

Now, at the same time, you want to hold people accountable. So you have to reconcile how you do both at the same time. It can be done.

Mr. Luddy: I think Dr. LaPlante is highlighting something really important. This does raise a tension, though, between the very important information sharing about threats, breaches, methods of addressing threats that we are trying to promote within industry and between industry and DOD, on the one hand, and the well-intentioned prospect of making levels of cybersecurity a matter of differentiating in contract and source selection. I understand where that comes from, and there is something to be said for it. But we just have to balance that with anything that will cause companies, for reasons of competitive advantage or disadvantage, to not share the details or specifics about a problem that they are facing across the companies. Right now, I think certainly at the higher levels, our companies do a good job of exchanging information and collaborating on how best to meet the threat. We do not want to put anything out there that discourages that.

Senator Rounds: Thank you.

Joe, anything else?

Senator Manchin: No.

Senator Rounds: Gentlemen, first of all, your full statement is a part of the record. We most certainly appreciate your participation here today. I am sure that we are going to be doing something along this line once again. But I would like to, once again, on behalf of the subcommittee, thank you all for your participation and your frankness. I think this goes a long ways towards informing the subcommittee and then the committee of some ideas or some processes that can be explored with regard to improving not just the culture but the overall process for addressing the issues of cybersecurity within the Department of Defense.

With that, Senator Manchin, anything?

Senator Manchin: No. Thank you.

Senator Rounds: Very good. We will call this subcommittee to a close. Thank you.

[Whereupon, at 3:36 p.m., the hearing was adjourned.]