Stenographic Transcript
Before the

Subcommittee on Cybersecurity

COMMITTEE ON
ARMED SERVICES

UNITED STATES SENATE

HEARING TO RECEIVE TESTIMONY ON
THE DEPARTMENT OF DEFENSE'S
CYBERSECURITY ACQUISITION AND
PRACTICES FROM THE PRIVATE SECTOR

Wednesday, November 14, 2018

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 DEPARTMENT OF DEFENSE'S CYBERSECURITY ACQUISITION AND PRACTICES FROM THE PRIVATE SECTOR

Wednesday, November 14, 2018

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

The subcommittee met, pursuant to notice, at 3:01 p.m. in Room SR-222, Russell Senate Office Building, Hon. Mike Rounds, chairman of the subcommittee, presiding.

Subcommittee Members Present: Senators Rounds [presiding], Fischer, Gillibrand, and Blumenthal.

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

Senator Rounds: The Cybersecurity Subcommittee meets this afternoon to receive testimony on the Department of Defense's cybersecurity acquisition and the practices from the private sector.

Our witnesses are Mr. Dmitri Alperovitch, Co-Founder and Chief Technology Office, CrowdStrike; Major General John Davis, U.S. Army, retired, Federal Chief Security Officer, Palo Alto Networks; Mr. Francis Landolf, Principal, Core Consulting, LLC; and Mr. Ron Nielson, Vice President and Chief Technology Officer, Parsons Corporation. Let me just begin by saying thank you to all four of you for coming in today and visiting with us. It is greatly appreciated.

Every single day adversaries attack the Department of Defense through cyberspace attempting to gain critical information about our ongoing operations, weapon systems, and service members. These attacks are only as successful as the Department's cybersecurity capabilities and practice allows them to be.

And to its credit, the Department possesses many extremely effective operators, program suites, and mitigation tools to protect its networks and computing infrastructure. However, the Department's cybersecurity and cybersecurity operations are decentralized, which means that

certain DOD components exhibit better cybersecurity than others. In other words, the Department has produced pockets of excellence within the DODIN, or the Defense Information Network, but opportunities remain for the Department to improve its cybersecurity capabilities and practices across the enterprise.

For example, the Department's centralized cybersecurity operators, the Defense Information System Agency, often lack visibility into networks across the Department. Further, the Department's cybersecurity operators, including CYBERCOM's cyber protection teams and the thousands of IT cybersecurity specialists maintaining the Department's networks are not particularly well integrated with each other or with the cybersecurity capabilities used across the Department.

The Department's cybersecurity acquisition is slow, decentralized and often over-reliant on the National Security Agency's product evaluation and indigenous production, and because of this, the Department's capabilities often pale in comparison to the best available in the private sector.

While we have confidence that the Department will bolster its cybersecurity in due time, we believe that this improvement could come as a result of improved cooperation with private sector cybersecurity companies and

reconfiguration of the Department's cybersecurity capabilities to match the state-of-the-art offerings in the private sector.

We hold this hearing today to find out how the Department and the Congress can achieve these advances. We look forward to our witnesses' commentary on questions to include: Where are the Department's cybersecurity capabilities, architecture, and operators lacking as compared to the cybersecurity leaders in the private sector? What capabilities can the private sector provide to fill these gaps? And how are the Department's acquisition processes and cybersecurity policies failing at cybersecurity?

With that, once again, thank you, and I would turn to my colleague, Senator Gillibrand, who is here, as Senator Nelson is not available today, but Senator Gillibrand, welcome and any comments you may have.

STATEMENT OF HON. KIRSTEN GILLIBRAND, U.S. SENATOR FROM NEW YORK

Senator Gillibrand: Thank you, Senator Rounds. I join you today in welcoming our witnesses as we discuss the critical topic of securing the nation’s networks. I am sitting in for Senator Nelson who is unable to attend today, and I ask unanimous consent to enter his opening statement for the record.

Senator Rounds: Without objection.

[The prepared statement of Senator Nelson follows:]

[SUBCOMMITTEE INSERT]

Senator Gillibrand: I want to start by stating how essential I believe today's topic is and how important it is to ensure that our government's approach to cybersecurity leverages the best of the private sector. We have long understood that the future of warfare is both online and in the physical world, and in the past few years, we have seen an increase in both the tempo and the level of cyber attacks. Our adversaries are on the offensive. We now understand the alarming extent to which Russia has undermined our election process, China's ability to use cyber tools to obtain our most cutting-edge technology, and the many foreign governments and private actors that have threatened our private and public sector infrastructure.

Cyber obviously does not have geographic or bureaucratic boundaries. Yet, our government still often operates as though it does with inadequate threat sharing and analysis between federal agencies with different missions and between federal and State authorities.

We have also had a hard time attracting and retaining talent, a critical issue in the area, and I know we will particularly hear today about the difficulty we still have in procuring the most up-to-date resources and in ensuring that our defense contractors fully secure their networks.

I want to thank the chair, Senator Rounds, for holding this hearing so that we can hear from these experts their

recommendations for improving the nation's cyber defenses, and thank you all for your time.

Senator Rounds: Thank you, Senator Gillibrand.

The way we would like to do this today -- each of you has a full opening statement. That will be a part of the record. We would ask each of you to perhaps do a 5-minute statement in front of the committee now, but once again, your entire message will become a part of the record, without objection.

At this time, I would simply work our way down the row. The process after you have completed your 5-minute messages -- we will take turns on either side, 5 minutes apiece back and forth, and kind of move from there. Hopefully, we will have other members of the committee who will also be participating as well today.

And with that, Mr. Alperovitch, if you would like to begin

STATEMENT OF DMITRI ALPEROVITCH, CO-FOUNDER AND CHIEF TECHNOLOGY OFFICER, CROWDSTRIKE INC.

Mr. Alperovitch: Thank you. Chairman Rounds, Senator Gillibrand, thank you for the opportunity to testify at today's hearing.

I co-founded CrowdStrike more than 7 years ago with a mission to stop cyber breaches. Today it is one of the world's leading cybersecurity companies and protects thousands of enterprises and government networks across over 100 countries. On a daily basis, we engage in virtual hand-to-hand combat with sophisticated adversaries from global criminal groups to nation states such as China, Russia, Iran, and North Korea. Our job is to use cutting-edge technology to hunt such adversaries and eject them rapidly from customer networks before a breach occurs. We are exceptionally good at this job, and I am here to offer you a perspective based on this experience.

The Department of Defense faces a similar challenge to that of the private sector. The very same threat actors that are targeting private industry today to steal intellectual property and sometimes carry out destructive attacks are trying to break into DOD networks to conduct espionage and degrade our warfighting capabilities.

In facing this threat, DOD has a number of advantages. DOD's cybersecurity operators are every bit as talented and

motivated as their private sector counterparts. In fact, some of the best people we have at CrowdStrike have backgrounds with the Department and our military services. As a nation, we have also applied significant resources to DOD cybersecurity. There is likely no organization on the planet that spends as much on cybersecurity as the Department.

Still, the private sector has the advantage of operating in the relatively unconstrained commercial environment. The environment has fostered agile responses to our shared threats that outpace DOD's capabilities in some notable ways. The most capable private sector organizations have succeeded by maintaining a primary focus on rapidly detecting and ejecting adversaries from the networks which they are infiltrating on an almost constant basis.

I believe that applying a similar focus to DOD's defensive mission will advance the Department's ability to protect its enterprise and thus the security of our nation. The three most important strategies DOD should utilize to gain an upper hand in this fight are hunting, cloud technologies, and what I call the 1-10-60 rule.

First, DOD needs to refocus on continuously hunting for adversaries on their networks. Much of what the Department does today is cyber hygiene. Implementing security controls

is hygiene. Patching vulnerabilities is hygiene. Building an asset inventory is hygiene. No matter how good the Department gets at these tasks, they alone will not accomplish the most important mission: stopping foreign intelligence and military services from countries such as Russia and China from breaking into our networks. Let me reiterate this critical point. Good cyber hygiene will not stop determined GRU or PLA cyber actors, just as having locks on the door of a house will not stop Navy SEALs from getting in. And too often these hygiene efforts come at the expense of hunting down and ejecting adversaries that are likely already in the network.

Hunting is less labor intensive than it may sound. For example, CrowdStrike's OverWatch service, which hunts 24/7 across thousands of networks and millions of machines around the world that make up our entire customer base, is comprised of approximately 20 people. We do have top-tier talent in these roles. Our customer environments are well instrumented, and we have architectures in place to support the mission. But DOD can use similar capabilities and ramp up these hunting operations without an enormous personnel mobilization effort.

Second, the private sector has successfully deployed cloud-based security technologies to flip the asymmetry between offense and defense. Once a threat is identified in

one part of the network, cloud-based security technologies can instantaneously distribute protection across the entire ecosystem. With millions of systems under management, DOD can leverage cloud systems to turn its scale into a strength rather than a challenge.

Last, what DOD and, frankly, the Federal Government as a whole needs most is to define a new high-level defensive concept that drives measurable accountability. I suggest a model I developed at CrowdStrike called the 1-10-60 rule. This rule is derived from the premise that to win a battle in cyberspace, speed is paramount. The only way you beat an adversary is by being faster than them. The very best private sector companies we work with strive to detect an intrusion on average within 1 minute, investigate it within 10 minutes, and isolate and remediate the problem within 1 hour. 1-10-60. And there are industry organizations that achieve that level of rapid response routinely.

These numbers are important because CrowdStrike research shows that it takes an adversary on average an hour and 58 minutes, almost 2 hours, to break out of the initial system they comprise on the network and access other sensitive resources. If you contain or eject them within that window, you have stopped the breach. The 1-10-60 rule can be used to measure the efficacy of DOD's cybersecurity programs and enhance accountability.

DOD must prevail in its mission to defend and secure its IT enterprise. Failure is not an option. Refocusing on hunting, wider and faster adoption of the cloud, and the use of the 1-10-60 rule can help.

I have focused my testimony today on concepts rather than technologies, but everything I have described is achievable through practices and capabilities that are widely utilized in industry. DOD can adopt these capabilities and, by enhancing its own security posture, strengthen national defense.

Thank you again for inviting me to testify today. I look forward to your questions.

[The prepared statement of Mr. Alperovitch follows:]

Senator Rounds: Thank you, Mr. Alperovitch.

Mr. Davis, General Davis, please.

STATEMENT OF MAJOR GENERAL JOHN DAVIS, USA, RETIRED, FEDERAL CHIEF SECURITY OFFICER, PALO ALTO NETWORKS

Mr. Davis: Thank you, Chairman Rounds and Senator Gillibrand, for your leadership in this critical issue.

It is my honor today to discuss with you innovation in the cybersecurity industry and how DOD can better leverage this innovation in order to improve its cybersecurity posture.

I joined Palo Alto Networks a little over 3 years ago after 35 years in the U.S. military. Most of that time was spent in special operations and information warfare, but the last decade I spent in assignments dealing with cyber operations, cyber strategy, and cyber policy. So I believe that I bring a unique perspective to innovation in both the commercial cybersecurity industry, as well as efforts at DOD, to successfully leverage innovation in cybersecurity.

I should point out that Palo Alto Networks collaborates extensively with key stakeholders across the U.S. Government and internationally with like-minded governments in addition to DOD. We believe being a good partner with the Federal Government is critical to our mission of defending our way of life in the digital age by preventing successful cyber attacks.

Before I discuss innovation in the cybersecurity industry, I want to point out two big challenges that I

think innovation must address.

The first is the adversary. We live in an environment that overwhelmingly favors the attackers. As the cost of computing continues to decline, adversaries are able to conduct increasingly automated successful attacks at minimal cost. The network defender is generally relying on legacy security technologies that are often cobbled together as point products that solve discrete problems but do not work together well. This increases complexity and it creates a dependence on people, often the least scalable resource in an organization, and it requires the people to manually defend against these automated, machine-generated attacks. Network defenders are losing the cybersecurity battle because they are bringing people to a software fight. It is like bringing a knife to a gunfight.

The second challenge is that the world of technology and the world of cybersecurity are moving in opposite directions. Our digital world, IT, operational technology, and even the Internet of Things, is getting simpler and easier to use, more connected by design with automated functions requiring fewer people to execute and overall more convenient. On the other hand, the security world is producing more products operating in individual silos not interoperable with other security products and continuing to rely on human decision-making and manual response, overall

creating a slower, less efficient, and more complex environment.

To turn this around, the cybersecurity industry needs to leverage the example of the smart phone and the application experience. Some of your news, sports, finance, weather, navigation, many other functions on your phone will be made by Apple, Google, and others by third party vendors, but all of them work seamlessly together. In the security world, we are innovating to seamlessly integrate at at least three levels: one, a platform that is the infrastructure that automates capabilities everywhere behind the scenes; number two, an open interface that allows any company to build an app for security with deep technical partnerships to ensure they integrate seamlessly; and finally, organizations that are integrated through effective threat intelligence sharing partnerships such as the Cyber Threat Alliance.

Ultimately, innovations in the cybersecurity marketplace all take advantage of automation, software, and advanced analytics, such as machine learning, that are designed to increase the scale and speed of identifying and preventing most cyber threats. And this is how you bring software to a software fight.

Lastly, how can DOD adopt these cybersecurity innovations?

First, I would say DOD should review the requirements for its cloud-based procurements to ensure that security is considered comprehensively. Contracts must underscore the shared responsibility between mission owners and cloud service providers. To date, they weigh heavily on the latter.

Second, DOD should expand and make greater use of real world operational testing and evaluation programs for security technologies rather than relying on static checklists that require outdated technology.

And third, officials should consider how to take advantage of the massive repository of threat intelligence housed and shared by organizations such as the Cyber Threat Alliance.

And finally, I would just add one comment that DOD should consider how to create incentives for companies to adopt best practices in areas like supply chain risk management.

Chairman Rounds and Senator Gillibrand, thank you very much for the opportunity to testify today, and I look forward to taking your questions.

[The prepared statement of Mr. Davis follows:]

Senator Rounds: Thank you, General Davis.

Mr. Landolf?

STATEMENT OF FRANCIS LANDOLF, PRINCIPAL, CORE CONSULTING, LLC

Mr. Landolf: Senator Rounds, Senator Gillibrand, thank you for inviting me to testify before you today. My name is Francis Landolf, and I had the privilege to serve in a 30-year career at the National Security Agency.

It was during my tenure as an analyst and later as a leader of the signal analysis and cryptanalysis missions at NSA that the agency had to transition from Soviet-centric proprietary analog communications to digital communications and later the real transformation in communications, and that is the transition from circuit switched communications to commercial, standards-based packet switched communication and convergence to the Internet.

Most missions in the government do not have such a large number of technically savvy government employees capable of developing software and systems as NSA. NSA, though, uses contractors extensively in level of service-based contracting mainly to augment the large government workforce that leads and guides the development of new systems and capabilities. That makes NSA technically adept, but leads to problems in integrating commercially available products that serve mission applications and are the product of private sector innovation. I believe that cybersecurity is one such situation.

It seems very clear to me that, for example, the $7.7 billion in venture funding in 2017 for cyber represents an enormous investment in innovation that would be impossible for NSA to match. By building their own products and performing cybersecurity functions without integrating commercial cybersecurity products, the agency is not taking advantage of that sizable investment in commercial innovation in cybersecurity. Therefore, I believe that the private sector is out-innovating the agency in many areas and that pace is accelerating.

The Defense Department is directly affected. NSA has long been rightly recognized as the center of expertise in the U.S. Government in cyber. NSA's leadership played a major role in persuading successive Presidents and Secretaries of Defense to create and invest heavily in military cyber command and the national importance of cybersecurity. The nation is indebted to NSA for this vital role as a catalyst.

However, unfortunately for too long, the Defense Department assumed that NSA would provide the technology and capabilities needed to secure the Department from cyber attack. This led the DOD to overlook and neglect what the commercial sector has been producing for the last 15 years or so. Silicon Valley and other technological hotspots around the country are continuously generating innovative

security solutions that the DOD fails to notice or procure in a timely manner. The DOD lags behind the mature state of the art in commercial technology.

Since retiring from government service, I have worked in multiple capacities, helping new companies grow and attempt to find government customers. I am now or have served as an advisory board member for panels for the National Security Agency, the Cyber Incubator for startups at the University of Maryland Baltimore County, a nonprofit technology group known as Mission Link in northern Virginia that tries to help young companies do business with the government, and Virginia Tech Hume Center in Arlington. I have been a member of the technical advisory group for the Senate Intelligence Committee and am a senior fellow and member of the Board of Regents for the Potomac Institute for Policy Studies.

I have observed as a rule that companies with exciting new technical approaches in cybersecurity backed by prestigious, savvy venture capital investors struggle to get meetings with the Defense Department, much less a chance to demonstrate their products and make sales. This is true even when there appears to be genuine government interest. The time and effort required to close a deal is too great for small companies, especially where an equal amount of exertion yields far more success in the financial services

or other commercial sectors.

Indeed, I have met with multiple venture capital firms that actively steer their companies away from even trying to market to the government. Savvy companies seeking investment know to not use the DOD business as a likely source of revenue during their fundraising pitch to potential investors. I do not mean to pick on the DOD. While NSA and DOD present unique challenges for the cybersecurity industry in particular, but more generally for small, new companies where much of the commercially based innovation is taking place, there are plenty of generic barriers to government acquisition of commercial solutions, which I would be happy to discuss during the Q&A.

There are, however, some encouraging signs. DOD's civilian leadership, now spanning two administrations, and Congress now recognize the tremendous potential of commercial technology to solve vexing problems not only in cybersecurity but a host of new information technologies, including Internet of Things, machine learning, analysis of exascale data sets, and cloud computing. Congress and the Pentagon are beginning to streamline and provide more flexibility to acquisition processes, establishing outposts such as DIUx, and create acquisition organizations with a mandate to increase the pace of technological experimentation, adoption, and fielding.

I have some ideas and recommendations for NSA and DOD that could improve their approach and processes, which I will outline here and can pursue in greater depth during the Q&A.

I see that I am out of time. You have them in my record. Thank you very much for the opportunity to present to you, and I will conclude my testimony with an offer of my assistance to the committee in any way that I can further the goal of bringing innovative commercial cybersecurity technology to bear on the safety of our nation’s networks and information. Thank you.

[The prepared statement of Mr. Landolf follows:]

Senator Rounds: Thank you, Mr. Landolf.

Mr. Nielson?

STATEMENT OF RONALD NIELSON, VICE PRESIDENT AND CHIEF TECHNOLOGY OFFICER, PARSONS CORPORATION

Mr. Nielson: Yes, sir. Chairman Rounds, Senator Gillibrand, thank you for the invitation and the opportunity to testify today as a subject-matter expert concerning the Department of Defense's cybersecurity acquisition processes and practices.

From the private sector's perspective, but as well, I served as a DOD civilian at the National Security Agency and a member of our armed forces for 20 years.

To that end, I have been asked to discuss the challenges and provide some recommendations regarding what lessons can be learned from a program that I managed for a lab called SharkSeer while it was actually led through the National Security Agency and the Department of Defense.

Our nation's cybersecurity prowess is best measured as an integration of people, processes, and technologies, however. Our ability to succeed in this critical mission area requires all three to function in unison across government and indeed industry. I have been very fortunate to assist the Department's cyber operations now for many years.

Thank you for your support in this critical mission area. And I'm going to cut it short, and I look forward to answering your questions as they may arise.

[The prepared statement of Mr. Nielson follows:]

Senator Rounds: Very good. Thank you very much.

Let me walk my way into this a little bit. As we have learned more about the processes within the Department of Defense, the DODIN itself, the system which protects and which is the system in which we communicate within the Department of Defense, it appeared to us -- and the research that has been done -- that, number one, we have some areas of the Department which are very well protected based upon the capabilities, competency, manpower, and so forth that individual locations or programs have. Others have, to a lesser degree, a protection, an overall umbrella protection, but not necessarily to the degree that others have. The expertise found in some areas is not necessarily shared across the entire Department.

And at the same time, it seems as though we have this challenge always, regardless of whether we are talking about new systems, weapon systems, infrastructure. We have this process or a series of processes in place that we pursue to acquire these products. And software, the capabilities to protect our systems, are bound up in this same acquisitions process that folks talk about.

I am just curious. It seems to me that that leads in many cases for the Department to find a way to organically develop some of their own protections and their own systems.

Mr. Alperovitch, you indicated that you believe in the

1-10-60 process. How often is your company capable or would you say that your company is in compliance with your goal of meeting that approach of finding it within a minute, investigating within 10 minutes, and actually repairing or finding the fix within 60 minutes and throwing them out within 60 minutes? How often are you in compliance with that goal?

Mr. Alperovitch: Thank you, Chairman.

Very often. That number is an average target. So there are certainly outliers with some of the more sophisticated adversaries. But the goal is speed and how do you quickly detect them, how do you quickly investigate that detection and eject them. And ejection sometimes is the hardest thing because oftentimes you have to coordinate with the end user. You have to find who is the asset owner. You cannot just turn things off willy-nilly and not expect to have a performance issue. So that is the reason why it takes the longest. But at detection, we are excellent at identifying, on an almost daily basis, Russians, Chinese, Iranians, North Koreans, as well as criminal groups targeting those networks. So it is absolutely doable.

But the key thing I think I would say is the best technologies in the world are not going to solve the problem if you do not have hunting processes where you marry the technology with the people that are thinking like an

adversary. They have an offensive mindset. They are saying if I were in this network, where would I hide. How would I move around, what would I try to accomplish, and then looking for those indicators because the reality is some of these adversaries are going to get in and if you are dealing with a foreign intelligence service or military service, as the DOD is doing routinely, you also have to assume that they are using human assets that are already inside that are helping them achieve those objectives. So we have to start with the assumption they are on the inside. There is no perfect security. How do we find them quickly and eject them? And it is absolutely doable.

Senator Rounds: So are you doing this with manpower? It sounds like you are doing it with machine power.

Mr. Alperovitch: We are using both. We are using artificial intelligence, but we are also using people. And you can use the technology to help people scale. So as I mentioned, we protect millions of machines around the world with 20 people. So it is absolutely a scalable problem. They can focus on finding new things that have never been seen before. Once they do that, you can have the machine look for that so that the humans are not occupied with that process.

Senator Rounds: Did you do this with organically developed systems or did you go outside of your organization

to find this system that is working for you?

Mr. Alperovitch: We developed this organically as we built the company. But a lot of the people that we have brought in have come from the National Security Agency, have come from the Department of Defense. We think that it is really helpful to have people that have an offensive mindset that perhaps have done offensive work for the government and can think like an attacker and find those attackers on our customer networks.

Senator Rounds: Thank you.

Mr. Davis, you have worked within the organization, within the DODIN. You are outside of it now. Is the Department of Defense capable with the existing public policy restrictions in place today -- are we actually capable of creating or going outside and pursuing this, or do we have to continue to look inside organically to get the types of results that we are finding within CrowdStrike?

Mr. Davis: Thank you for the question, Chairman Rounds.

I think it is a combination. For me, I believe that I am very optimistic about the ability of the Department to better leverage machines and software to do what machines and software do better than people. I agree that it is always a combination of people, processes, technologies, and policies. That is a comprehensive way to approach this

problem, and you need all of those elements.

But I do not believe we are leveraging the technology today. I do not believe the Department is leveraging the technology today in ways that enable the machines to do what machines do better than people. And save your people for only those things that people can do better than machines, at least they can still do better today.

I would look at it this way. Leveraging security technology, automated security technology, helps you wipe a lot of the noise from the radar because a lot of the noise is not sophisticated nation states. A lot of it is criminal actors and activists and all kinds of organizations. And by the way, I believe many of those nation states that my colleague mentioned leverage all those surrogates, criminal organizations, surrogates, research organizations to do their bidding. So what is coming at the Department is a lot of noise. And by leveraging machines and software to clear that radar off, you can get a better bang for your buck with your people, and those high skills that are required to do effective things like detection, response, remediation, resilience, those type of things.

And I do believe that a partnership between DOD where DOD can build and bring some of that to the fight internally and DOD can leverage other things that the commercial sector maybe can do better than DOD. I think that that partnership

is the answer.

Senator Rounds: Thank you.

Senator Gillibrand?

Senator Gillibrand: Thank you, Mr. Chairman.

Mr. Alperovitch, over the coming years, more systems within the Department of Defense, as well as the broader society will be incorporated into the Internet of Things. This growing number of devices and their increased interconnectivity creates a new cybersecurity challenge.

How can the Department of Defense best secure the communication between devices within the Internet of Things and how can the supply chain be secured in a cost-effective manner?

Related, how can security requirements driven by DOD best proliferate into the broader market where attacks on items the general public uses could create large-scale destruction in society?

Mr. Alperovitch: Thank you, Senator Gillibrand.

You are absolutely right that IOT, Internet of Things, presents an enormous challenge to industry and to the Department. The biggest problem we face with IOT devices is their lifespan. Once those devices leave the factory floor and get incorporated into systems, it is typically 12 to 18 months until the manufacturer forgets all about them and stops updating them and move on to the new version. And

security vulnerabilities found afterwards are no longer fixed by those manufacturers.

So that is a challenge that I think we need to think about from a regulatory perspective perhaps of how do you make sure that once a device is shipped, people do not just forget about it, particularly devices as is the case with a lot of these Internet of Things systems that interface with the physical world and can actually impact physical systems beyond just IT. So it is a very critical issue.

But I would say, generally speaking, we have to start with an assumption that any device is hackable. There is no perfect security, and adversaries will find their way in. That is why I believe it is so important to focus on finding them quickly, hunting for them, and ejecting them.

Thank you.

Senator Gillibrand: General Davis, your testimony talks about the need to bring software to a software fight and do so strategically and swiftly, as swiftly as the threat moves, using the DevSecOps model.

How does DOD procurement need to change to achieve this? Is there additional legislative authority or requirements that you recommend to achieve this? Also, if DOD is to leverage more of the commercial model, does it ensure that the hardware is not tainted by foreign components and it is not exported to adversary nations, both

issues that are hard to tackle with the global nature of technology? And can we do this more efficiently with a single acquisition force across DOD instead of reinventing the same capabilities in each of the services?

Mr. Davis: Thank you for the question, Senator Gillibrand.

It is a tough question and there are two parts to it.

I believe that on the supply chain issue, we know a lot about cyber threats. We know how they operate. We know the attack process. It is called the lifecycle, the kill chain. I think Lockheed Martin trademarked that term. But we know the steps that any actor or organization uses in order to achieve an outcome regardless of what type they are. Even supply chain threats, things that are embedded into the infrastructure that may be used for whatever purpose -- that threat is usually not at the location it needs to be successful, and it has still got to crawl through that process in order to achieve some type of an outcome. Usually there is some sort of a control channel that is opened up. There is lateral movement. There may be escalation of privileged access. These things are detectable.

So from my company’s perspective, we believe in this comprehensive view that you need to have consistent visibility and protections across all those different types

of environments because different parts of the kill chain occur in different parts of your environment, some at the perimeter, some in your data centers, some at your endpoints, including IOT devices, some in the cloud, now that everything is moving to the cloud.

What the cybersecurity industry has done over history is they have built discrete solutions to look through a soda straw at different parts of that environment, and that makes it very difficult for a defender to be able to pull all that together and see what is happening to identify a threat, attack sequence in process. If you take a comprehensive view of that, even supply chain threats, even insider threats are visible if you are looking at the entire attack process. And that gives you the ability to apply visibility and protections across that process in order to stop a threat before it achieves a successful outcome.

Senator Gillibrand: Thank you, Mr. Chairman.

Senator Rounds: Thank you.

Senator Blumenthal?

Senator Blumenthal: Thank you, Mr. Chairman.

Mr. Alperovitch, I was intrigued by your analogy to the SEALs getting in through locks and then having to hunt them down and the inevitability -- I am not sure you used that word, but the unavoidability of some intrusions taking place as long as there are human beings involved because they

create the openings for adversaries to infiltrate our systems.

So my question is whether the focus now on cyber hygiene is inhibiting the hunting objective and whether you would -- and maybe this is a question for the other panelists as well -- whether you agree with this theory whether the two are somewhat mutually exclusive in terms of resources and effort or whether in fact they can be combined because you would argue, to take the analogy of break-ins, it is not a bad thing to have a burglar arm because at the very least, it will alert people that you are going to -- that there is a break-in. But then you have to hunt them down. You cannot prevent SEALs from getting in, but the hygiene part of it might -- in other words, having an alarm -- might enable better detection.

Mr. Alperovitch: No. Absolutely. Thank you, Senator Blumenthal.

I would like to clarify because I do believe hygiene is important, just like locks on the doors are important. It is not enough. And the challenge that I see in the Department today is 90-plus percent of the effort is focused on hygiene when hygiene is not going to stop the PLA. It is not going to stop Russian military intelligence. And I would argue that is the primary threat the Department faces in terms of the enemies that are trying to steal our secrets

or degrade our warfighting capabilities. So there needs to be a balance, and I would argue our primary focus right now should be on finding those actors, getting them out of the network quickly. Then you can start rebuilding and building on hygiene methods. It is just the priorities are inverted today.

Senator Blumenthal: Let me ask the other panelists. Do you agree that, as a matter of fact, 95 percent of the resources are on hygiene and there has to be a better balance between hygiene and hunting so to speak? General Davis?

Mr. Davis: Thank you, Senator Blumenthal.

I believe that basics matter. In my experience in the last 10 years of my service, there was not a single major cyber incident that was not totally preventable by basic standards and discipline. Not a single one. That information may be a little bit dated, but I do believe basic standards and discipline can make it much more difficult because even though -- nation states do have sophisticated capabilities, but in my experience -- and I can tell you this even from a U.S. perspective when I served -- you do not necessarily use your most sophisticated capabilities all the time. You use what works, and usually what works is waiting for somebody to make a mistake and being patient. And people make lots of mistakes,

unfortunately.

So I do think that the human behavior side of this, standards and discipline, is very important, but it is, I would say, necessary but insufficient. You still need technology. You still need processes in place. You need a comprehensive system, but you cannot just give away the basics. The basics matter.

Mr. Landolf: That was my line. The hygiene is necessary but not sufficient.

One area in which the commercial sector outpaces the government sector is the automation of the hygiene. And if there are a lot of resources being applied to hygiene, it is because we have not kept up with the commercially available processes and technology that perform these hygiene functions in an automated fashion.

Senator Blumenthal: Mr. Nielson?

Mr. Nielson: Senator Blumenthal, the other panelists have said things well. An analogy would be we would not probably send our tanks into combat without preventative maintenance checks and services. We would do what we think to put it into an operational state and to maintain it there.

From the Department today, is it skewed? Possibly so. I believe Senator Gillibrand made a comment earlier that we really cannot paint the Department with a single brush

either. Some portions of the Department may actually be better prepared or be more active in hunting or defensive capabilities than others.

I call attention to something very simplistic I thought, very productive for the Department was the acquisition of Windows 10. As a software acquisition for the enterprise, I think that was a very smart move. It provided hygiene. It provided a lot of capability, a more secure platform, and it kind of changed our way of looking at the endpoints from a security perspective. So less room for the adversary to roam, less tools for them to employ against us.

So I do not think it is a one size fits all. I would like to see some more active cyber defense, the hunting. We used to call it pursuit operations.

But another aspect was also brought up. I think Chairman Rounds had mentioned it. Hygiene is not just hygiene. It is architecture. And when we actually construct systems of communication that are inherently not safe, we actually induce or employ other avenues for the adversary to take advantage of. So I do not know that architecture and design, proper design and implementation of technology is necessarily hygiene. I think it has to have a consideration. We would want to start with a defendable terrain if we were to choose a terrain on a map, and we need

to consider that when we choose the terrain in cyber as well.

Senator Blumenthal: I have one more question, Mr. Chairman, if I may.

Mr. Alperovitch, we have heard about how difficult attribution is. When the DNC was hacked, CrowdStrike I believe was able to pin responsibility for the hacking on the Russian government virtually from the time it was first disclosed. What was it that enabled you to do it? And are there any broader lessons that can be discerned from that action?

Mr. Alperovitch: Thank you, Senator.

I would say that attribution is actually getting easier and easier in cyberspace. In fact, most of the major attacks that we have seen over the last 30 years have been attributed and certainly have been attributed by the government. The government, of course, has phenomenal capabilities in terms of intercepting phone calls and listening in on intentions of foreign leaders beyond just technical attribution.

But even on the technical side, we are seeing private sector companies being able to do better attribution because, frankly, they are engaging with the enemy on a daily basis. It is not that this was the first time we had ever sent that group before. We had seen them many times

over the course of many years. So as you have more and more exposure to them, as you engage with them on a regular basis, you tend to find more and more about them in every engagement. After all, humans make mistakes and they do make mistakes. And when you see thousands of operations over a course of decades, you can collate that information and get a very good view on who they may be.

Senator Blumenthal: I think this point is important because, to put it very simplistically, one of the objections to retaliatory or deterrent measures in the cyber domain that I have heard expressed is the difficulty of, quote/unquote, attribution. So how can you attack back if you cannot attribute with some degree of certainty and publicly disclosable certainty who the enemy is that attacked?

So I take it from your answer that attribution is not only becoming -- I think you used the word “easier,” but also more reliable. And therefore, one of the obstacles to a more efficient deterrent mechanism in this space would seem to be eliminated.

Mr. Alperovitch: That is right. And I would point you, Senator, at the Justice Department’s actions over the last literally 6 months where they have indicted Chinese hackers, North Korean hackers, Russian hackers. So the government certainly has great visibility not just in the

countries that are doing this but the individual people and the military or intelligence agencies that are working with them. So I do believe that on major national-level attacks, the government certainly has a lot of capabilities in this space and are usually very certain.

Senator Blumenthal: Thank you.

Senator Rounds: Thank you.

Gentlemen, this is too good of an opportunity for us not to pursue this a little bit farther. So I want to continue on just a little bit.

I am curious. In your experience in dealing with the Department, there are times in which contractors are hesitant to talk about challenging issues within the Department because the Department can watch in open session and see who is complaining about their processes. But I would suspect that the Department also has frustrations with those same processes that have, in many cases, been created by Congress in the first place. And if we are ever going to fix them, we have got to have an open dialogue about what they are. And so what I am going to ask you to do is to go out on a limb here a little bit and trust us in that we are trying to get to the bottom of public policy changes that need to be made in order to improve the process in which private companies at the appropriate time can participate in these contracts on a simplified basis.

What I would like to know is, from each of you, if you could, in your own experiences, what is perhaps the most challenging or aggravating factors inhibiting cybersecurity acquisition processes today. And I am not doing this to be critical of individuals within the Department but rather of the processes that they have to participate in as well. Can you share with us? And I am just going to go right down the line, and Mr. Nielson, you are first up this time. Share with us what you think are some of the perhaps most frustrating things that you would love an opportunity to see us change and might very well be within our purview to do.

Mr. Nielson: Well, Chairman Rounds, thank you for calling on me first for this one, I think.

So I will speak from my time while in service in the government. Even then, I was frustrated at times because the rule was if you give the government a chance to say no, then they will. Risk aversion due to legislature, policy, controls.

The requirement to take a commercial technology and add it to a government network comes fraught with all kinds of compliance issues, certification, processes that take hundreds of thousands of dollars at times to bring a product to bear, just to test it.

As has been said earlier by some on the panel, it is a difficult and daunting task if you are not a large,

successful cybersecurity firm today. If you were a smaller firm, you would not even be able to approach. So you would move away.

Risk aversion and the lack of understanding. I think this is something we could probably do something to fix. Many, I feel in the government -- or let us just say some -- would take a position to be risk averse in acquiring technology or look at a regulation and say, well, maybe this will be challenged. Maybe there will be a protest, or maybe we have to go through our acquisition processes for a fair and open competitive engagement, which may take us 2 to 3 years. And those are all reasons to say no. So to engage or to start a process of acquiring a commercial technology and testing it in your enterprise could be very daunting. It could be very time consuming with no progress or no -- something achievable or accountable that they can look towards.

So I think if we look at things differently, I think the Department and even the White House has put together a paper in cyber about high-value assets. And so my tenor there would be if we know what our assets are exceptionally valued in the DOD or the Department, maybe we could find test grounds or test beds for JCTDs, joint capability test and demonstrations, where the rigor of compliance could possibly be given an easier path where we could take these

technologies maybe through OTAs or BAAs and bring in technology and integrate it into an operational state.

But the true test of commercial success in the Department is not a lab test. It is not what it has done or a SLC sheet or a meeting at RSA. It is done when you can implement the technology in the environment with which we have to defend, and that is a very difficult path. I think we could find a method or an organization or an entity to take some responsibility for rapidly prototyping or rapidly integrating and assist commercial technology firms with the ability to get that product semi-certified or certified with reservations or controls. Try to find a more rapid way.

I think we have talked about the time of 1, 10, and 60, and I like that.

But 3 years is far too long to take a piece of emergent technology and try to test it. Just test it. And if it is successful, it might take 3 more years to acquire it. And in 6 years after it was emergent, after 6 years of potential benefit, we are still struggling to see that technology demonstrated in our environment that brings the great success to us, I think we have to challenge that. We have to say there must be a better way to take these technology components and really demonstrate their value and accept risk. I do not want to be flippant, but I think we should accept risk and let our workforce and our leaders know we

take risks every day, that in cyber we are going to have to take some risks, measured, professional risks, in order to adopt commercial technology quickly.

Senator Rounds: Thank you.

Mr. Landolf, same question.

Mr. Landolf: I will address the small, innovative startup community. And essentially for them to make a sale into the Department, it is really three sales. They first have the roadblock of finding the mission owner with the problem that their technology potentially addresses. So given that they found that person, that mission owner, the second problem is they have to go with that mission owner and find somebody in the enterprise with the money. And once they find the person with the money and convince them that this is a good thing for the Department, a good thing for the mission, the third sale they have to make is to the person that owns the contract vehicle, and that is normally a large company which has absolutely no incentive whatsoever to sell a product to the government which is not one that they have made. And they are much more incentivized to make a product that serves that function that the small company is trying to sell into the government than it is to find a way to get that product into the government.

So one of the solutions to that I think is to have contract vehicles in which the government can deal directly

with the small companies whereby the company does not have to go through the owner of a large contract vehicle, that they can deal directly with the mission owner, they can come and contract directly with the mission owner, or there is money already allocated for the procurement of products from small, innovative companies.

Senator Rounds: Thank you.

Mr. Davis?

Mr. Davis: Yes. Thank you, Chairman Rounds.

I have two thoughts on this. One deals with increasing the speed at which we can buy things and put them in the hands of mission owners. In my experience, the procurement community and the mission owner community are driven by different objectives and there are stovepipes between them. And we have a procurement process that is largely legacy and Industrial Age and cannot keep up, cannot keep up with the speed at which these requirements are changing in both the technology environment, as well as the threat environment. So it makes it very difficult.

One of the things that we have seen DOD do to address this issue is the idea of operational test and evaluation. And this is to shorten the cycle at which you get the best capabilities and tools into the hands of the operators with a risk assessment. You are not trying to be perfect with risk. You are trying to manage risk. But get it into the

hands of the operator so that they can leverage the best available technology today rather than waiting for that longer cycle to build the perfect. So I think that is one aspect of doing this.

In the commercial world, that is called the DevSecOps model, software development, operations, security all cycling together in much shorter parallel processes rather than a sequential series of things that takes a much longer amount of time.

The other idea that comes to mind is finding out ways for both procurement officials and for mission owners to leverage the tremendous amount of cyber threat intelligence telemetry that is available out there in commercial organizations. I mentioned the Cyber Threat Alliance as one. This is over 20 cybersecurity companies, all competitors, that have agreed to share information, cyber threat intelligence, every day so that basically whatever one of those companies sees around the world, that information is brought in, and then all companies are able to essentially immunize their client base based on what anyone sees. It gives you an over-the-horizon capability.

I think we should be asking DOD officials in both procurement and mission owner arenas -- they should be asking if the companies that want to do business with them, the cybersecurity companies that want to do business with

them, if they are not in the Cyber Threat Alliance or an organization like it, why not.

So I think those are two ways that I think you could address both the speed and the scale at which we are currently seeing challenges.

Senator Rounds: Thank you.

Mr. Alperovitch, you have the toughest job being at the end of the line this time.

Mr. Alperovitch: Indeed, it is.

But, Mr. Chairman, I would say the landscape today is very different from where it was 15 years ago. I would argue 15 years ago, the Department, National Security Agency were far ahead of the private sector because they were actually the ones that were engaged with these sophisticated threat actors and the private sector at that time was not. Nowadays, the situation is very different. The private sector is facing the same threat actors. They are seeing them even more regularly. And I would say they have come up with some of the more advanced and forward-leaning technologies to combat this threat than the Department has implemented. And as a result, I would offer three thoughts.

One, let us not reinvent the wheel. Let us leverage what the private sector is doing successfully to combat these very same threat actors and organizations out there, research organizations like Gartner and Forrester that

regularly evaluate those types of solutions, put together regular rankings for vendors and technologies that are good at various aspects of combating the threat. So the Department should do more to leverage that as opposed to try to reevaluate what the private sector has already learned.

Secondly, I would echo the comments of my panelists, shortening the acquisition time frames. If it takes you 3 years to figure out if the technology is good enough, it is probably already obsolete by the time you deploy it.

And third, I would say that, again echoing General Davis' comments, a much more realistic testing environment, real-world testing environment is essential in figuring out that the solution is going to work, not just that it is going to be effective at stopping threats but also that it is not going to break any mission-critical systems, which is an important category of testing that needs to be done. So I would just say that similarly to weapon systems that need to be tested in combat in combat-like scenarios before we deploy them and call them mission-ready, we need to do the same thing for cybersecurity technologies, and that is not happening, by and large, in the Department today.

Thank you.

Senator Rounds: Thank you.

Senator Blumenthal, did you want to --

Senator Blumenthal: Yes. I just have a couple more

questions.

I wonder whether the panel would have a view -- we have been talking mainly I think about hardware and the technology. What I have heard is that there is a shortage of trained personnel and that the Department of Defense sometimes has a difficult time attracting the kinds of people because of possibly the culture or the pay. When I say culture, I mean -- I do not want to name names, but the military personnel have said to me, you know, when we go out and recruit people, they do not have the culture or the background or the mindset -- I do not know how you want to describe it. But the military to them is not a place where they necessarily feel at home. And I can say this, having four children, two of whom have served, and they have done extraordinarily well while they were in and since leaving. But not every one of their friends would fit into the Navy or the Marine Corps where they served.

This is kind of a longwinded way of asking a question. I do not know whether there is an answer to it that you would be willing to offer.

Mr. Alperovitch: Senator, I would offer a slightly different perspective because, as I mentioned in my opening statement, at CrowdStrike we have phenomenal people. Many of them have come from the Department of Defense. And in my interactions with the National Security Agency, with parts

of the military -- in fact, General Davis and I were at an event this morning that was put up by the Army Cyber Institute -- phenomenal, cadets from West Point, Naval Academy -- they are studying cybersecurity, really amazing talent that you face in the Department.

So I do not know that it is necessarily a talent shortage. I would argue maybe the priorities are not right, and we are not focusing them on the right things. But these people are phenomenal. We have many of them that are still in the Reserve and go back regularly for active duty in cyber missions. So I think the people are phenomenal there.

Senator Blumenthal: General?

Mr. Davis: Senator, that is a great question, and I could talk for hours about a bunch of different aspects of that. But let me offer you a couple of thoughts.

One, on the people side, from my previous experience, I do think we have to look at innovative ways of attracting the right kind of talent into the military. But I still believe, because what military people are doing in cyber operations, it is such a potentially sensitive area that you want people who understand the chain of command. You want people who are disciplined. You want people who are precise. The standards maybe need to be adjusted in some aspects, but in other aspects, I believe it is so important because things can get out of control and you do not want

that happening. You want control over what your military is doing in the cyber realm.

Another aspect of people is the aspect of training, education, awareness certifications. I know that there are many different organizations. My company has invested in many nonprofit things to try to help the overall ecosystem, including the military in terms of education, awareness, et cetera. We host an annual event for the joint service academies, the Army, Navy, Air Force, and the Coast Guard service academies, Joint Service Academies Cyber Summit every year, to bring former graduates who are out in industry back together with military, government officials, and the academies to look at how do we improve the type of talent that we are bringing into the military and how do we leverage it in the commercial space.

And even things like with the Girl Scouts. We partner with the Girl Scouts to create 18 cybersecurity badges, K through 12 over the course of the next several years. The first batch of six of them came out last summer. That is to get at the aspect of women in this field who we need. We are very under-represented in women and other under-represented minorities, and if we have such a personnel gap, how are we ever going to get at that if we are excluding so much of our population? So efforts to try to increase that I think are very, very important.

My final comment would be despite all of those efforts, we are never going to have enough people to solve this problem. And that to me is why it is so important to leverage technology and machines to do what machines can do better than people. Hunting is such an important skill, but in order to reduce the scope of what you are actually hunting on your network, if you have a machine learning capability like we do that can go through a software-based ability to identify suspicious behavior in a network and automatically turn that into protection mechanisms to the tune of 1.6 million every week, that helps your hunting capability focus in on the really sophisticated stuff. And like I mentioned before, it helps you clear the noise off of the radar screen so you can use your people more effectively.

So I could talk for hours about this aspect of it, but I think those are three things that come to mind.

Mr. Landolf: Senator Blumenthal, that is an extraordinary question. And I agree with you. This is a very, very major problem. And I wish my answer could give you a very easy problem to work on. But my answer is that the government has to find a way to shorten the security clearance process. I would venture to bet that we lose more than 50 percent of people who would be willing to come and work in the government on these problems to the fact that it

takes up to a year to get them cleared. And the people that we really want are going to be getting offers from well known names in the industry during that period of time that are too great a temptation for them to pass up.

The major attraction that we have, if we think about the research that has been done on what motivates the people that we want to work in this area, it is autonomy, mastery, and purpose. Many companies give the autonomy and mastery, but the government gives a purpose, a very, very noble purpose for one's work and one's labor. And we have to capitalize on that and shorten the process required to bring these good people on board.

Senator Blumenthal: Thank you.

Mr. Nielson: Senator Blumenthal, I appreciate the question. I guess I will try to offer something maybe as a variant.

I worked on the SharkSeer program for the Department. At the time we began the program as an enterprise capability for the DOD, that mission was probably 500 or 1,000 or more people working in that mission space, in that arena, analysts and on-net operators, those kinds of people. It was not really just solely technology. And I am sure you have heard maybe in the past some buzzwords like "orchestration." We have heard about "DevSecOps." But the development of a security operation is not necessarily a

piece of software. It is an orchestration event. It is automate the processing of movement of data from one part of our collection process into an activity process or an action or reaction process.

I was really proud to say just back in August that that SharkSeer program had detected and mitigated over 2 billion unique events in a month, in a 31-day period of time. And these are things that had eluded or evaded other systems within the DOD. But it did that with a handful of people.

So in the commercial sector, I work at a wonderful company that I enjoy, Parsons. We have a labor shortage. And we understand and we try to employ ways to entice employees with culture and incentive and opportunity just as the government does. But at some point in time, again with the acquisition of commercial technology, we might be able to instrument 80 percent of the mission, as the General has stated, and then have only 20 percent remaining. We may be much more fast. We may be able to actually apply mitigations, but in SharkSeer, it is done in microseconds without a human. And at time and culture, we will accept the machine doing.

I remember a long story. Maybe it is not relevant. It was to me because I hated it. I was in the Army. And we had to be our own gate guards. We had to mow the grass. At some point in time, the DOD decided that their soldiers

needed to focus on warfighting and not mowing grass. And we stopped.

That may be a trivial allied story to what we are facing today, but I think you can have applied machine learning. You can have orchestration and automation in the network. So it is not a point solution. It is how do we prosecute the fight and let technology take over that portion of the mission, one that it is exceptional at. It does, in fact, finger mistakes like we tend to. So there is an application. I think we could look to replace some of our functions, some of the data volume.

Again, an older story. I remember talking to analysts when I was building SharkSeer, and I said, what data do you need to prosecute your mission? I thought that was a very simple question. But the response was, all of it. Well, all of it would have cost a fortune. It would have cost a fortune to move it. And so I countered, well, what pieces of the all of it are you going to actually use to come up with a substantive, meaningful, actionable response? And they did not know.

So I think we can apply some of this high speed -- I was at the Naval Academy yesterday. There are quality, high-speed folks that know what they want to do. Just empower them with using technology to solve pieces of the puzzle. And I think we could do that.

The clearance process is daunting. You asked, Senator Rounds, what we could do in some ways. Consider this. I got a clearance in 1983 I think, and I have held it proudly since. But that acquisition process takes a long time to acquire a clearance. There are aspects or facets of the Department of Defense that handle no classified information whatsoever. And in the military, we used to do train the trainer. Maybe we can onboard some of this talent from the commercial space and let them work in less classified, less sensitive mission areas while they are being paid and they are developing or honing their skills and then advance them and mature them into highly classified or more classified areas, which by definition would be a smaller place that we would have to serve and less personnel. But I do think there is something that could be done to accept personnel of caliber, high-tech folks.

And lastly, I will just leave with a separate kind of comment. I started on the offensive side a little bit. We were not exactly the people that were compliant with procedures and well documented with training. We were more apt to find ways around things than to do things properly or well documented. But it is high caliber talent.

So, again, I could challenge the Department to look at ways to utilize unclassified, maybe sensitive but unclassified environments to use commercial talent or to

bring and onboard personnel, and then mature them into more sensitive and classified environments as the clearance process adjudicates itself.

Thank you.

Senator Rounds: Thank you.

Senator Blumenthal: Thank you all very, very much.

Senator Rounds: I would like to take this opportunity first to thank our members who have participated. I know Senator Nelson could not be here, but Senator Gillibrand filled in as ranking member. Senator Blumenthal, thank you for your time today. Senator Fischer was here as well. I would like to thank all of them for participating.

And I would really like to thank our panelists today for the work that you have done and what you have shared with us today. It is a small step, but as we move forward, we want to modernize the way in which we do our acquisition process within the cyber side at least, hopefully within the Department of Defense’s information network and to learn from you what works and what does not work and to look at best practices outside of the agency that we can bring in, to look at some of the frustrations which you have expressed.

And I think you have hit it on the head when it comes to -- receiving a security clearance is not just within those individuals working on cyber but across the entire

processes as we have geared up once again within the Department of Defense and the challenges we have just in terms of getting contractors who can get their manpower up to speed. This is an area which is a bottleneck, and it is one that needs to be addressed. And once again, you have highlighted that.

I want to say, once again, thank you for your time, your efforts. Thanks for participating in this today.

And at this point, unless there are other comments, we will close the subcommittee hearing at this time.

[Whereupon, at 4:20 p.m., the hearing was adjourned.]