Stenographic Transcript
Before the

Subcommittee on Cybersecurity

COMMITTEE ON
ARMED SERVICES

UNITED STATES SENATE

HEARING TO RECEIVE TESTIMONY ON DEPARTMENT OF DEFENSE ENTERPRISE-WIDE CYBERSECURITY POLICIES AND ARCHITECTURE

Tuesday, January 29, 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
DEPARTMENT OF DEFENSE ENTERPRISE-WIDE CYBERSECURITY
POLICIES AND ARCHITECTURE

Tuesday, January 29, 2019

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

The subcommittee met, pursuant to notice, at 2:29 p.m. in Room SR-222, Russell Senate Office Building, Hon. Mike Rounds, chairman of the subcommittee, presiding.

Members Present: Senators Rounds [presiding], Wicker, Scott, Blackburn, Manchin, Gillibrand, and Blumenthal.

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

Senator Rounds: The Cybersecurity Subcommittee meets this afternoon for our first hearing of the 116th Congress.

Before we begin, I want to welcome our new Ranking Member, Senator Joe Manchin. I'd also like to welcome all of our former members back to the subcommittee and extend a special welcome to the new members joining us. On the Majority side, we are joined by Senator Wicker, Senator Scott, Senator Blackburn. On the Minority side, we are joined by Senator Heinrich.

Two years ago, this subcommittee was formed to address the most pressing national cybersecurity matters, with a focus on DOD-related legislation and oversight. I look forward to legislation that builds on the hard work we have done over the past 2 years, and continuing our important oversight of the plans, programs, and policies related to cyberforces and capabilities within the Department of Defense.

Today, we will receive testimony on the Department of Defense enterprise-wide cybersecurity policies and architecture form: Mr. Dana Deasy, the Department of Defense Chief Information Officer; Vice Admiral Nancy Norton, the Director of the Defense Information Systems Agency, and Commander of the Joint Force Headquarters-

Department of Defense Information Network; and Brigadier General Dennis Crall, the Principal Deputy Cyber Advisor and Senior Military Advisor for Cyber Policy. We welcome you.

We have a lot of information to cover, so I will be brief. At the conclusion of Ranking Member Manchin's comments, our witnesses will make their opening remarks. I would appreciate the witnesses limiting their remarks to about 5 minutes, with the option of providing a longer statement for the record. After they finish their remarks, we will have a round of questions and answers.

One of the Department's main cyberspace objectives articulated in the 2018 Department of Defense Cyber Strategy is securing DOD information and systems against malicious cyber activity. Unfortunately, in recent years, we have seen relentless and sophisticated cyberattacks on the DOD enterprise, other government agencies, and the private sector, while the capabilities of our adversaries continue to increase. Simply continuing to defend our networks as we have in the past is not adequate to counter the growing threats that we face.

At a hearing with private-sector witnesses last fall, we heard about the advances that industry has made in developing new tools and techniques for defending large enterprise networks. While there are many unique challenges because of the complexity and scope of the Department of

Defense Information Network, also known as the DODIN, it is important that, where possible, we leverage the best practices from industry to defend our networks. In addition, it is equally imperative that the acquisition process of DOD is not precluding it from organically developing and producing state-of-the-art cybersecurity capabilities. In this context, we look forward today to learning more about JFHQ-DODIN and, in particular, how the organization can achieve a complete, realtime picture of the entire DOD network.

The Department's cybersecurity tools are not the only factor important to robust defense of the DODIN. It is also critical that the Department formulate and implement appropriate cybersecurity policies and stand up a robust cybersecurity workforce. Specifically, we are looking forward to learning how the Department is implementing their 2018 Cyber Strategy in these areas of cybersecurity.

Across the cybersecurity spectrum, it is vital that we are consistent in our approach as we further centralize, standardize, and integrate the complexities of DOD's cyber enterprise. We cannot afford to waste time or resources with the duplication of effort across the services, combatant commands, and support agencies. In that context, the witnesses here today are charged with these important tasks toward further streamlining and modernizing the

Department's cyber defensive posture. We look forward to hearing how you are accomplishing this challenging task.

Today's discussion builds on many of the themes that were discussed in our cybersecurity hearings with the private sector this past fall. While most of our subcommittee hearings are closed because they include classified information, I chose to hold an open hearing today so that private industry would have further insight into the Department's plans and future cybersecurity needs. I encourage DOD and private industry to continue a robust dialogue so that you can help each other to achieve overlapping goals and prepare for our upcoming cybersecurity hearings this year. Any questions that would require a classified answer can be submitted for the record, for which we would appreciate the Department's timely responses.

Let me close by thanking our witnesses for appearing today, and for their service to our Nation.

Senator Manchin.

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

Senator Manchin: Thank you, Mr. Chairman.

As you said, this is my first hearing as the Ranking Member of Cyber Subcommittee and how it doves in well with my Ranking on Energy, which we have oversight of cyber also, so it's really going to be helpful.

I'm delighted to be joining you, Senator Rounds. We've worked together as Governors together, and now we're back together again as a partner to improve the cybersecurity of the Department of Defense and, indeed, I hope, the Nation.

I join you in welcoming our distinguished witnesses today: Chief Information Officer Dana Deasy -- is it -- is -- am I correct on that? Okay. Defense Information System Agency Director, Admiral Norton; and General Crall, who has the challenging task of overseeing, on behalf of the Secretary of Defense, the implementation of the Department's new Cyber Strategy. The committee has long looked for a way to empower DOD with the ability to adopt an effective strategy and plan of action to deter cyberattacks and defend against them. Thankfully, based on initial reviews of the new Cyber Strategy and the results of the new Cyber Posture Review, there is optimism that DOD has turned a corner, that we now have a credible strategy and a commitment to implement it.

The specifics of the new wide-ranging strategy are quite complicated, but I believe common sense can make this all understandable to our constituents back home. Here are some examples:

I'm told we have not one network in DOD, but, in fact, thousands. Each military service, defense agency, and every component within them have built their own networks, with chaotic results. They can't work together effectively, and they are hard to defend. There is now a plan to break down these fractured networks and implement a common security architecture. We cannot allow computer and other device to be connected to the network without verifying who installed it and whether it's correctly configured and protected. We have to be able to manage who accesses the network and what they can see and do, according to the role they are assigned. We have to monitor the activity that people and the computers they control are conducting on our network to guard against insider threats, like Snowden. We have to improve the security of the networks of the companies that build weapons and provides services to DOD. We cannot allow China to keep stealing our technology and program plans to cyberattacks on the industrial base. We have to recruit, train, and retain real experts in cyber warfare, despite fierce competition with the private sector and the hiring obstacles that the government faces. We have to figure out how to apply new artificial intelligence and machine learning technologies to detect cyber intrusions, as well as to help our cyber forces operate better and faster.

These are the types of issues that the committee and DOD have talked about fixing for a long time, but now, finally, the Department may be prepared to take real action. We hope so.

So, I want to thank you, Mr. Chairman. And we look forward to y'all's testimony.

Senator Rounds: Thank you.

And I would note, also, that former Governor Scott is here with us, as well.

Senator Manchin: Yeah.

Senator Rounds: So, now you face questioning from three different Governors from --

Senator Manchin: Things will happen now.

Senator Rounds: -- as well. So, going to start things popping.

And thanks, Joe. We look forward to working --

Senator Manchin: Yes, sir.

Senator Rounds: -- with you on this project, as well.

We'll do the questioning in 5-minute cycles, and we'll just take our time and work our way through. We'll try to limit our questions to get specifics, and then we'll ask each of our members if we would try to limit them to 5 minutes, and we'll move back and forth.

So, as I said earlier, you are all welcome to provide a complete transcript -- or a record -- or a statement for the record, but we would appreciate it if you would also keep your opening statements to 5 minutes, as well.

And, Mr. Deasy, I'll turn to you first, if you'd like to begin, and then I'll let you decide how you would like to proceed from there.

STATEMENT OF DANA DEASY, DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER

Mr. Deasy: Okay. Thank you.

Good afternoon, Mr. Chairman, Ranking Member, distinguished members of the subcommittee. Thank you for this opportunity to testify before the subcommittee today on the Department's cyber architectures and policies.

I'm Dana Deasy, the Department of Defense Chief Information Officer. With me today are Vice Admiral Nancy Norton, Director DISA and Commander JFHQ-DODIN; and Brigadier General Dennis Crall, Senior Military Advisor for Cyber Policy and Deputy Principal Cyber Advisor to the Secretary of Defense.

Since my arrival at the Department last May, I have made cybersecurity one of my top priorities. In September of 2018, Department released a top-level DOD Cyber Strategy. This Strategy represents Department's vision for addressing cyber threats and implementing the cyber priorities of the National Security Strategy and National Defense Strategy. The Department also released its Cyber Posture Review to Congress, which provided a comprehensive review of the Cyber Posture for the DOD and identified gaps in our strategy, policy, and cyber capabilities. Also last year, the Secretary and the Deputy Secretary asked me to undertake a study to determine what the Department's cyber priorities should be. This led to the creation of the top ten cyber priorities. Cyber roles and responsibilities are shared across the Department. Only by working together, as you will hear from the three of us today, we are able to close the gaps and secure our systems.

For the first time under the authorities granted by Section 909 of FY18 NDAA, the DOD is reviewing, commenting on, and certifying all of the IT budgets, which includes cyber, across the Department. Additionally, DOD now has -- the DOD CIO now has the authority to set and enforce IT standards across Department. Together, DOD CIO, DISA, and PCA work regularly to implement the DOD Cyber Strategies, in close coordination with the military departments and other DOD components. DOD CIO and PCA co-lead a weekly meeting focused on cyber issues with the Deputy Secretary of Defense, at which all military departments and OSD principals are in attendance.

A key element of the Department's approach to standardizing cybersecurity across Department is setting the standards in the cybersecurity reference architecture, which is the tool providing cyber guidance for the family of architectures that align to the DOD overall enterprise architecture. As we aggressively leverage automation, new endpoint security technologies, and standard architectures to achieve military advantage through information, having strong assurances of who is accessing the data and how they are accessing the data is critical. We have been actively deploying a DOD identity credential and access management strategy that recognizes the changing environment and addresses the increasing dependence on digital identities to share information rapidly and more securely.

Turning to cyber workforce. As my Deputy, Ms. Essye Miller, testified before you last September, DOD recognizes the importance of growing and maintaining the cyber workforce. It's an imperative that DOD attract the next generation to view the Department as an employer with unique and challenging opportunities within the cybersecurity career field. Recent authorities provided by Congress have allowed the Department to adjust existing policies and to implement new policies that account for this dynamic need in an increasing important mission area. One of these key authorities has been the establishment of a Cyber Excepted Service.

In closing, the close working relationship between DOD CIO, DISA, and PCA is critical to our ability to address cybersecurity vulnerabilities. The importance of connection between policy, standard architectures, and remediation cannot be overstated. The Department has clearly defined cybersecurity problems to be solved, has a well-thought-out remediation approach; the right mechanisms are in place to monitor and report on our progress on the top ten cyber priorities.

I want to emphasize the importance of our partnership with Congress in all areas, but with particular focus on cybersecurity. Continued support for a flexible approach to cyber resourcing, budgeting, acquisition, and personnel will help enable success against an ever-changing, dynamic cyber threat.

Thank you for the opportunity to testify today, and I look forward to your questions.

And, with that, over to Admiral Norton.

[The prepared statement of Mr. Deasy follows:]

Senator Rounds: Vice Admiral Norton, welcome.

STATEMENT OF VICE ADMIRAL NANCY A. NORTON, USN, DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY, AND COMMANDER, JOINT FORCE HEADQUARTERS-DEPARTMENT OF DEFENSE INFORMATION NETWORK

Admiral Norton: Good afternoon, Mr. Chairman, Ranking Member, and distinguished members of the subcommittee.

As Mr. Deasy said, I'm Vice Admiral Nancy Norton, and I serve as the Commander of the Joint Force Headquarters-DODIN, or JFHQ-DODIN, and the Defense Information Systems Network -- I'm sorry, the Director of the Defense Information Systems Agency, also known as DISA.

Thank you for your invitation to join Mr. Deasy and Brigadier General Crall here today as we discuss our cybersecurity efforts.

The JFHQ-DODIN was created to globally integrate command and control for DODIN operations and Defensive Cyberspace Operations Internal Defensive Measures, or DCOIDM, across all 43 DOD components. As an operational component command under U.S. Cyber Command, JFHQ-DODIN provides unity of effort and unity of command across the DOD's layered defense construct to protect DOD networks. JFHQ-DODIN exercises Directive Authority for Cyberspace Operations, or DACO, to establish a coordinated approach for implementing priority actions at all levels of cyber defense.

In addition, we issue orders and directives to all DOD components that address threats and vulnerabilities to the DODIN. Our daily interactions with all 43 DOD components involve sharing cybersecurity operations information and cyber intelligence, validating status of directed cyberspace actions, and updating defensive cyber priorities regarding unclassified and classified networks and cyber-enabled devices that are connected to the DODIN.

JFHQ-DODIN provides the operational requirements and expected outcomes align to the Cyber Strategy and the cyber top ten, which benefit from the standardization of capabilities across the cyber enterprise that is directed under the DOD CIO's authority. Additionally, JFHQ-DODIN conducts cyber readiness inspections, which require each network owner and their cybersecurity service providers to understand how their cyber readiness relates to their own mission and operational risks, and reviews their cyber compliance factors.

DISA is a combat support agency that provides, operates, and assures command-and-control and information-sharing capabilities in direct support of joint warfighters, national-level leaders, and other mission and coalition partners across the full spectrum of operations. Its primary purposes are to provide the information technology necessary for the DOD to protect our Nation and to support the JFHQ-DODIN and U.S. Cyber Command in defense of ongoing cyber attacks, clearly critical to national security.

DISA is a combined workforce of approximately 16,000 military, civilian, and contract employees. DISA is operating and evolving a global enterprise infrastructure based on common standards set by the DOD CIO, enabling effective, resilient, and interoperable solutions that support multidomain warfare in the face of escalating cyber threats. DISA directs, coordinates, and synchronizes the DISA-managed portions of the DODIN supporting the DOD around the world, and supports U.S. Cyber Command in its mission to secure, operate, and defend the DODIN.

DISA's acquisition strategy works to provide efficient and compliant procurement services for information technology, telecommunications, and cybersecurity capabilities in defense of our Nation. The agency relies on a robust partnership with industry to achieve its mission. Just as the military services look to industry to design, build, and field weapons and platforms based on stringent requirements, DISA looks to industry to design, build, and field cybersecurity tools that will meet our stringent requirements in the rapidly evolving cyber domain. DISA's trusted partnerships with industry are critical to bringing effective and secure capability to leaders and warfighters around the world. DISA routinely engages with industry to ensure they have a clear understanding of what the Department needs are now and how we anticipate they will evolve in the future. Both DISA and Joint Force Headquarters-DODIN focus on one primary endeavor: to connect and protect our joint warfighters in cyberspace to increase lethality across all warfighting domains in defense of our Nation.

I thank you for this opportunity to be here today, and I look forward to answering your questions.

Thank you.

[The prepared statement of Admiral Norton follows:]

[SUBCOMMITTEE INSERT]

Senator Rounds: Thank you, Vice Admiral Norton.
General Crall, you may begin.

STATEMENT OF BRIGADIER GENERAL DENNIS A. CRALL, USMC, PRINCIPAL DEPUTY CYBER ADVISOR AND SENIOR MILITARY ADVISOR FOR CYBER POLICY

General Crall: Thank you, sir. I certainly appreciate, like the others, the opportunity to come before the subcommittee and share a few thoughts and ideas, answer your questions. But, more importantly, I thank you for your genuine interest and help in this critical domain. It's made a difference.

Just want to cover a couple items. If last year, maybe, the theme was on strategy, sir, and you've mentioned the fact that we finally published a Cyber Strategy, complete with a posture review. We can take a look at some of those gaps that we have, and get after them. I would say this year's moniker is a bit different. This is about implementation. We know where we need to head. We know the pacing that we have in front of us. But, it's now time to show results. So, I would say that this is the year of outcomes. And that's what we're focused on, is delivering the capabilities and improvements that we've discussed for some time. We have actionable lines of effort that come from our Cyber Strategy. These are things we can do and we can measure our progress against. And that's what we're focused on.

So, while it's a good year for implementation, I would say it may not be a good year for some items. And let me just share with you a couple of those.

The first is stovepipe solutions. It's a bad year for those who like to approach this in a way that we have endless niche capabilities, that those run off and do business their own way, lack of standards, individual development, and difficulty in integrating. We're putting an end to that practice, which has really robbed us of success.

It's also a bad year for those who don't like measures of effectiveness or discussions in data-driven return of investments. We owe an accountability for how we've spent our money and also a level of accountability on what capabilities we've achieved in the spenditure of that money and effort.

And lastly, I would say it's a bad year for those who like endless pilots, pathfinders, and experiments that lead to nowhere. This is about getting to results, experimenting quickly, informing the -- and the learning that we get from those, and putting that back into implementation.

So, I do agree that there's a sense of optimism. I think the Department has turned a corner. But, this is the year that we really have to show the results of that effort.

And I look forward to answering your questions.

[The prepared statement of Brigadier General Crall follows:]

[SUBCOMMITTEE INSERT]

Senator Rounds: Thank you, General Crall.

We've just been advised that we have votes at 3 o'clock. And so, we will probably just keep the committee going, but we'll take turns leaving, going and getting the vote in, and then coming back in. So, no disrespect meant, but we're going to be rotating in and out.

To all witnesses -- and this is a question that I guess I gave you all, kind of, a heads-up on that I'm going to ask today -- in a hearing with private industry on best cybersecurity practices, we heard from Dimitri Alperovitch, of CrowdStrike, that they have a 1-10-60 challenge for responding to cyber intrusions: 1 minute to detect it, 10 minutes to understand it, and 1 hour to contain it. How well would DOD measure against these metrics? And are there any services or components that are better positioned to meet these goals?

Mr. Deasy, I'll let you start, and --

Mr. Deasy: Sure.

Senator Rounds: -- you can pass it off, if you'd like.

Mr. Deasy: So, this is clearly a operational question on how you handle a realtime event.

Senator Rounds: This is a metrics question.

Mr. Deasy: Absolutely. So, this is clearly best for Vice Admiral Norton to answer, since this is what she faces every day.

Admiral Norton: Yes, sir.

So, I appreciate that question, and definitely enjoyed the conversation that you had with industry in talking about that. That way of thinking about the challenge that we have, 1-10-60, was a good way of laying out what kinds of speed that we need in order to pace cybersecurity threats.

I -- we have not, in DOD, laid out a similar kind of benchmark, like the 1-10-60, but absolutely are looking at what it -- what are the requirements for detecting as rapidly as possible, responding as rapidly as possible, and how we can continuously increase that pace at the pace of cyber. So, I would like to take that question off the record for specifics on the response, but very definitely understand that we are watching and building towards a timed pacing of our adversary like that, just with not -- without that 1-10-60 construct.

[The information referred to follows:]

[SUBCOMMITTEE INSERT]

Senator Rounds: Okay. But, I'm going to go one step farther, and this time I'm going to direct it to General Crall. Metrics are important. In this particular case, CrowdStrike, who is public, clearly can say, in public, that's their goal. Metrics like this, are these -- are these metrics that should be attainable, or are these metrics that an enterprise such as the DODIN -- is this something that they can -- that they look at right now? Are there metrics out there that we're trying to achieve? Share with me your thoughts about the importance of this type of an approach.

General Crall: Yes, sir. I think, even in my opening, I talked about our ability to measure. So, there's no doubt that we need metrics in place. I can't comment specifically to the 1-10-60, whether that's the right metric for every DOD domain. These domains are constructed quite differently. And, even with some tactical-edge considerations on how they operate, we take some unique risks at the tactical edge that we might not take in other aspects of our network. So, those need to be tailored to the mission at hand.

But, I would say this. The right question is -- for a closed session, perhaps -- is, What are our metrics? And how are we striving to achieve them? And, in a closed session, I think we could talk about some of the first efforts that Mr. Deasy has laid, that I'm helping institute, as it comes to some detection, remediation efforts that would drive to that.

Senator Rounds: Thank you.

Mr. Deasy, you have publicly announced that your four priorities are cloud, AI, cybersecurity, and C2. What progress have you made in modernizing the Department's cybersecurity? And does your office have all of the resources it needs to execute these priorities?

Mr. Deasy: So, I would say that, when I talk publicly about those four priorities, one of the things that I point out is how interlinked those are, meaning that, if you're having a cloud conversation, cyber is -- the way we're going to institute cloud is very much going to help our cyber posture. It's going to help the way we build applications, it's going to way the house we -- the way we house our data. When we think of AI, AI is very much going to help the cyber agenda. Some of our early national mission initiatives are looking at, How do we use AI, for example, to look at insider threat? How do we look for anomalies in our environment? And then, finally, command-control communications, the C3 side. We know that we have generations of communications equipment that was designed in what I'll call a pre-cyber era. So, as we build the next generation of command-control communications, we are building them, first and foremost, with, What does it mean to have the right cyber in place?

So, I would say that, as I go about discussing these priorities, we always say that cyber is at the heart of the digital modernization of Department of Defense. Everything that we are baking in and building for the future is starting with the mindset of, we must bake cyber in from the start.

Senator Rounds: Thank you.

Senator Manchin.

Senator Manchin: Thank you, Mr. Chairman.

And, if I can, with Mr. Deasy, you have a -- quite a -- quite an impressive resume, basically in the private sector. Coming to the government sector, we appreciate you for your service. And seeing that, basically, over the years, how we've been hacked and espionage that's gone on, and the things that I have mentioned, as far as a thousand different sites, if you will, and none of them seem to be talking to each other or protecting each other, do you believe that we can rapidly close that gap and change our approach to how we do business?

Mr. Deasy: It's a -- it's an outstanding question, and probably one of the top ones every day I address. And I think General Crall actually hit upon it. The days that people, what I like to refer to as rolling their own solutions, standing up unique systems to solve unique mission sets, has to be revisited. So, one of the things, especially now, given the new authorities that I have, is that we are putting out a tone that, as we go through the remediation of our various cyber programs, the days of debating, "What's the various tools and software that we're going to use?" -- we have to stop. We have to quickly move from the debate of "What's the right source of a solution?" to the implementation approach. I've always said, there's no reason we need different tools to solve for many of these problems. The way we will implement those tools are obviously going to be different if you're dealing with a tactical edge and advanced space versus if you're going to deal inside the Pentagon. But, I have been very direct and quite vocal that we need to standardize more, we need to stop rolling individual solutions, and we need to move beyond the debates of, "What are the right product sets?" And we need to spend all of our time talking about how to get the work done.

Senator Manchin: I wanted to ask you about your cyber top ten to see where you're working. But, first of all, on -- the different types of systems we have been using in different applications in the companies we have dealt with, or contracted with, speaking of Kaspersky, Huawei, have you gone through -- have you all been able to see if we're still using those contractors?

Mr. Deasy: Yeah.

Senator Manchin: Or their equipment?

Mr. Deasy: I would say that some of this discussion should probably be held in a --

Senator Manchin: Classified.

Mr. Deasy: -- private -- you know, classified session. But, I can say, generically, that, yes, we are aware of the capability of those particular --

Senator Manchin: Let me just ask you. Have you all evaluated --

Mr. Deasy: We have evaluated --

Senator Manchin: -- what your -- because I was on Intel, so I -- I mean, I know where you're coming from. But, have you all done the evaluation we probably requested in Intel to tell us who is still using -- in any departments, are still using these --

Mr. Deasy: Yes.

Senator Manchin: -- these components?

Mr. Deasy: We have evaluated. Happy to share with you, offline, what the results of that are --

Senator Manchin: We'd love to see that.

Mr. Deasy: -- and, more importantly, share with you the approach we're using, as we find additional vendors, how we deal with this.

Senator Manchin: Well, maybe Chairman and I can get together with you all on that --

Mr. Deasy: Okay.

Senator Manchin: -- in a classified setting.

How about your top-ten issues to characterize your priorities?

Mr. Deasy: Yeah. So --

Senator Manchin: Can you tell me what are your items of your top-ten list, and what's the relationship with the Cyber Strategy?

Mr. Deasy: So, the way that I describe the top ten is, we stepped back -- because if -- depending on who you went and talked to inside the Department and said, "What is a risk?" you would get a very different answer, because your commander, if you're talking to someone who's sitting at a endpoint, your desktop, or if you're out managing a weapon system. So, we stepped back and said, "If you think this through the eyes of an adversary and how they think of the world, how they would traverse the Department of Defense," we stepped back, and we laid out a set of priorities to address all the points of interventions where we think adversaries would try to intersect with us. Obviously, it would not be prudent for me, today, to walk through each of those individual ten things, as one could draw conclusions from that, but suffice to say we've taken a very holistic approach, for the first time, of how we think about all aspects of the chain of how data moves across Department of Defense, and then, What are the points that we need to put prioritization against?

Senator Manchin: And just -- Admiral Norton, you're the Director of the Defense Information System Agency, correct? But, you're also dual-hatted as the Commander of the Joint Force Headquarters for the DOD Information Network for the totality of the DOD's networks. Are all the cybersecurity -- all the cybersecurity providers scattered across DOD, are they under your purview, your command?

Admiral Norton: They are not under my command, sir, they are under my Directive Authority for Cyberspace Operations. So, those cybersecurity service providers, in some cases, work for me, as DISA; in other cases, they work for the military --

Senator Manchin: How about the cyber protection teams?

Admiral Norton: The cyber protection teams are the same thing. I do have some. I have six of those that are -- that work for me, specifically, as the Joint Force Headquarters-DODIN, directly supporting the DODIN backbone and the perimeter defenses. But, others of the cyber protection teams are assigned to the services and some to each of the combatant commands, as well. But, all of those, both the cyber service -- security service providers and the cyber protection teams, as well as every system administrator, every -- every one of those cyber workforce, is under my authority for -- Directive Authority for Cyberspace Operations, meaning I can synchronize the actions across all of the DOD of any responses that we need to take, any changes that we need to make on the network, based on that DACO authority that I have under U.S. Cyber Command.

Senator Manchin: Well, I mean, your last response there, but, basically, how can you prevent, through cyber, the attacks that may be going on, could be going on, if you're not over total control? And, basically, if your one directive goes across all of the different commands, if they're -- what I'm understanding, at first, you're not -- they don't report directly to you, and they are in each -- each of the commands have different chains?

Admiral Norton: Yes, sir. So --

Senator Manchin: Is that a disconnect there? Are we not --

Admiral Norton: I don't believe it is. JFHQ-DODIN was stood up specifically to do the synchronization and command-and-control of the defensive cyberspace operations forces across the DOD. So, you know, it would be very difficult to aggregate them all into one command. There are about 250,000 cyber workforce across the DOD. They're as disparate as, you know, serving in a squadron in the Air

Force or a submarine in the Navy, every one of the agencies, across the board. But, with that Directive Authority for Cyberspace Operations, I'm able to mandate what kind of actions they're taking on a daily basis, and do that through a daily cyber tasking order that we have with all 43 components.

Senator Manchin: I think, in a nutshell, what I'm asking, How do we prevent a Snowden from continuing all the different breaks that we've -- that the public knows about? There's more that they don't know about. The ones that have been very public, have we taken steps? And, Dr. -- Mr. Deasy or General Crall, you've seen this through your career. Is there steps being taken to close that loophole so that doesn't repeat?

Admiral Norton: Yes, sir. We absolutely have. There are many, many actions that we've taken. Snowden, of course, was an insider threat, and we have taken specific actions --

Senator Manchin: Right.

Admiral Norton: -- addressing an insider threat, across the Department. There's always more to be done, because that's a very complex problem, getting at that. But, we absolutely have. And Joint Force Headquarters-DODIN has only been in existence for 4 years, this week, so we are maturing in the ability to synchronize all of those efforts.

We didn't have this when Snowden -- you know, Snowden was able to infiltrate and exfiltrate the data that he did.

Senator Manchin: I'm going to go vote, and I'll be right back.

Admiral Norton: Yes, sir.

Senator Rounds: Let me just continue on, because I think that's an important part of it. The reason why we do the open hearing now is to talk a little bit about how big this challenge is, because you're talking about not just all of the Armed Forces, but you're also talking about our acquisition processes, you're talking about a huge contractor base out there that is just as susceptible to cybertheft as our armed services are. And yet, all of our air, land, and sea domains are at risk if our cyber domain is not secured, just like our space domain has to be secured. And I think that's part of the message we're trying to get here, is, This is not something that can be done simply by the Department of Defense alone. This is a case of where we have to have the rest of industry, obviously, in tune with us. Can you talk a little bit about the coordination which you're trying to do with those entities that are defense contractors and their subcontractors, how big this is, but also what you're doing to try to focus on that?

Mr. Deasy: I -- I'll be happy to address that.

So, it turns out, on that top-ten priority list, one of those is the defense industrial base, or often referred to just as the supply chain. I mean, look, it's very, very clear that -- and you're right -- defending our networks extend all the way out to our contractor networks. You could argue they're just an extension of what we do. We pass classified data. They do things on behalf of us. So, there's no doubt, when you look at the first tier and the second tier, and you think about exfiltrations and the problems that have occurred, we have to treat our subcontracting base the same way that we think about defending our own networks.

Now, to that end, we get some help. There is standards that our defense contractors are obligated to follow. It's the NIST standard. It's the same one the Department of Defense follows. We have recently stood up -- you probably have heard -- the Deputy Secretary stood up a task force. I had made a recommendation that we need to look at, holistically, from the day we awarded a contract to the moment we have an exfil or spill occurred, and how we then handle that needs to be re-thought through. And so, right now, there is a task force that is stepping through the entire way that we handle our contractual relationships, our notification of problems, our forensics, and, when we do have a problem, to improve upon that.

One of the problems we see is, this problem is not necessarily a tier-1 supply level -- is, to your point, it's down in -- really, when you get to the tier 3 and the tier 4.

Senator Rounds: Explain what that is.

Mr. Deasy: So, in this -- in many cases, we will contract with a very large traditional defense, but they don't build everything for us, they don't engineer everything for us. They will go out and contract with a firm --

Senator Rounds: Which means they share classified information with their subcontractors, who may very well share that same classified information with a subset of contractors again.

Mr. Deasy: And that entire chain is tracked. Where the issue breaks down is, as you go down to those various subcontractors, do they understand, equipped, have the knowledge and the capability to defend themselves? And what is it that we should be doing more to help them learn how to defend themselves at those tiers?

Senator Rounds: Okay. It's not a new problem. But, most certainly, it's one that this is where we find a lot of our hygiene problems at. And that's the way most of our information is lost, is through improper cyber hygiene, meaning somebody at a level, basically, made a mistake, and somebody got into their system and now has access.

Can you talk a little bit about -- it's one thing to make a law or a rule. It's another thing to be able to enforce it. Talk to me about your enforcement actions and how you see ways to, not only make the law, but enforce the law, and then to follow and audit the process. What do you have in place, and where are you short of capabilities today?

Mr. Deasy: So, first of all, you make a very good point. If you look at a lot of the problems that have occurred and where the forensics' been done, it is -- it does come back, many times, to basic hygienes. So, we start with a self-certification process. We are now looking at a new process that A&S is leading, and that is, How do we then build in a confidence score against their --

Senator Rounds: ANS.

Mr. Deasy: -- certification? The AFGAT position --

Senator Rounds: Okay.

Mr. Deasy: -- Ellen Lord's -- Ms. Lord's organization, where they go through and they evaluate that self-assessment, they put a confidence score against that, and then, what they're now looking at is, How do we go out and have a closed-loop system, where we can go out and validate what it is that they self-assessed against? Now, of course, this is a massively large supply base, so there's discussions right now on, What is the right approach on doing that, given that trying to get every single member of that supply base might be overly challenged? And so, how do you sample, and how do you do this in a way where you can start to get confidence that, as you move down those tiers, that their self-certification --

Senator Rounds: Let me follow up, because I think that's a critical lead-in to another piece here. And, as other members come back, we'll allow them to get into this, as well, but I -- I have to ask. Even if you could hire -- and I know that you need to hire more experts in cybersecurity, but you're also going to have to hire and contract out with entities that have real expertise in cybersecurity. Do you have a process in place to invite and vet expertise within cybersecurity that we can use to help us? And then, once you get past that stage, the -- you recognize that you can't do it with manpower alone, you're going to have to have the additional electronic resources, including AI. Can you talk -- work your way through that, from the -- from looking outside of government, manpower needs, and then also moving to AI?

Mr. Deasy: So, as you know, I do come from private industry, and this problem for large companies, private industry is no different; i.e., they don't have the capability to evaluate every one of their supply-chain vendors. So, what has happened in private industry, which is what we are now looking at for the DOD, is actually a process of identifying, possibly even certifying, companies that can play the role that can follow the NIST standard and actually go in and look at a second-, third-tier supplier.

Senator Rounds: Are you taking invitations for that now?

Mr. Deasy: No, we are just in the early discussions of how we would --

Senator Rounds: Okay.

Mr. Deasy: -- might do that. As I said, A&S is the lead for this. I've been advising them on how this has been done elsewhere.

We haven't started -- I mean, to your AI question, there is definitely going to be value in looking at, How do you take the entire supply base, the NIST standards, the hygiene problems we see, and can you apply AI to this problem to start to identify where you may -- most likely are going to experience problems inside your supply chain? We are just -- literally just in discussions. I do not want to suggest that we have an active program underway. But, I would suggest that this is a good case where we can apply machine learning to looking at this problem.

Senator Rounds: I will give Senator Scott an opportunity to get settled, but I'm just going to ask you one more question. Then I'll move to Senator Scott.

Right now, there really is a difference between AI and machine learning. Are you deeper in with machine learning right now to cover a lot of the items right now that otherwise we just don't have the manpower to cover? How far along are we?

Mr. Deasy: We are still very much in the early days. I would actually be very happy to come and have a session with you on what is called the Joint Artificial Intelligence Center and how we're using that to apply new AI/machine-learning algorithms to solve for some of these problems that I think you're touching upon here today. But, probably best that I come and talk to you offline about how we're approaching the AI/machine-learning problem.

Senator Rounds: Very good. Thank you.

Senator Scott.

Senator Scott: I'm sorry if I ask a question that somebody's already asked, go do a vote.

How do you deal with -- how -- you know, you get a lot of wonderful vendors all -- from all over the United States and around the world that want to sell you stuff. How do you make a -- how do you all make a decision what you're going to buy and who's the best vendor?

Mr. Deasy: So, there's a number of us that can do that. Why don't we start with Vice Admiral Norton.

You use a number of suppliers. How do you go through your vetting process?

Admiral Norton: Well, we have a lot of different mechanisms that we interact with industry, starting with very public and very open things, like we have a forecast industry, where everybody is invited to come in and hear about what we're doing, what -- you know, what is already ongoing, what is planned in the near future, and then opportunities for each of those vendors to talk to the program managers and the leadership at DISA and get an understanding of what they might be interested in pursuing. We have a Small Business Programs Office that specifically targets and interacts directly with the small businesses that have interest in any of our activities. They feed back into different parts of DISA for -- you know, for further communications. So, that gives us, sort of, the understanding with industry of what -- what's available.

And then, from there, it's evaluation based on the performance criteria that we've set for the particular product or particular capability that we need in understanding what the acquisition strategy might be. In some cases, that means doing a major evaluation of a number of different contractors at companies that have similar products, and evaluating them for the best fit. In some cases, it means something like an other transaction authority, where we have a couple of different prototypes, and both of them are able to build out and demonstrate, you know, what capability would best suit the need that we have.

General Crall: Sir, thank you.

You know, this really does come down, as Admiral Norton talked about, to requirements. That's both stated, what I need today, and what I anticipate, not just simply, as you know, sir, you know, chasing after capability that I might not need or couldn't find a use for, which sometimes they come packaged. We do look at performance. And we look at performance in measures at that tactical edge, which is different. We've found vendors, in many cases, that work very well in a flagpole or garrison environment, but, when we start getting to thin line, red line, or austere conditions, the product may not perform as well, and that's a consideration for a warfighting machine that's expected to operate in an information-contested environment. So, that's one area that we take a look at. And, of course, no shortchanging the idea of cost at something that's sustainable or affordable.

But, the other piece that I think is important is how flexible it is, the thing that we're looking at. You know, requirements do change, and one of the big concerns is not getting locked into something that requires a level of emulation, patching, or, really, caretaking that could exceed the cost of the product to begin with. So, really looking at more, you know, informative ways to do it.

But, the problem really isn't so much about us finding the right vendor that can provide what it is, it's the vendor's patience in dealing with us and our lack of flexibility in acquisition. We find more vendors most likely to walk away from trying to deal with us because of the -- simply the way that we contract. And I'm not saying that we shouldn't contract that way. There's reasons why we have some of the contracting rules and regulations, to ensure that we behave properly. But, you know, in industry, as Mr. Deasy will attest, his experience of finding a solution, matching a vendor with a need, can be done very quickly in the civilian world, where we might find ourselves years out. By the time we compete properly, line up the resources, make sure it's within our POM cycle, and actually move on it, the product might not even be viable at the time of purchase.

Senator Scott: So, what needs to change?

General Crall: Sir, I think we're doing the change on the front end, as we are focused on requirements. So, I think we're doing our part. We've had great relationship with the -- vendors are -- really, industry is going to help us get through many of the problems we're talking about. They absolutely bring the technology we need to bear. But, focusing on requirements, that's our responsibility. I think we've done a better job. The way we consume products, moving toward, as a service model, vice having to own everything, is a methodology that we're looking at. And I think we need to be more thoughtful on how we come back to Congress and ask for some help on how we acquire. The acquisition machine on -- I believe, needs to change.

Mr. Deasy: If you ask me, it's one word: speed. I think about how, in the private industry, from the time that they identify that the adversary now has a new set of methodologies and tactics, your ability to go out and scan industry to see who's -- is addressing that, quickly find those companies, bring them in, evaluate them, move through the procurement cycle, and get them operationally installed inside the environment -- it has to be done with a lot more speed than we have today, sir.

Senator Scott: May I continue?

Do you -- so, do you ever feel taken advantage of by a vendor that talks you into a -- an -- a type of RFP, and then you find out, at the end, there were other vendors that you couldn't even do business with because of how you started -- the RFP you started out with? And how do you deal with that, if that's true?

I used to be an investor in national security, and we'd do business with the government. And we'd -- a lot of people talked about -- we didn't -- we won based on how well we did -- helped with the procure, the RFP. Do you feel like -- that industry does that to you?

Mr. Deasy: I would -- I have not seen that. What I have seen sometimes is a poor understanding of your requirements up front, and so you're misaligned because you haven't spent enough time really understanding what your requirements are. The vendor's then -- trying to then come in and sell you something that may or may not meet your requirements. And I see more of a disconnect between what the vendor is trying to tell you they have versus the requirements. And that needs to be, I think, probably vetted at the front end more -- better.

Admiral Norton: One of the things that DISA has done routinely is, we put out RFIs -- requests for information -- in advance of an RFP broadly, and have an ongoing dialogue with industry so that we get a good understanding of what it is that we're looking for, what is available, not -- you know, not trying to put out an RFP for something that will never be produced and will never deliver. So, we'll spend a lot of money on some vendor trying to do that. We don't do that anymore. We always baseline with an RFI, and that gives us a lot of opportunity for understanding.

Senator Scott: Do you think -- you know, part of being decentralized is that it seems like it would make it difficult for somebody to intrude, and, as you get more centralized, then it wouldn't -- are you concerned that'll make it easier for somebody, because, once they figure out exactly how to intrude in your system, they've -- they hit everybody at the same time? Do you have any concerns about that?

Admiral Norton: I am always concerned about that, sir, the -- you know, the balance between the ease of operation and the speed at which you can operate a very homogenous network at, you know, large scale, so if everything is the same and you're able to automate the processes of changing that, then you can do that very rapidly. So, operation and cybersecurity can be done very, very rapidly. But, that same ability is also a potential weakness if an adversary is able to get in, because then they can do the same kind of thing. So, you have to balance that and understand where, essentially, your -- I'm in the Navy, so your watertight doors are for -- you know, for watertight integrity. How do you block that so that that kind of adversary behavior isn't able to penetrate entire -- your entire network?

Mr. Deasy: One of the things I've been advocating since joining is, people -- that's a great question -- people always ask, Are we better off being decentralized? And I would say, but then you have a thousand ways of which someone can get in, so that's the downside of that. If you centralize, then if someone could get in, the breadth of the surface space they can cause damage in, it's much larger. And I always say, it comes down to how you architect for that centralized approach. If you architect with a very flat area, where, once they get in, they can cause great havoc, that's not appropriate. If you're smartly architecting for a centralized approach, where you're limiting what I like to call the "blast radius," what the problem can be occurred, then actually centralization has some huge merits that you don't get, obviously, from a decentralized site.

Senator Rounds: Thank you.

Let me just move on. And I'll have Senator Wicker.

Senator Wicker.

Senator Wicker: Well, thank you very much.

And it's too bad we've got so many balls in the air, we can't be here for the entire hearing.

Has anyone asked you all about China and Huawei and ZTE and Chinese-owned information companies yet? Has anyone asked that in this hearing today?

Mr. Deasy: Yes, sir. Earlier, it was asked. And what we said was, yes, we understand the nature of the problems with those products. We have a good understanding of where they are, and are not, inside of our environment. And we said that, if you would like to go deeper, given the sensitivity and the nature of what those products do, we'd be best to have that conversation in a closed hearing.

Senator Wicker: Yes. But, let's see what we can talk about --

Mr. Deasy: Okay.

Senator Wicker: -- in an open setting like this.

In terms of our National Security Strategy, our new national security policy, is what is contained in there adequate to meet this challenge? How much of DOD's information flows over commercial networks, for example? And do we need to be concerned about that? Is there something going on now with commercial providers to improve cybersecurity of these information networks that involve crucial national security matters?

Mr. Deasy?

Mr. Deasy: Yeah, there's a couple there. There's a part on strategy, and I'll let General Crall take the strategy.

To your point, you bring up a good point. If you think about how data trans- -- moves across Department of Defense, both CONUS and OCONUS, you have to ask yourself, Where are you touching the commercial side of an environment, and how well do we understand the commercial nature of what products, like Huawei's, might be in there? We have a very good understanding for CONUS, what that looks like and what those vulnerabilities are. For OCONUS, as you can imagine, it's a lot more complicated, because those networks sit with providers outside the U.S. And so, we have to architect and be a lot more thoughtful about how we set up on an OCONUS basis because of that.

Senator Wicker: If there are Huawei products, what's our concern?

Mr. Deasy: The concern is that, inside those products, there will be engineered solutions that allow them to send -- capture information that can be sent back to the adversary.

Senator Wicker: And those solutions would already have been engineered and already implanted, in certain instances. Isn't that correct?

Mr. Deasy: I cannot speak to the detailed engineers' designs of the Huawei products, but, in theory, yes, if that product was engineered with backdoors where it was exfiltrating, that would be the case.

Senator Wicker: So, I'm concerned that that capability may already be out there and installed in many places outside the continental United States, which is what you're saying when you say "OCONUS."

Mr. Deasy: Uh-huh.

Senator Wicker: Now, General Crall, what would you like to add about that?

General Crall: Sir, I realize the focus on outside CONUS, but I don't know that I would exclude inside CONUS.

Senator Wicker: Right.

General Crall: To your point, a lot of the gear -- when you talk about how we're talking about networks and service providers in -- and that there's some level of granularity you can have in researching the flow of traffic and how they're handled, but there's also the smaller end the, you know, peripherals, the switches, the routers, the hardware that allow these, you know, connections to take place. We understand what white gear is. These are -- you know, the fact that you can't trust what's on a label. There's a concerted effort to ensure that what's marked is, in fact, what's inside. So, to your point, you have concerns, potentially, that there could be challenges in making sure that the authenticity of the gear is what's stated. And that concern is shared. And, in a closed session, sir, we'd be able to provide a little more detail on how we examine that.

Senator Wicker: Admiral, do you have anything to add?

Admiral Norton: Just that we have done an enumeration of that equipment, and so we do understand what is out there. And again, we can talk about the specifics in a closed hearing.

Senator Wicker: Very good.

Well, thank you very much.

And I am told that Senator Gillibrand is next.

Senator Rounds: Senator Gillibrand.

Senator Gillibrand: Thank you so much.

I want to ask a little bit about cybersecurity architecture, because I took, from Senator Wicker's questions -- he talked about ZTE and Huawei already. Forming consistent and comprehensive cybersecurity architecture across the DOD and, frankly, across all of government, is vital to our national security. What roadblocks are currently in place that inhibits this from being a reality? And do you all feel that you have the necessary authorities to overcome those roadblocks?

Mr. Deasy: I don't see roadblocks. I see legacy. That is probably our biggest challenge. So, for years -- we had this conversation earlier -- we have allowed services and various components to roll and implement unique solutions that maybe aren't interoperable or standalone. As I said earlier, with the new authorities that the DOD CIO office was granted, starting this year, it now allows my office to establish the standards and the architectures that the components and the services have followed, which was why General Crall made the comment earlier that this is the year, now, where there will be a lot of noise in the system, because we are going to drive those standards. We're going to drive implementation. And we know there will be people that are going to be very uncomfortable about the fact that we're no longer going to allow them to stand up their own architectures or solutions.

Senator Gillibrand: Right.

Either of -- do either of you have anything to add?

Admiral Norton: Yes, ma'am. I'll just add that one of the difficulties of changing the architecture in the military is that we rely on these systems for ongoing missions every day.

Senator Gillibrand: Yep.

Admiral Norton: And so, the time that it takes for finding time where you can take a system offline in order to make the upgrade ends up oftentimes being the long pole in the tent of actually changing the architecture, which is why we have -- oftentimes have a lot of legacy. Funding can become a problem, but the time is actually the driver in most cases. And, you know, we have to -- as we build out future architectures, we have to build in the ability to make those changes very rapidly on the fly, without having, in some cases, you know, weeks and even months of downtime for the systems for something like a ship or an airplane or a headquarters building.

Senator Gillibrand: Yep.

General Crall: Ma'am, I used to think that starting things was the most difficult thing in the Department. I've since learned that stopping them, potentially, is more difficult.

Senator Gillibrand: Welcome to the Federal Government.

[Laughter.]

General Crall: So, I think that really driving toward ensuring that, while we have a plan to onboard new capabilities, we're smart in making sure that we can retire legacy, where appropriate, because we end up in this position where it's simply not affordable to keep it all alive. And we've been a little slow on retiring legacy, but we have a plan, under the new Strategy, in the lines of effort to get after that.

Senator Gillibrand: A section of the NDAA I helped craft directed the Secretary of Defense to enhance awareness of cybersecurity threats among small manufacturers and universities working on DOD programs. What actions have been undertaken to execute this order? And how successful do you believe these actions have been? And, more to that point, a lot of the industrial base has led to an emphasis on bringing in more small businesses in the process, but meeting cybersecurity requirements is really hard for them. So, related, what does the DOD do now to help those small businesses with cybersecurity so that they could participate in the future?

Mr. Deasy: So, as we had discussed earlier, that topic is actually part of our top ten priorities. A couple dimensions of that -- I'd actually say there's probably three dimensions. You mentioned the academia dimension of that. You mentioned the small business dimension of that. We definitely need to help figure out how we're going to handle small businesses. If you look at what it takes today to do good cyber hygienes to stay ahead of the adversary, we know many of the second- and third- or fourth-tier supply base simply doesn't have the wherewithal to do that. We have some thoughts underway about how we can bring them into -- whether it's a cloud or an extension of our network, and we can fortify them with services that we provide. We are in the very early days of that. But, you should know that we're in active conversations of how to do that.

The other thing we're doing, as was discussed earlier, is, we've stood up a task force that reports directly to the Deputy Secretary of Defense. And that task force is looking at the end-to-end way that a supply chain works, which includes the academic world around base research that's done, or maybe more classified work that's done on our behalf, and how do we really understand and get a better handle on how that research is done, where it's done, and what are the mechanisms that these institutions are using to ensure that things are being done in a safe, sound manner.

Senator Gillibrand: Thank you.

Thank you so much.

Thank you, Mr. Chairman.

Senator Manchin [presiding]: Thank you, Senator.

I have a quick question, and then we'll go back to Senator Wicker for a second round.

As -- in any competition, you're always evaluating your opponent. As we evaluate, in the cyber technology realm, if you will, our opponents, how do you rate our opponents, China and Russia -- where they are today, where we are today, and their opportunity, basically, either to stay ahead, pull ahead, or you feel comfortable, the direction we're going, that we can basically offset the advancements they've made in such a quick period of time?

So, we can start -- General Crall, and just come right across.

General Crall: Yes, sir. I think I'd have difficulty answering that in open forum. I would say this, though, just to characterize your question, is that we are -- you never rest, as you know, on any capability or laurels that we have. We know what we know, but there's a concern about what we don't know. And we have a lot of suspicions on where our peer and near-peer competitors are --

Senator Manchin: You're identifying your two competitors, or two of your most challenging competitors. I guess it would be -- we've said this in open meetings before. I mean, it's going to be China and Russia, correct?

General Crall: There's no doubt, sir, that they are at the top of our --

Senator Manchin: Okay.

General Crall: -- priorities. And when you look at their capabilities, they are increasing, as are ours, and --

Senator Manchin: Yeah.

General Crall: -- which is why it requires great vigilance.

Senator Manchin: I think Senator -- no, go ahead if you were going to --

Mr. Deasy: Yeah, I was just going to -- just --

Senator Manchin: Go ahead. Go ahead, Mr. Deasy.

Mr. Deasy: So, to the General's point, difficult, in this setting, to answer some aspects of that. I will tell you that I have a weekly session, where I am briefed by U.S. Cyber Command and NSA, and we specifically are briefed on China and Russia. And one of the reasons I wanted to get into this normal cycle of doing these briefings was, to the very point that I think you're trying to poke at, is trying to understand, vis-a-vis where we are on our offensive as well as defensive capability. And suffice to say that these are very strong, capable adversaries, but, at the same time, we have some strong, capable --

Senator Manchin: Yes.

Mr. Deasy: -- abilities, ourselves.

Senator Manchin: Admiral?

Admiral Norton: Yes, sir. I will echo their comments about specifics, in terms of capabilities against our adversaries would be better in a closed session. But, I will say that China and Russia both have very clearly exercised and demonstrated their, not just ability, but willingness to fight in this domain. And we see that every day. And, regardless of the adversary, we see the concerted effort to attack the United States and the Department of Defense.

Senator Manchin: Acting Director Shanahan, do you -- is he committed to implementation of the new Cyber Strategy?

Mr. Deasy: Absolutely. One of the things I said in my opening remarks that I should really stress is, when I came onboard, one of the things that he wanted to establish was a weekly cadence for CIO Cyber. We call it the CIO Cyber Working Group. He personally, before his new duties came into play, chaired that meeting. He was at it every week. He would look for the metrics. He would be quite the tasker of ensuring the activities were getting done. And he's done a very strong handoff to, now, the -- assuming the duties of a Deputy Secretary Norquist, who is now continuing that. So, you should know that one of the things I have been incredibly pleased since joining the Department is to see the top of the house be extremely active on a -- what I'll call a very frequent basis -- i.e., weekly -- in the engagement of all the activity that you heard us talk about today.

Senator Rounds [presiding]: Senator Wicker.

Senator Wicker: Well, that's good to know. And it -- it's encouraging. And I'm sure it's encouraging to Senator Manchin, too.

My last question deals with data rights and data control policies, getting the best technology, but at an affordable price. You've got a company there with good technology. They're profit-oriented. They don't have to make a deal with anybody. They're under no special obligation to do business with the government. So, how are we doing with regard to our policy there? Does it deter cutting-edge cybersecurity companies from doing business with the Pentagon? Is it difficult to strike a balance between getting the best and getting something we can afford? And what's your assessment of the Department's data-rights and data-control policies?

General Crall: Yes, sir. I can certainly tell you there's a focus. And you bring up a couple issues when it comes to rights. I think the verdict is still out, by the way, on who owns data. Lawyers will tell you, when you go through this understanding of where it's housed, how it's moved, what residual components of data reside. We care. We're concerned. And we have policies in place on where we put that data in the Department of Defense.

What I think the -- you know, and, to your comment about the struggle between affordability and really doing business with the best -- the best customers are always the desired customers -- it would not be truthful for me to tell you that, in every instance, we get the best of both worlds. Again, because of some ways that we acquire services, we often, or at times, have gone with what is the most expedient or those we could do business with based on rules and regulations. So, we're still finding our way through that, in some cases.

But, the real focus, I think, for the Department, when it comes to policy and implementation on the strategy, is really how we start focusing on data and data security at rest and in transit. Maybe less with how it's stored or transported in conventional ways, but more accurately now is, How do we safeguard it in all aspects of it at rest and in movement?

Senator Wicker: Are you able to be specific about rules and regulations that you referred to? What would be an example?

General Crall: Sir, I could -- I mean, I would like to come back to you in writing on rules and regulations, to be specific. But, the idea, for example, if we wanted to host data in a commercial cloud today, and let's say that data was unclassified data, there's a reason why we tend to put these -- this data repository under certain controls, like Federal ramp, you know, conditions on storage and security, but also on premises. I can just answer for the Marine Corps, that, when I was the CIO, prior to this job, I personally felt uncomfortable in some business arrangements of putting my data in a commercial cloud, where I could not guarantee that, if I stopped doing business with that company, of what it meant to return the data to me. It's electronic. I didn't know what I would get back. So, a very specific example personally --

Senator Wicker: You didn't know if you would get it all back.

General Crall: That's correct, sir. So, I ended up storing that data on prem, where I could control it, and I asked for services to push that data through those commercial contractors. But, things have changed since then. There are some safeguards that are out there that make doing business that way maybe a little better when it comes to encryption, which is what I was getting after, meaning I might be able to house that data under certain rights where I hold the keys to that encryption and feel more secure about where it resides.

Senator Wicker: Okay. Well, you're going to get back to me with a supplemental answer on it for the record.

General Crall: Yes, sir.

[The information referred to follows:]

[SUBCOMMITTEE INSERT]

Senator Wicker: Thank you.

Thank you, Mr. Chair.

Senator Rounds: Thanks.

Senator Blumenthal.

Senator Blumenthal: Thank you, Mr. Chairman.

And thank you all for your service and for being here today.

In an annual assessment of cyber threats reported by Bloomberg News -- you may have seen that report -- the DOD's Operational Test and Evaluation Office, according to that report, found that the Department has not fully grasped how to counter new threats posed by emerging technologies like artificial intelligence. Mr. Deasy, the CIO position has served as the principal advisor to the Secretary of Defense for a breadth of issues beyond cybersecurity, including information technology, communications networks, and the like, command systems. In your prepared remarks, you cite a number of emerging technologies that DOD has identified for potential use, such as software-defined networks. I know that Senator Rounds asked you some questions on this topic. You also noted that DOD has evaluated machine learning, artificial intelligence systems that are working to integrate these capabilities and networks. So, for you, and maybe for all the witnesses, what are the artificial systems currently useful at DOD, and what's holding DOD back elsewhere in -- is it in-house expertise, technical resources, state of the field? And maybe you would comment on the Bloomberg report, as well.

Mr. Deasy: Yeah. So, work very close with the DOT&E, very much aware of that report. It's quite interesting. When you go through the observations in that report, they point out things like leadership responsiveness finding hygiene problems. They point out things like nuclear command and control in the age and the serviceable life of equipment. They talk about stolen credentials, breaches of defense contractors. The top-ten program that we have been referring to throughout the testimony today was actually created, as I said earlier, to look at, holistically, where are all the intervention points that adversaries can touch us, and how do we address that? So, I'm pleased that, when I look at this report, that many of the things that are sitting inside of the top-ten stuff that we're starting to implement actually mirrors very nicely to the report.

The other things inside that report, on the very end of that report, it makes observations about where they see improvements. And one of the things that they point out clearly in there is that they now believe the Department of Defense is scoping the task properly, they believe there is a followup -- there is an organizational construct in place across Department of Defense to address these problems, and that we now know what are the tools and the skillsets that we have to put in place to get after it. So, that's kind of part A to your question.

To the part around the other activities, may it be artificial intelligence, the use of cloud, the use of next-generation command and controls -- as I stressed earlier, when I talk about the digital modernization of Department of Defense, I always like to remind people that this is a highly integrated set of things that we're doing. I always start off by saying there is no doubt that AI and what it's -- offers the Department is going to be quite significant. How we implement that is going to require that we put in a robust enterprise cloud. How we secure that cloud, how we use commercial providers to put the AI on top of that is very important. However, if we don't solve for next-generation command-and-control communications, we will not get the necessary information out to the warfighter. So, you must look at cyber from a communications standpoint, a satellite standpoint, as well.

So, all of these things, to me, are tightly, tightly integrated, and that's why, when we talk about the digital modernization programs Department of Defense, cyber has to sit at the forefront of everything that we do, sir.

Senator Blumenthal: Do either of the other -- do you have any comment?

Admiral Norton: Yes, sir. I'd like to say a couple of things.

One of the things that they talk about in that report is the importance of understanding the cyber terrain and starting to really grasp that. That has been a major effort of the Joint Force Headquarters-DODIN. We actually put out an order that specifically lays that out for the 43 DOD components to identify, map their cyber terrain, map what is key cyber terrain so that we can recognize what -- where additional forces need to be put, where additional emphasis might need to be, to include putting some of our cyber protection teams on that key cyber terrain. And in my opening comments, I mentioned that I am responsible for the command readiness inspections that we have changed from a -- just a readiness inspection of a checklist of configuration to an operational readiness inspection that takes -- that operational evaluation is going to that command to understand, Do they understand what their key cyber terrain is, relevant to their mission, specific to their mission? And therefore, do they know how to protect their mission by protecting that key cyber terrain? Those are the kinds of things that DOT&E has recognized that are really critical for us to move forward and to, you know, not have to expand resources tremendously to protect everything equally, but to focus our resources on the things that are most important in the DOD.

Senator Blumenthal: Thank you.

General Crall: So, sir, I find it interesting that we answer that question a little bit based on some of our portfolio experience and where we sit. So, Mr. Deasy talks about, you know, scoping the problem set, which is in the report. Admiral Norton talks about knowing your terrain. A third in that top three of what they talked about the Department may be doing fairly well at, or at least at the cusp of, is unity of effort. So, one of the areas that --

Senator Blumenthal: Unity of effort.

General Crall: Yes, sir. The idea that finally pulling together -- Mr. Deasy has talked about not going our own ways or allowing, you know, these niche solutions that don't really work well together. So, as one of the implementors of that strategy, we have a strategy that we can execute, we have very clear goals and guidelines, and really looking to ensure that we do this smartly, that we come together to solve that problem. So, I think those three answers really fit well in the top three that came out of the findings in that report.

Senator Blumenthal: Was lack of unity of effort a problem, do you think?

General Crall: I think it has been a problem, sir, to be fair. I think that we've turned a corner on that, that, even well-intentioned people doing business in opposite directions really puts a -- puts us in a fix. For example, of simply putting requirements out on a table and allowing them to be solved in any way, shape, or form sometimes means to get those solutions, to work together as the government needs it to do, especially DOD, you might have more money in emulation and more engineering problems in getting things to fit that are dissimilar than you would if you had a common solution going forward. So, yes, I think that's a -- it's a fair criticism of past performance, but I'd like to say that I think we're on a different track. And I'm pretty optimistic that we can pull together.

Senator Blumenthal: Thank you.

Thank you all.

Senator Rounds: I'd like to follow up just one step further. And I'm going to go to Vice Admiral Norton with this. Today, the Department's cybersecurity architecture appears to be fairly decentralized with, in this particular case, JFHQ-DODIN possessing what I think would be only limited visibility into its components, networks, and endpoints. Is this -- number one, is my premise correct? I think it is. Second of all, if it is, then is this because of a policy decision that needs to be changed? Is it a capacity issue on behalf of JFHQ-DODIN? Or is it a technical problem? And does JFHQ-DODIN need additional resources or authorities to be more effective?

Admiral Norton: Well, first, it was definitely not a policy decision to decentralize the data. Remember, I said that Joint Force Headquarters-DODIN has only been in existence for 4 years. We just reached full operational capability a year ago, this week. So, all of those networks that Senator Manchin talked about -- you know, those thousand networks -- they all grew up with their own ability to look at their own network independently. And, over time, we're starting to aggregate that in a way that does centralize the ability to view that.

Over the last year, Joint Force Headquarters-DODIN has made tremendous progress in getting -- gaining visibility on all of those networks across the DOD. And certainly at the tier-1 level, at the Internet access points, and at the endpoints, and helping to aggregate, as General Crall said, in some cases, you know, in difficult ways, because the technology doesn't necessary make that easy, because they all acquire those in different ways. But, bringing that data together in a way that gives us, at Joint Force Headquarters-DODIN, a much better understanding of what everybody's cyber posture is across all of those networks.

We're certainly not perfect. It's certainly not in a manner that is technically easy and quick, based on the disparate kinds of --

Senator Rounds: Specific --

Admiral Norton: -- solutions --

Senator Rounds: -- resource needs?

Admiral Norton: So, I -- one, an architecture that allows for the kind of standardization that Mr. Deasy is working on and the policy that requires more standardization that General Crall has talked about, so those are already in work. I have the authority, as -- under that Directive Authority for Cyberspace Operations, and have used that, to great extent, to be able to get that data and start to give that visibility to both my forces and to U.S. Cyber Command.

Senator Rounds: Thank you.

Senator Manchin: Can I --

Senator Rounds: Senator Manchin.

Senator Manchin: -- follow --

Senator Rounds: Yeah.

Senator Manchin: Just one followup, there.

I think, for Mr. Deasy and General Crall, I understand that there's a so-called cross-functional team and -- composed of a small number of experts from across the Department, which works, I think, with both of you all. So, I guess I would ask -- Congress created this cross-functional team. Sometimes we're not always spot-on, to say the least. I want to know if you all agree with this team? Is it functioning well, or is there things we can do to help?

Mr. Deasy: So, I'll start with that. And much of the work is actually led by General Crall.

I think we actually have, for the first time, a series of things that are going on that are well. You have a Secretary and a Deputy, as I mentioned earlier, that are highly actively engaged in this topic. So, you need the top of the house to be --

Senator Manchin: Right.

Mr. Deasy: -- highly engaged on this. B, you have a set of leaders that are very impatient, including myself, that are done admiring the problem and are moving into tasking. This is including being less tolerable on people being able to go off and use their own solutions. The authorities that you all gave me, starting this year, around being able to set architectural standards is quite significant. We are now starting to use those new authorities.

And then, finally, you used the term, you know, "cross" -- you know, a team that's been brought together. That, in my opinion, is probably the biggest thing that has helped us, is empowering General Crall by giving him a set of experts that cut across the Department, that are actually helping him now to drive those solutions.

General Crall: Sir, Congress got that right. The cross-functional team works. And it has several advantages. It's only as good as it's paid attention to. There are probably examples of some cross-functional teams maybe not producing. But, the cross-functional team that's involved under the PCA is well resourced, in the sense that we've got the right people. The participating agencies that provide representation in the workforce sent us their best. So, I'll start with that. We've got good people.

The second piece is, we can approach problems in ways that don't have some of the biases. You know, we don't have any stake in the fight or any legacy that we hold on to. It really is about the mission. So, we normally come to the table with an advantage in solving some of those problems. So, it's been instrumental in moving the strategy into implementation.

Senator Manchin: Great.

Thank you all so much. Thank you all for being here.

Senator Rounds: Okay.

I want to take this opportunity to thank our members and Senator Manchin for participating today. This has been very helpful to us.

I'd like to thank our witnesses today for their participation. There were several questions that you indicated you would prefer to answer in a classified setting. I would ask that you provide us with those answers. Committee staff has indicated that you may bring those in at the level of SCI in your responses. And we would expect you to be able to do that in the next couple of weeks. Okay?

[The information referred to follows:]

[SUBCOMMITTEE INSERT]

With that, I want to thank everyone for participating. And this subcommittee meeting is adjourned.

[Whereupon, at 3:55 p.m., the hearing was adjourned.]