Type text here

Stenographic Transcript
Before the

COMMITTEE ON
ARMED SERVICES

UNITED STATES SENATE

TO RECEIVE TESTIMONY ON ENTERPRISE SECURITY AND INFORMATION TECHNOLOGY OPERATIONS OF DEPARTMENT OF DEFENSE NETWORKS AND SYSTEMS

Tuesday, March 24, 2026

Washington, D.C.

ALDERSON COURT REPORTING
1029 VERMONT AVE, NW
10TH FLOOR
WASHINGTON, DC 20005
(202) 289-2260

TO RECEIVE TESTIMONY ON ENTERPRISE SECURITY AND INFORMATION TECHNOLOGY OPERATIONS OF DEPARTMENT OF DEFENSE NETWORKS AND SYSTEMS

Tuesday, March 24, 2026

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

The committee met, pursuant to notice, at 2:30 p.m. in Room SR-232A, Russell Senate Office Building, Hon. Mike Rounds, chairman of the subcommittee, presiding.

Committee Members Present: Senators Rounds [presiding], Rosen, and Reed.

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

Senator Rounds: Good afternoon, and welcome to this afternoon's Cybersecurity Subcommittee hearing on enterprise security and information technology operations of Department of Defense Networks and Systems. I want to begin by thanking our witnesses for appearing today before this subcommittee. Your testimony arrives at an inflection point for how the Department of Defense fights, decides, and wins.

This hearing is fundamentally about warfighting. The digital backbone of the Department of Defense is no longer a support function. It is a weapon system. Our tanks, ships, aircraft, and ground forces depend on connected, resilient, and secure networks to operate at the speed and precision across vast distances. Sensors all over the world will connect to shooters across the theater in a vast kill web that must operate faster and more efficiently than our enemies' systems. This is especially true for future conflicts, as we continue fielding software intensive systems designed for decision advantage and speed of action.

While quantity may have a quality all of its own, the ability to optimize our targeting and orient, decide and act more quickly than the enemy will likely decide the outcome of the next major war. The Department's cultural shifts

towards recognizing networks and information technology infrastructure as a warfighting platform is one I agree with.

Yet, I realize there is still a long way to go. Software can be developed and deployed in minutes, hours, or days. The bureaucratic processes governing how we acquire, certify and field it does not match that timeline, at least not yet. This reality is no longer merely an inconvenience. It is a strategic liability. We have talked long enough about solving these problems. This subcommittee wants to see them resolved.

Compounding the urgency is the condition of the infrastructure itself. Defense information technology budgets have long served as the bill payer absorbing cuts to fund near-term priorities. The result is a technical debt problem of historic proportions in both hardware and software. Our adversaries are not blind to this. Not surprisingly, they are taking advantage of this blunder. Every day we delay modernizing is a day we strengthen their hand in the cyber domain.

As we modernize, speed without security is not an improvement. We must be disciplined about not punting today's problems to the future. That means patching what we have while building with foundational security baked in.

This cannot be a government-only endeavor. The private sector can move with speed and provide capabilities the Department cannot match. But partnership only works when our processes and requirements are transparent and consistent. We owe our industry partners clarity and we owe our warfighters results. We must ask what kind of compute capacity, network resiliency, and data infrastructure our warfighters require, not just today, but as artificial intelligence is deployed at a scale across the force. If we cannot answer that question with specificity, we cannot build toward it.

Today, this subcommittee looks forward to hearing from both of you on where the Department stands in addressing these efforts. We want to understand how bureaucratic barriers are being dismantled, and how our processes are being made more welcoming to industry partners. It is especially important for us to hear whether our networks have the capacity, resilience, and performance our military requires for modern warfare against a capable adversary.

Thank you again, and now I would like to recognize the ranking member for her remarks. Senator Rosen.

STATEMENT OF HON. JACKY ROSEN, U.S. SENATOR FROM NEVADA

Senator Rosen: Well, thank you, Chairman Rounds. Ms. Davies, General Stanton, appreciate you being here. I want to welcome you, and Ms. Davies, congratulations on your recent confirmation and assumption of duties. And so, Ms. Davies, as you get settled into this position, we'd like to hear more about your priorities, get some of the ideas of where you're going to be placing emphasis on funding from fiscal year 2026 appropriations and any reconciliation funding you may have received as well.

And so, without discussing specifics, it would also be helpful to know where we might see significant budget swings for programs so we're not surprised when the fiscal year 2027 President's budget request is released. That request is already nearly 2 months late. It's not expected for a few more weeks, and that leaves little time in our NDAA process to delve into the details and it's critical for us to be able to do that.

General Stanton, I want to welcome you back. Thank you for your years of service. I hope you will also share your thoughts on all of these topics as they relate to your role as director for the Defense Information Systems Agency and commander for the Department of Defense Cyber Defense

Command. As the organization charged with running DOD networks, you have a unique operational perspective on how policy decisions from the Department CIO are translated, well, into action, but that also means that you have a slightly different view as to the resourcing and workforce needs. The implementation of technology for the warfighters different maybe than the development, right? The impact of technical debt on the ability of our department to modernize. You can speak to that in practical sense.

So, we also have a long list of long-term issues we want to make sure the Department is addressing so they don't get lost in the immediate priorities of the day or the specific priorities of this administration. For example, implementation of the cybersecurity maturity model certification process, improving the authority to operate, process for software to be placed on the DOD networks, and addressing the backlog of technical debt in our IT programs to make sure our networks are more modern, more resilient, and of course, more secure.

These are just a few of the areas where I think we have common cause and desire to work together to improve the Department for the long term. We want to work collaboratively with you on these issues. However, the Department has not been particularly timely or forthcoming

on information. So, for us to conduct our statutory obligation to oversee the Department of Defense, requires us to have open and honest conversations. There's definitely a trust deficit right now, but I think it's fixable if the Department can be more responsive to the requests of this committee and to our members. So, I hope we can use this hearing, both open and closed, to help us get started on the right foot.

And with that, I'm going to turn it back over to Chairman Rounds. Thank you.

Senator Rounds: Thank you, Senator Rosen. Today, we're pleased to have our two panelists with us, Kirsten Davies, who is the chief information officer at the Department of Defense, and Lieutenant General Paul Stanton, United States Army director, Defense Information Systems Agency commander, the Department of Defense Cyber Defense Command. We welcome both of you here, and we look forward to your opening statements. Your written statements will be a part of the record, but we would welcome your opening statements.

And with this, Ms. Davies, would you like to begin?

STATEMENT OF HONORABLE KIRSTEN A. DAVIES, CHIEF INFORMATION OFFICER, DEPARTMENT OF DEFENSE

Ms. Davies: Thank you. Good afternoon, Chairman, Ranking Member, Senator Reed, thank you for the opportunity to speak with you today about the Department's strategy to transform technology and cybersecurity into a decisive warfighting advantage.

Our focus is to enable data supremacy and decision dominance on the contested battlefields of today and tomorrow at the speed and scale our warfighters deserve. In the latest initiative in Secretary Hegseth's drive for efficiency and effectiveness, we are undertaking a bold transformation of enterprise IT and cybersecurity program, unifying these capabilities under the Department's Chief Information Officer. Through this effort, we will eliminate inefficient spending, reduce technical debt, accelerate modernization, drive consistent and up leveled cybersecurity, and unleash data and innovation from the core to the edge across our joint forces.

Leveraging my oversight of DISA, the NSA's Cybersecurity Directorate, and the Department's Cyber Crime Center, we are working with the military services, joint staff, combatant commands, and defense agencies across four transformation pillars. I'll provide a few highlights here.

Under pillar 1, the Enduring Digital Foundation, we're transforming our network infrastructure and communications transport, which extend from undersea cables to terrestrial fiber to advanced satellite capabilities, connecting everything from the home front to the tactical edge. This foundation supports every warfighting system and our global installations. We're driving continual modernization, expansion, and hardening, as well as broad 5G usage and data center modernization. We're evolving our cloud strategy in JWCC Next, and we're also leading a proactive approach to spectrum management and advancing PNT efforts, ensuring ready and resilient capabilities that enable American warfighting dominance.

Under pillar 2, agile digital capabilities, reflecting some of your comments, Senator Rounds, we are expanding our and maturing digital offerings. We're accelerating delivery of software and SaaS services, and standardizing data architectures, streamlining our data flows. We're shifting from slow legacy software development to modern agile delivery, driving interoperability by design, and delivering applications and analytics at the speed of relevance. We're driving extensive defense business systems work, whether modernizing or sunsetting those systems to enable clean audits and reduce wasteful spends. We're also deploying

mission partner environment as persistent, secure environments where trusted partners can be rapidly integrated.

Under pillar 3, cybersecurity for the warfighting ecosystem, in alignment with President Trump's National Security Strategy and the National Defense Strategy, we're moving from checklist-driven compliance towards unified, holistic, risk-based approach. We will emphasize automation and dynamic and continuous monitoring.

We will drive risk reduction rather than burdensome paperwork, focusing on anti-fragility and resilience through a holistic blend of streamlined processes, advanced technologies, and skilled people. We're refining the authority to operate, process, and accelerating our deployment of Zero Trust principles. We're also refining our risk management process and reigniting the debate to align with the Secretary's arsenal of freedom initiatives.

Finally, through pillar 4, skills and partnerships, we recognize that people are our decisive edge. As part of our transformation, we're reviewing IT and cybersecurity roles to ensure clear responsibilities, accountability for outcomes, and a bias for action. We're leveraging your provisions in the fiscal year 2026 NDAA to enhance recruitment and retention of cyber professionals and expand

competitive compensation.

We will be launching an expanded top tier certification program in partnership with industry and academia, which will offer upskilling and reskilling to our warfighters, from new recruits to seasoned service members. And because we do not fight alone, we're doubling down to influence the digital transformation efforts of our allies and partners, which will better enable all of coalition force readiness.

As we advance this bold strategy, thank you for your continued interest in and support of IT and cyber security, and for the resources you provide to protect national security. The race for data superiority and decision dominance is won or lost every day, and this strategy is a key part of how we, together, ensure the technology race is won by the United States. Together, we will ensure the resilience, readiness, and lethality of America's warfighters across every domain.

I look forward to your questions.

[The prepared statement of Ms. Davies follows:]

Senator Rounds: Thank you, Ms. Davies. Lieutenant General Stanton.

STATEMENT OF LIEUTENANT GENERAL PAUL T. STANTON, USA, DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY/ COMMANDER, DEPARTMENT OF DEFENSE CYBER DEFENSE COMMAND

General Stanton: Chairman, Ranking Member Rosen, Senator Reed, thank you for the privilege of appearing before you today to explain the fundamental shift we are making to ensure that our weapons system, the Department of War Information Network, provides our warfighters with decision advantage. I'm honored to represent the highly skilled and dedicated professionals of the Department of War, Cyber Defense Command, and the Defense Information Systems Agency that design, build, secure, operate, and defend our environment.

We must deliver a secure, standardized, resilient, and efficient architecture that supports combatant commands. Combatant commands execute warfighting. Nested within the Department of War CIO's vision, the Defense Information Systems Agency has a responsibility to provide functionally relevant capability that aligns with the time and tempo of the warfighter's mission. As the Department of War Cyber Defense Command, we have an added responsibility to ensure that our systems and data are properly defended against continuous and sophisticated attacks.

Combining these two responsibilities, and said simply,

we must get the right data to the right place at the right time, such that our commanders make better and faster decisions than our enemies. We are a sub unified command and a Department of War Combat Support Agency. Our mission, and therefore our culture is to support warfighting. We are fully engaged to move and maneuver the network and our data according to the changing conditions of the operating environment. We design, build, secure, operate, and defend in lockstep with commanders at echelon. We campaign to execute our missions and defeat our adversaries. We present and defend the architecture so that commanders can fight. We are doing so right now in Operation Epic Fury.

But we cannot rest. We must transform ourselves and the means by which we support to leverage the most modern and effective technology. We are in a perpetual state of continuous modernization; new solutions, artificial intelligence, commercial SATCOM, mobile data centers. They emerge at industry's pace, and we must integrate them into our architecture and missions at speed.

Further, we must be prepared to fight alongside our partners, sharing data across warfighting functions within decision cycles. The coalition information environment, as recently prototyped during an exercise in the Indo-Pacific theater, is a cornerstone of our approach. We know that our

adversaries, our enemies, are watching us and will certainly attempt to delay or degrade our decisions, and we will defeat them.

We are developing solutions that are secure by design, incorporating perimeter defenses that defeat known attack vectors and employing Zero Trust to detect, bound, and defeat new and novel tradecraft. Our internet access point and our cloud-based internet isolation warfighting systems continuously adapt to new threats at our boundary. Our Thunderdome implementation of Zero Trust is proven, expanding rapidly as we transition defense agencies and field activities into DODNet. We will use these tools and the associated data in an informed, productive, efficient, and speedy manner, automating our defenses and employing human tradecraft for advanced analysis.

We prioritize our defenses on what matters. In order to preserve decision space for commanders, we must defend the critical systems upon which they are dependent. Our approach employs a mission thread defense that we nest and plan amongst commanders and their staffs for synchronization. We align our cyber defenses to how their systems employ and move data, ensuring that they have confidence in the data upon which they make their decisions. Our defenses and our strategic goals require optimization.

We have to see ourselves holistically. We have made and continue to make significant progress in sensing, logging, aggregating, and analyzing our data accordingly. Our data analytics support cell is employing our common data analytics platform to continuously run queries and analytics that optimize performance and support defensive operations. CDAO feeds into USCYBERCOM's joint cyber warfighting architecture for enrichment with classified intelligence, and coordination with offensive cyber forces for speed and lethality.

Our success is the innovation, talent, and motivation of our workforce. Readiness is a requirement. A trained and ready force has confidence to act with disciplined initiative. Demonstrated confidence leads to trust to make decisions at speed. When we combine our transformational architecture with a talented and trained workforce, we are postured to meet our requirements. This is an imperative. The effectiveness of the DoWIN is inextricably linked to our missions and our Nation's defense. With the continued support of the committee, we will preserve the decisive advantage.

We look forward to your questions. Thank you.

[The prepared statement of General Stanton follows:]

Senator Rounds: Thank you, General Stanton.

Normally, we would begin with 5-minute rounds, and I would start, Senator Rosen, the ranking member, would be second, and then we'd move back and forth. But we also have the ranking member here. And if you would like to --

Senator Reed: No sir. Regular order --

Senator Rounds: Okay. Regular order it is.

Senator Rosen: You heard it from the Ranking Member.

Senator Rounds: Very good. Well, then I will begin. Ms. Davies and General Stanton, the ability of our warfighters to operate in a contested or a degraded environment is directly tied to how resilient and modern those networks are. Where does the Department stand on network modernization, and are our warfighters confident they can operate if those networks are attacked or denied? Ms. Davies.

Ms. Davies: Thank you, Senator Brown, for that great question. I'll allow General Stanton to get into a few of the details. But as I reflected on pillar 1 of our transformation strategy, this is active work that we are doing right now that DISA has been conducting for quite some time under General Stanton's leadership and previous leadership as well. This is a key area of focus for us.

Our forces are globally located. Our joint forces are

globally located. We are currently, obviously, in a mission right now with partner forces as well. And the resiliency and the efficacy of the traffic of our network is quite critical to that. It's a key focus area for us, Senator.

Senator Rounds: General Stanton.

General Stanton: Senator, thank you for the question. And with great support from Congress, we have an initiative that we reference as design, security, and resiliency. So, the Defense Information System Network, where we focus on undersea cables, increased bandwidth for terrestrial fiber, multimodal satellite communications capabilities we refer to as an agnostic peering gateway that allows us to communicate over military SATCOM waveforms, but also via commercial SATCOM capabilities.

As our forces move into theater, as they currently reside in theater, we have a primary alternate contingency and emergency plans put into place. We're never single threaded on any capability as we enter into the fight such that if we suffer degradation, we have fallback capabilities. We're seeing that in spades currently, operating across terrestrial space based and undersea capabilities.

Senator Rounds: So, recognizing that we're in an unclassed environment, we'll go into a classified

environment when this when this meeting is done, specifically, I think what you're indicating is there's a couple of different areas where we may have, some challenging communications problems. You mentioned, undersea cables, you mentioned space-based assets and so forth. Are those perhaps the most challenging that we're going to face that we can talk about in this environment today?

General Stanton: Well, Senator, I think it's the combination and the fact that as our warfighting formations are outfitted with capability. We never isolate down to a single mode of transport. We ensure that we have the ability to route terrestrially. We hit two peering points such that we can leverage undersea cables. We're never bounded by a single undersea cable. We always have a plan to route around or have an alternate path.

And then, the proliferation of space-based assets, specifically in the commercial world, is really game changing technology to give us leap over capability if and when we do suffer a degradation.

Senator Rounds: It's an interesting lead in on it. Then for us to talk a little bit about the reason why we no longer talk about a kill chain. We talk about a kill web, and that is because we have multiple avenues to move from a

spotting system back into where you actually have the ability to trigger a weapon. So, multiple ways to get the communications from point A to point B, not simply one line. Fair way of looking at it?

General Stanton: Precisely. Yes, sir.

Senator Rounds: Ms. Davies, many smaller Defense Industrial Base companies lack the internal security capability to defend themselves against a sophisticated state actor. What is the Department doing to reach that tier of the industrial base, and is voluntary participation in government support programs getting us there?

Ms. Davies: Senator Rounds, this is a key focus area for me as well. I think we have focused largely on confidentiality of data in the past. I know that there has been some burdensome requirements that have been placed on large and small businesses alike. In the new transformation, one of our key pillars is going to be working directly with the Defense Industrial Base. Their resiliency is our resiliency. Their security is our security.

But it needs to make sense. We've heard Secretary Hegseth talk about reducing the burdens to entrance, allowing entrance, new entrance for smaller companies as well. This is a key focus area for us, whether it's

providing guidance, providing principles for them to follow. It's coming alongside them and partnering them, but it's also tailoring these requirements so that they are effective for the arsenal of freedom that we are driving.

Senator Rounds: Thank you. My time has expired. Ranking Member Rosen.

Senator Rosen: Thank you, Chairman Rounds. I'm going to just say something and I'll ask for more details in the classified briefing. Just building on what Senator Rounds said, I want to hear a little bit about the lessons you learned from the recent military operations in Venezuela and Iran that relate to the DOD networks in terms of showing us a little bit of stress testing in the real world, right? We're in conflicts in both places, and what we've learned about what we might be changing for future protracted conflicts. So, we'll save that one. Just put that out there.

General Stanton, I want to talk a little bit about IT support during a war. So, the Defense Information Systems Agency, you're a combat support agency for the Department of Defense. So, I'm hoping that you can explain for all of us what that means, practically. Given our current posture in the Middle East, what does your agency do during war time that could be different than what it does during peace time,

if you could elaborate on that?

General Stanton: Yes, ma'am. Absolutely. Thank you for the question. So, we are at war, and we're executing Operation Epic Fury currently. Which means that every day inside of our operations center, the Defense Information Systems Agency, and Cyber Defense Command, get together to ascertain what has transpired in the context of the network, what assets are still up and running, what assets need to be resolved? How do we route around problems? How do we dynamically solve problems with emergent technology and do so rapidly.

From a DISA perspective, a lot has to do with network transport. And so, it -- where are the terminals located? How do we get them to the right spot? Do we need to lease a new circuit on the fly in order to ensure that critical data gets from point A to point B? These problems present themselves in real time, and inside of our ops center we are dynamically solving and developing resolution.

Senator Rosen: Thank you. I'm going to move on to you, Ms. Davies, because we want to talk a little bit about the Joint Warfighting Cloud Contract. And the Joint Warfighting -- it's a mouthful. The Joint Warfighting Cloud Contract -- do not try to say that quickly -- we'll just say the JWCC, it's a little bit easier, is reaching a point soon

where it's going to be need to be recommitted, and there'll be a need to be a replacement contract. And so, what lessons has DOD learned from the JWCC that we might see next in an updated JWCC, and how do you see AI impacting your decisions?

Ms. Davies: Thank you for the question. It is a mouthful, isn't it?

Senator Rosen: It is, it is, yes.

Ms. Davies: We are expanding JWCC into a unified cloud marketplace, integrating additional providers, embedding financial operations, automation, and multi-cloud management to enable enterprise-wide cost control and interoperability. I can speak from being new in the role and seeing that there are contracts everywhere, and different points of authorization with different cloud that's happening.

One of the key areas that we need to be looking at from a multi-pronged approach is, is this the most efficient way to be driving cloud compute? It's not. We need to be continuing on in the JWCC Next. Is it the most -- is it the best way to see the spend. It is not. So, JWCC Next is going to provide us that financial transparency that's there, and it's also going to provide General Stanton and his team the ability to do better defense across all this, because we're going to know where all of the cloud compute

is, and that's key for us in asset identification and asset security.

Senator Rosen: Thank you.

And then I'm going to continue with you, Ms. Davies, because I want to talk about the enterprise chief information officer collaboration. Right? So, DOD, you're like -- you're saying you're just a vast conglomeration of networks, clouds, operating cultures, systems, you name it. It's difficult to craft a one-size-fits-all policy, although you can set standards, and you can at least lay out the templates for it. You can map out where everything is, essentially, but in my view, there are benefits to having each of the military departments and defense agencies having their own CIOs so that they can tailor technology and policies to the needs of the various organizations.

So, could you describe for us your relationship with your CIO counterparts in the military services and defense agencies, and are there any lessons, helpful or otherwise, you might have picked up in your time so far?

Ms. Davies: Some great lessons indeed. I'm holding regular meetings with my military department counterparts as well as the DAFA counterparts. I'm learning where the operational efficiencies are, where the centers of excellence and expertise are, also where the gaps are. So,

I think there's varying levels of competencies, varying levels of operational cadence that are there. And one of the things that we will be getting after with this new strategy is to take a hold of those rising tides, raise all ships to make sure that we're all pointing in the same direction and focused on operational excellence in cyber defense.

Senator Rosen: I yield.

Senator Rounds: Senator Reed.

Senator Reed: Well, thank you, Mr. Chairman, Madam Ranking Member. I thank the witnesses not only for being here today, but for your dedication to our warfighters. Thank you.

Ms. Davis, I'm sure you're aware of the recent decision by the secretary to designate Anthropic as a supply chain risk. Indeed, you, yourself, signed out a memo on March 6 directing the removal of Anthropic from DOD systems within 180 days. However, the committee still has not heard the rationale from the Department about why the designation was made, nor received a full notification, which is required under law by Section 3252 of Title 10.

And this notification requires a summary of the risk assessment and a summary of the basis for the determination, including what less intrusive measures were considered, and

why they were not reasonably available to reduce supply chain risk. We have not received that information, yet, it is required under the law. So, first, are you aware of the actual reason in designating Anthropic a supply chain risk?

Ms. Davies: Senator, thank you for the question. I was involved, as many of my counterparts were, in this collaborative decision-making process that followed the regulatory requirements.

Senator Reed: Well, why was it done?

Ms. Davies: Sir, we're in active litigation right now, so I won't go into the details of it. We have reached out and offered a briefing for your offices into the depths of it. I will say that there are some -- the filing in the California court is available. We have made that available, but it was only available to us this morning. So, we did provide that over with the risk analysis. That was a part of it.

Senator Reed: It's just interesting that you would file required documentation for the California court before complying with the law, and filing it, and sending it to us. I don't believe it's been sent to us officially or unofficially. Why haven't you, the Department, complied with the law.

Ms. Davies: Senator, I'm aware that the -- our

colleagues in Legislative Affairs have followed the regulation of what they were in -- what they were supposed to provide. I do know that we followed all of the steps of the regulatory requirement of the Title 10, 3252.

Senator Reed: Well, I don't think we've received it. We have not received it.

Senator Rounds: Just in checking with staff, I do not believe that we have received it at this time.

Senator Reed: Thank you, Mr. Chairman.

But as you pointed out, a California court has received it because of the litigation. Let me just -- one additional question is, are you aware of any estimates that were made as to the potential cost impact on DOD uses for removing and replacing Anthropic from DOD systems, or the cost to replace Anthropic with another large language model.

Ms. Davies: Senator, I'm aware of the risk analysis that was conducted as a part of that, and I'm aware that we have also constructed our data architectures to be able to be interoperable with a variety of different AI capabilities. And so, the deep assessment of replacement of that, I'm unfamiliar with right here, I can take that away as an action for you.

[The information referred to follows:]

[SUBCOMMITTEE INSERT]

Senator Reed: It would be appreciated because the idea of the scale and the magnitude of the disruption would be helpful. Further, it's my understanding that Anthropic's Claude system is being used today in Iran in our military operations. Is that true?

Ms. Davies: Without going into the details in this forum, Senator, the use of the system is active right now. This is also why we provided for a measure of time we felt was reasonable, as well as an exception process for removal of the Anthropic systems.

Senator Reed: It just seems odd that you would continue to use a system which you determined to be a supply chain risk. Does that strike you as odd?

Ms. Davies: Senator, at no time, in any way, will we interfere with the success, the lethality, and the resilience of our warfighters. And for that reason, we've provided what we feel is a reasonable amount of time for those systems to be replaced. We can -- I can also say that according to -- you know, with President Trump's great leadership, we have a number of technology companies that have come to the table wanting to do business with us as the Department of War and across the U.S Government. So, we know that we've architected this appropriately in order to use competitive advantage as well.

Senator Reed: Thank you very much, Ms. Davis. General, thank you.

General Stanton: Sure.

Senator Rounds: Thank you, Senator Reed.

Let me just follow-up on that for just briefly here. My understanding is that there has been a 180-day notification with regard to Anthropic. I presume, and you can correct me if I'm wrong, but I presume that there is additional time frame here in which there is the possibility of additional negotiations that can occur during that time period, recognizing just what a significant change this would be to the Department with the reliance right now on the Anthropic product at this time. Fair enough to say?

Ms. Davies: I'm not sure what part of the question to answer for, Senator Rounds. Let me let me try to unpack that for you. We have architected our data insomuch as we can deploy multiple types of AI across our data. That's something that the -- General Stanton and the DISA colleagues have been very careful about. Number one.

Number two, we have provided what we feel is an appropriate amount of time to remove the Anthropic systems in accordance with the designation by the secretary of the supply chain risk designation in and of itself. Does that answer your question?

Senator Rounds: Yeah. Except that I think the other entities that we are looking at, many of them have also indicated that they have Anthropic within their systems as well. And what I'm looking for is, is the possibility that as this discussion goes on in a business-like manner, I'm assuming it will be done in a business-like manner, that there are opportunities for additional negotiations to continue to occur?

Ms. Davies: Senator, I will defer that to my colleagues in the legal department who are undergoing that active litigation right now, and we will certainly bring a report back to you.

Senator Rounds: That's fair. And I do think it'd be fair to say that I think the committee as a whole, and I can't speak for the chairman, but at least with regard to the subcommittee, this is something that we have a real interest in, and we will want to get in a classified setting probably deeper into the details at some point when you're prepared to share that with us -- with the appropriate personnel.

Ms. Davies: Senator, we'll take that for action, absolutely. Thank you.

Senator Rounds: Thank you.

Let me go on a little bit here. I'm just curious,

General Stanton, one item that we've talked about is deterrence. And as we will use our offensive capabilities, one of the reasons why you use offensive capabilities is to deter future attacks, and to let people know that you know who they are, we know where they are, and we do have access to some very exquisite capabilities to stop them from actually using kinetic activities or kinetic systems.

Can you talk a little bit, in this open session, just so that the American public will understand, just kind of some of the things that we have the ability to do now that we've actually utilized some of them, and are -- the bad guys know that what we can do? Can you talk just briefly about that, just to share with the American public what their taxpayer dollars are buying?

General Stanton: Yes, Senator. And I look forward to having a more robust conversation in a classified setting.

Senator Rounds: I understand, but the public can't see that. And like I said, I don't want to do any damage to our ability to do it in the future. But I think it's fair for deterrence's sake, to maybe talk a little bit about what our capabilities are, if that is acceptable.

General Stanton: Yes, Senator. So, I think I'll address it in two principal ways. The first is there's a deterrent effect associated with cost imposition. If you

make it really hard for the enemy to attempt to achieve the effects that the enemy intends, then it is a cost imposition. The enemy has to spend more money, more time, develop more resources, and apply it in ways that that the enemy may not have been prepared. That's a cost imposition.

In addition, we have offensive cyber capabilities. And we have offensive cyber capabilities that can, respond at speed to evidence of adversarial activity beyond the bounds of our U.S. networks. So, when we see operations in foreign space as actioned by our cyberspace foreign adversaries, we have the capabilities to deny them those resources.

Senator Rounds: Fair to say we can deny them the ability to communicate in some cases?

General Stanton: Yes, Senator.

Senator Rounds: Fair to say that we can sometimes make it so they can't see what they want to see on their systems --

General Stanton: Yes, Senator.

Senator Rounds: -- to know what's going on in their in their part of the world? Fair to say that we can make them see things that maybe aren't even there today.

General Stanton: So, the ability to deny access to systems, the ability to manipulate data to get inside the decision cycle of the adversary, are all the art of the

possible in techniques developed in support of offensive cyber operations.

Senator Rounds: All of which means that our young men and women are then safer when they go in harm's way, because we limit the adversary's ability to respond to our young men and women who are on the battle front?

General Stanton: Unequivocally --

Senator Rounds: Thank you.

General Stanton: Unequivocally -- yes, Senator.

Senator Rounds: Thank you. Ranking Member Rosen.

Senator Rosen: Thank you.

I want to in the classified, I'm going to ask a little bit more about how you've architected -- it's a new verb, architected -- your data to feed into many different, I would assume, large language models or the like. I think that it's very interesting to me.

But for this open session, I want to talk about the authority to operate process, because I'm encouraged by the Department's continued support for improving cybersecurity and supply chain risk management, of course, and you've made progress towards reforming and accelerating acquisition, testing, authorization of commercial software. But more, of course, can always be done to streamline the authority to operate, ATO, our single process into a single department-

wide accreditation for secure software providers, streamlining the process.

So, can you talk about the status of your efforts to streamline that process, of what actions you're taking, and what plans your office may have to establish and encourage reciprocity for ATOs between individual service branches and department components. So, pulling all that back up to the center.

Ms. Davies: Ranking Member, a great question. The ATO process is part of the broader risk management framework, as you are very familiar with. Right now, we have a very static snapshot in time with regards to risk management, and that needs to be moved to a much more dynamic framework and process, which includes inheritance of assessments that are conducted somewhere else across the Department on a piece of software. That inheritance can then travel to a new department that wants to leverage that piece of software, that inheritance of all the testing and the scalability and all of those types of things.

The ATO process as a piece of that also needs a reform. We're finding that it's very difficult for people to actually grab that inheritance over. It's very difficult to understand the work of that risk management framework because it's broken, it's fragmented, and it's static. So,

what we're doing is we're looking to do a lot more automation across this, having dynamic repositories of this information, and the testing in and of itself.

This work of the RMF framework, as well as the ATO processes, will be sitting underneath the Department's chief information security officer, who was presidentially appointed just a few weeks ago. But he's right on top of it and going to be working very actively with me to make sure that we're reforming that appropriate to the risk of the actual work that needs to be done.

Senator Rosen: Well, I understand what you're saying; how important it is to be more dynamic, and sometimes less static, but I'm also well aware of the vulnerabilities at places when you are quickly dynamic without the proper audits and controls over that as well because you never want to sacrifice speed. And I'm not saying static is always the way to go, but you have to be very careful about that dynamic architecture as well because it can create vulnerabilities, because moving at the speed of light, or sound, or nano second, whatever you want, is -- has risk in there as well. So, I hope that you're building in a good audit process review of how that's working, so in that speed --

Ms. Davies: Yes --

Senator Rosen: -- we will get to that.

Ms. Davies: -- and we're -- it's a great point. We're going to be bringing in a lot of industry-good practices across this as well, where we've learned to do a lot of the automation of processes, less paperwork, more dynamic checking across the software design lifecycle. We can do a lot of code scanning, code reviews. Those are the types of automation that will help us speed these things up while we're compiling appropriate data repositories for that constant risk checking.

Senator Rosen: Right. Because if you do it too fast, once a piece of bad code gets in, it's already replicated quickly across your system before you may have caught the bug, so.

Ms. Davies: That's right. You understand the risk process very much.

Senator Rosen: Yes, I think I do, but thank you.

I'm going to talk a little bit in my -- I just asked you a question about artificial intelligence, the validity. We talked about Anthropic. I know we're going to go talk some more about this, the validity of their output critical to the effectiveness of what we do. As we acquire and deploy more systems, artificial intelligence systems, warfighting -- you said we're in a war -- but it's going to

help our situational awareness, our decision-making, and we must secure these systems and the data that powers them. The data.

That's why I want to talk about how you architect your data. Data is power if you're smart enough to analyze it and use it. It's all about how you use it. The data is key, and so it's important and critical to maintain the trustworthiness, the integrity of all of that. Avoid any corruption, malicious manipulation. And so, how are you kind of -- as much as you can say here, what are you doing to ensure that you're leveraging existing commercial solutions, without making us vulnerable.

Ms. Davies: Yeah. Thank you, Ranking Member. In July of 2025, my office published the DOW AI-Cybersecurity Risk Management Tailoring Handbook. So, we provided some great guidance across that. This is an ever-evolving framework or competency, I would say. We've been tackling this in the industry across the last, I'd say, 5 to 7 years, providing appropriate guardrails, ethics, security across this, looking at the weights of models, as well as hallucinations, to try to reduce all of these factors that are there. We're going to be continually evaluating this as we go through.

We have provided strong guardrails. We're doing risk management assessing on a regular basis across this. And

so, this -- we will continue to have conversations around this because it is an evolving category of software, if we want to call it that.

Senator Rosen: Thank you.

Senator Rounds: I think at this time, we will conclude the open portion of today's Cybersecurity Subcommittee hearing, and as all of you know, we'll be reconvening here in a few minutes. We've got a vote at 3:15 that's scheduled. Matter of fact, three of them, but it'll give us an opportunity to make our first vote.

We'd like to reconvene at 3:30 down in 217, in the SCIF, for a classified portion of this. And then, for the information of members who will not be joining us for the closed briefing, questions for the record will be due to the committee within 2 business days of the conclusion of the hearing.

[The information referred to follows:]

[SUBCOMMITTEE INSERT]

Senator Rounds: And with that, I want to thank you for this open session. We look forward to visiting with you again very shortly, beginning at 3:30 in the closed session in the SCIF.

And with that, the subcommittee meeting is adjourned.

[Whereupon, at 3:16 p.m., the hearing was adjourned.]