S. HRG. 119–495

ENTERPRISE SECURITY AND INFORMATION TECHNOLOGY OPERATIONS OF DEPARTMENT OF DEFENSE NETWORKS AND SYSTEMS

HEARING

BEFORE THE

SUBCOMMITTEE ON
CYBERSECURITY

OF THE

COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

ONE HUNDRED NINETEENTH CONGRESS

SECOND SESSION

MARCH 24, 2026

Printed for the use of the Committee on Armed Services

Available via: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
64–328 PDF WASHINGTON : 2026

COMMITTEE ON ARMED SERVICES

ROGER F. WICKER, Mississippi, *Chairman*

DEB FISCHER, Nebraska	JACK REED, Rhode Island
TOM COTTON, Arkansas	JEANNE SHAHEEN, New Hampshire
MIKE ROUNDS, South Dakota	KIRSTEN E. GILLIBRAND, New York
JONI K. ERNST, Iowa	RICHARD BLUMENTHAL, Connecticut
DAN SULLIVAN, Alaska	MAZIE K. HIRONO, Hawaii
KEVIN CRAMER, North Dakota	TIM KAINE, Virginia
RICK SCOTT, Florida	ANGUS S. KING, Jr., Maine
TOMMY TUBERVILLE, Alabama	ELIZABETH WARREN, Massachusetts
MARKWAYNE MULLIN, Oklahoma	GARY C. PETERS, Michigan
TED BUDD, North Carolina	TAMMY DUCKWORTH, Illinois
ERIC SCHMITT, Missouri	JACKY ROSEN, Nevada
JIM BANKS, Indiana	MARK KELLY, Arizona
TIM SHEEHY, Montana	ELISSA SLOTKIN, Michigan

RICK BERGER, *Staff Director*
ELIZABETH L. KING, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY

MIKE ROUNDS, South Dakota, *Chairman*

TOM COTTON, Arkansas	JACKY ROSEN, Nevada
JONI K. ERNST, Iowa	KIRSTEN E. GILLIBRAND, New York
TED BUDD, North Carolina	GARY C. PETERS, Michigan
ERIC SCHMITT, Missouri	ELISSA SLOTKIN, Michigan

CONTENTS

MARCH 24, 2026

ENTERPRISE SECURITY AND INFORMATION TECHNOLOGY OPERATIONS OF DEPARTMENT OF DEFENSE NETWORKS AND SYSTEMS

TUESDAY, MARCH 24, 2026

UNITED STATES SENATE,
SUBCOMMITTEE ON CYBERSECURITY,
COMMITTEE ON ARMED SERVICES,
Washington, DC.

The Committee met, pursuant to notice, at 2:30 p.m. in room SR–232A, Russell Senate Office Building, Senator Mike Rounds (Chairman of the Subcommittee) presiding.

Committee Members Present: Senators Rounds, Rosen, and Reed.

OPENING STATEMENT OF SENATOR MIKE ROUNDS

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 toward 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 SENATOR JACKY ROSEN

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. 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.

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 National Defense Authorization Act (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 Depart-

ment of Defense Cyber Defense Command. As the organization charged with running Department of Defense (DOD) networks, you have a unique operational perspective on how policy decisions from the Department Chief Information Officer (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 Information Technology (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.

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.

With this, Ms. Davies, would you like to begin?

STATEMENT OF THE 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 Defense Information Systems Agency (DISA), the National Security Agency's (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 5th Generation usage and data center modernization. We're evolving our cloud strategy in Joint Warfighting Cloud Capability (JWCC) Next, and we're also leading a proactive approach to spectrum management and advancing Positioning, Navigation, and Timing (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 toward 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 en-

hance 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. 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:]

PREPARED STATEMENT BY THE HONORABLE KIRSTEN A. DAVIES

INTRODUCTION

Chairman, Ranking Member, and Distinguished Members of the Subcommittee, thank you for the opportunity to testify on our unified effort to transform the Department's technology ecosystem and Cybersecurity Program to deliver capabilities for the readiness, resilience, and lethality of our warfighters. Our primary goal is to enable data supremacy and decision dominance on the contested battlefields of today and tomorrow. To achieve this, great change is needed.

We are embarking on a bold transformation. Our strategy is anchored in bringing back to the center all of Enterprise IT and the Cybersecurity Program, in accordance with the authorities given by Congress to me as the Department's Chief Information Officer (CIO). This consolidation will fuel our transformation, eliminating duplicative spending, reducing technical debt, accelerating modernization, driving consistent and upleveled cybersecurity, and unleashing innovation from the core to the edge across our joint forces. Through our transformation, we will overhaul the IT and Cybersecurity operating model. We will revamp how we architect our networks, re-shape our engagements across our ecosystem, reform how we design and deliver capabilities, and unleash the power of our data. These transformative changes will drive efficiency and effectiveness, reduce cyber and operational risk, and ensure we can best leverage commercial technologies and industry best practices. We will empower our forces to move with speed and surety at the edge, while we drive resilience, security, and optimization at the core.

Leveraging my oversight of the Defense Information Systems Agency (DISA), the National Security Agency's (NSA) Cyber Security Directorate (CSD), and the Department's Cyber Crime Center (DC3), we will work in lockstep with the Military Services, Joint Staff, Combatant Commands and the Defense Agencies and Field Activities (DAFAs) to achieve this transformation across four main pillars of activity:

PILLAR I: THE ENDURING DIGITAL FOUNDATION

Our vast network infrastructure and communications transport extend from undersea cables to terrestrial fiber to advanced satellite capabilities, connecting everything from the homefront to the tactical edge. This foundation is designed to support every warfighting system, including the Operational Technology (OT) and Internet of Things (IoT) devices integral to our warfighting capabilities, connected warfighters, and global installations. Our strategy incorporates continual expansion, modernization, hardening, and resiliency across our network infrastructure, including expansive 5G usage. We are also pursuing extensive data center modernization and consolidation, leveraging our partnerships with commercial Cloud Service Providers (CSPs) to deliver critical route diversity and resiliency.

We are designing and deploying high-availability, low-latency network architectures and robust data and AI infrastructures to power next-generation capabilities

for our warfighters. Undergirding this digital foundation, we are evolving our cloud strategy with JWCC Next, which will provide streamlined access to cloud providers and a catalog of third-party, cloud-based capabilities, enabling Combatant Command timely access to critical data and analytics tools. We are turning vast amounts of information from across the joint forces into a Common Operating Picture (COP) at a pace our previous, hardware-bound data centers and legacy bandwidth network could never achieve.

I would be remiss if I didn't mention spectrum and PNT as part of our extensive foundation. We are driving a proactive and comprehensive approach with regards to the Department's usage of and needs for critical bands of the electromagnetic spectrum which enable our warfighter lethality. We will continue to work in lockstep across this Administration to ensure we together appropriately address and balance the breadth of national security needs, for our warfighters and for our economy. We will continue to also oversee a comprehensive approach across the Department for the resilience and modernization of our Position, Navigation and Timing (PNT), supporting American warfighting dominance.

PILLAR II: AGILE DIGITAL CAPABILITIES

Across this modernized network, we must also expand and mature our digital capabilities, including speeding the delivery of software and SAAS services, standardizing our data architectures, and substantially surging our data flows. Through our transformation, we are shifting from a slow, legacy software and capability development model to a modern, agile delivery that aligns with industry best practices. Driving consistency across software standards will produce interoperability by design, delivering software, applications, and analytics—including for OT/IoT environments—at the speed of relevance. Establishing clear data architecture frameworks will enhance the availability of data, further improving data insights across our ecosystem for every situation. The warfighter requirements are ultimately what we will deliver.

While we drive interoperability of new applications, we will continue to either modernize or sunset legacy applications. We will keep in sharp focus and proactive cadence the addressing of our vast expanse of Defense Business Systems, which will enabling clean audit and reduce duplicate and unnecessary spend.

A key characteristic of our strategy also includes our allies and mission partners. Historically, creating secure connections with allies and partners was a slow, arduous process, often resulting in disparate, clunky networks that impeded data sharing, hindered operational speed, and opened unintended cyber-attack surfaces. We are deploying the Mission Partner Environment (MPE), which fundamentally changes this paradigm. It is designed from the ground up to be a persistent, secure environment where trusted partners can be rapidly integrated, enabling us to share intelligence, logistics data, and a common operational picture in near real-time. By connecting our advanced Joint Operating Environment to the Mission Partner Environment, we enable every capability and data insight to be seamlessly available across the entire coalition force.

Our modern and agile delivery approach means that when a new requirement emerges in a combined operation, we can deliver the necessary software application, analytics tool, and data, not just to our warfighters and commanders, but also to our partners, with security and speed, leveraging an intuitive user experience.

Peace through strength is delivered physically, and digitally. We are delivering that strength across the digital wires.

PILLAR III: CYBERSECURITY OF THE WARFIGHTING ECOSYSTEM

In alignment with President Trump's National Defense Strategy, we are transforming our Cybersecurity Program. Our paradigm will holistically shift by pursuing a unified, holistic, and risk-based approach to cybersecurity. As a part of our bottom-up review of our risk management processes, we've already identified opportunities for improvement. We will deploy a more comprehensive cyber defense posture, moving beyond standard compliance checklists to automating at a greater scale our dynamic, continuous monitoring and uplifting rapid response capabilities. Our improved standards will drive risk reduction rather than paperwork creation, anti-fragility and resilience, rather than "one and done" security, and holistic incorporation of refined processes, advanced technologies, and appropriately skilled people.

To achieve this transformative paradigm, the Office of the DoW CIO will drive harmonization and streamline requirements and policies throughout the Department. We will clarify expectations, refine standards, and propagate standardization of approaches. Risk-based standards and fit for purpose governance are key enablers of our transformation and will be a major focus. From a process perspective, we are

refining our approach to supply chain risk, in alignment with the Secretary's Arsenal of Freedom initiatives. The Department's security posture extends beyond our own networks, we will drive the securing our supply chain. We cannot be secure if our partners are not, and we will treat their cyber defense as integral to our own operational readiness

Sound governance for cybersecurity necessitates clear roles and responsibilities which drive accountability and embed a bias for action. We are currently undertaking a holistic review of all IT and Cybersecurity roles across the ecosystem. As we clarify this critical component of governance, we will ensure empowerment and authority, appropriately refining Authority to Operate process across the Cybersecurity Program.

We will embrace technological advancements and industry best practices to better illuminate our vast ecosystem of digital assets as well as threats at any portion of our environment. We will overhaul our approach to defense, and build protections across the environment to deter and dominate the increasing capabilities of our adversaries. We will drive advanced approaches to Zero Trust principles, including our Identity Management, Authentication, and Access Controls (ICAM), which also underpins interoperability of applications and software. We will implement a more robust threat intelligence process which better informs our defenses and empowers our operators. We must embed Cybersecurity into every layer of technology and every stage of software development across technical ecosystem including critical infrastructure, operational technologies, distributed Cloud services, and networks.

We will next talk about our people and skills. But as a final note on this Pillar 3, we simply need to rationalize and better execute the budget and authorities that Congress has afforded my office. Frankly, the Office of the CIO is currently focused on cybersecurity compliance as an output, and this must be holistically transformed. Compliance is actually a bi-product of a well-constructed program which is effectively executed.

PILLAR IV: UP-SKILLING, CROSS-SKILLING AND PARTNERING

People are our decisive edge in the contested battlefields of today and tomorrow. While we must uplift and modernize our technical capabilities, there is simply no replacing a critically thinking, appropriately trained, decisive operator. America's most precious asset is our people, and as CIO I am doubling down on our approach to skills, training, and readiness.

Thank you for the expanded Cyber Excepted Service provisions in the fiscal year 2026 NDAA. They represent a critical step in addressing the Departments growing need for a highly skilled cyber workforce. This expansion has introduced up to 500 new positions, strategically focused on hard-to-fill, highly skilled roles essential for cyber planning and operations in support of US National Security. We are expanding the CE to enhance the recruitment and retention of elite cyber professionals, broadening eligibility to critical roles within combatant command, defense agencies, and field activities. We are expanding competitive compensation authority, to introduce significant pay flexibility, allowing the Department to offer competitive salaries comparable to other Federal agencies. To ensure we meet our objectives of strengthening US cyber capabilities, we are conducting a 3-year review, detailing the cost-effectiveness and outcomes of this NDAA expansion, focusing on how pay authorities were used and the resulting impact on recruitment and retention.

I personally bring extensive experience in effectively addressing the cyber skills shortages globally and across multiple industry verticals. These skills shortages are an all of society challenge. Hiring net new people to fill the vast gap is simply not an achievable goal. As part of our transformation, I am introducing an expanded skills training and certification program, partnered with the best of industry and academia, which will up-skill and cross-skill our warfighters, from new recruits to seasoned service members, providing critical cyber, technical, and AI skills which they can leverage in their existing role, transfer to a new service role, and leverage in their eventual retirement, enabling and empowering them to continue their service to our Nation in this ever expanding digital age. We will provide visibility into this strategic initiative in due course.

Our transformation strategy also heavily leans into the partnerships of our existing and future Defense Industrial Base. As we reduce barriers to new entrants in support of the Secretary's Arsenal of Freedom initiative, we are clearly aware that our supply chain's resilience is our resilience. We will expand our proactive engagements with our defense partners, ensuring increasing focus on security and resilience, providing acute focus on the part they play with us in warfighter readiness, resilience, and lethality.

Finally, we do not fight alone, and so the readiness of our partners and allies is our readiness. Through extensive partnership, collaboration, and American leadership, we will bring an intensified focus on the digital transformation and modernization journeys of our partners and allies, which will enable and empower an all of coalition forces readiness for the battlefields of today and tomorrow.

CONCLUSION

As we embark on this aggressive transformation strategy, I first want to thank Congress for the continued interest in Technology and Cybersecurity, an incredibly expansive and complex field, and for providing resources to address this very dynamic journey we are together on—protecting National Security.

The race for data superiority and decision dominance is won or lost every single day. The transformation detailed today, underpinned by the unification of Enterprise Technology and the Cybersecurity Program under the DoW CIO, represents our unwavering commitment to ensuring the Department's technology ecosystem remains a decisive strategic advantage for America's warfighters. By adopting industry best practices in agile development, cloud computing, AI, and Zero Trust, by overhauling governance and embedding accountability and a bias for action, and by uplifting our holistic skills and vast partnerships, we are building a more effective, resilient, and powerful Arsenal of Freedom. All these efforts connect at a single point: empowering and enabling our warfighters. The operational realization of their data superiority and decision dominance is the hallmark of the success of our strategic transformation journey—so this is what we will deliver. With the sustained oversight and partnership of Congress, we will ensure the United States can deter, and if necessary, defeat our adversaries across every domain.

Thank you. I look forward to your questions.

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 Satellite Communications (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. Chief Digital and Artificial Intelligence Officer (CDAO) feeds into United States Cyber Communication's (CYBERCOM'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 Department of War Informa-

tion Network (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 Lieutenant General Stanton follows:]

PREPARED STATEMENT BY LIEUTENANT GENERAL PAUL T. STANTON

Chairman Rounds, Ranking Member Rosen, and distinguished members of the Subcommittee, thank you for the opportunity to report on the fundamental shift we are making to ensure the Department of War Information Network (DoWIN) prevails as the critical weapons system providing decision advantage to the warfighter. I am proud to represent the teams serving at the recently elevated subordinate unified command Department of Defense Cyber Defense Command (DCDC) and the Defense Information Systems Agency (DISA). These are the warfighters who build, operate, and defend this strategic national asset with relentless purpose 24 hours a day, 7 days a week.

In the face of determined and capable adversaries across the globe, the Joint Force's success on the battlefield comes down to one core task: getting the right data to the right place at the right time to make a better and faster decision than the enemy. Every decision, every action, every command, from the tactical edge to the strategic headquarters, depends on our ability to move data securely and at the speed of relevance. But this is not a benign environment. The cyber domain is a contested battlefield, and our adversaries are actively attempting to degrade our capabilities and erode our advantage. This persistent, daily contact leaves no room for failure.

The DoWIN is the system of weapons systems that drives operational pace, connects the sensor to the shooter, and delivers lethal effects on the adversary. As the central nervous system that underpins Joint and coalition warfighting, its integrity, availability, and resilience are paramount. The modern operational environment is defined by vast distances and the convergence of disparate missions, requiring the orchestration of a complex array of sensors, multinational partners, and Joint Force assets across multiple domains. Our primary purpose is to ensure this platform functions in this environment under pressure and provides commanders at echelon with a decisive and uninterrupted information advantage, regardless of any adversary's actions or the challenges of the operating environment.

Meeting this challenge demands a fundamental transformation in how we operate and support the Joint Force. This new path begins with a disciplined focus on the warfighter, delivering integrated capabilities directly relevant to their mission at the time and place of need. To enable these capabilities, we are engineering modern, defensible architecture that is secure by design from its very foundation. In turn, this secure architecture allows us to shift our operational mindset from reactive defense to proactive campaigning against our adversaries. Underpinning all of our endeavors is our non-negotiable priority: readiness, which ensures our forces are trained, accountable, and ready to win in this contested domain.

DELIVERING DECISIVE WARFIGHTER CAPABILITIES

This architectural transformation necessarily begins with the enterprise itself. By standardizing the enterprise, we increase both lethality and defensibility for the Joint Force. A common baseline reduces an immense and varied attack surface to a single, well-understood environment that DCDC can more effectively protect. It also provides a stable technical foundation upon which future capabilities, like the Mission Partner Environment, can function as designed in a global fight. Technological advancements give us the opportunity to design the environment we need.

DISA's initial focus has been on Defense Agencies and Field Activities (DAFA) through DODNet. This effort consolidates the disparate networks of our DAFAs to create a unified security environment for the indispensable combat support functions—from logistics to intelligence to healthcare—that enable Joint Force readiness. I am pleased to report we have already successfully migrated over 40,000 users and more than 300 sites, and we are on a clear path to meet the Fiscal Year 27 Zero Trust mandate for all 11 Fourth EState DAFAs.

Applying the lessons from this proven model, DISA is now extending this rapid, agile execution strategy to our warfighting headquarters through CommandNet. Critically, this will realign our most talented cyber and communications professionals serving in areas of strategic significance to use technology effectively. We will shift, their focus from routine systems management to their core warfighting

purpose: operational Command, Control, Communications, Computers, and Intelligence (C4I) planning and direct support to the warfighter from strategic enablers down to the tactical edge.

This standardized enterprise is the prerequisite to revolutionize service delivery to the warfighter through Mission Network as a Service (MNaaS). Through MNaaS, DISA is collapsing today's landscape of disparate, single-purpose networks into a single, secure SECRET fabric. This new model fundamentally changes the paradigm for the warfighter. Instead of building mission networks from scratch—a process that can take months—commanders can incorporate combat power according to mission requirements by composing standardized sub-parts into a coherent system. This will simplify the process for military services to deploy warfighting software into the Joint environment. For the warfighter at the tactical edge, this means gaining faster, more reliable access to the intelligence and operational data they need to make critical decisions in contested environments.

However, because we recognize that any potential conflict will be fought alongside our allies and partners, this architectural transformation applies these same principles of standardization and service-based delivery to our most complex challenge: coalition interoperability. The Coalition Information Environment (CIE) is the technical engine of the Department of War's Mission Partner Environment strategy, engineered to break down the technical barriers that have historically impeded combined operations. As the foundational infrastructure, the CIE will be the modern network upon which the MNaaS service delivery model operates, capable of handling information up to the Secret level. Leveraging the success of our Joint Operational Edge-Coalition Environment (JOE-CE) prototype in the Indo-Pacific, DISA is on track to deliver the first live, mission-ready capability by January 2027. Designed and resourced with our partners, CIE will provide an on ramp to the Five Eyes and is the flexible system to build the specific coalitions among any number or combination of partners required for any contingency.

This entire architecture is underpinned by the enhanced resiliency of the Defense Information Systems Network (DISN), our global transport backbone. We are continuously modernizing the DISN with next-generation transport and Software-Defined Wide Area Networking (SD-WAN) to strengthen its resiliency, integrity, and availability. In a contested environment where the enemy has a vote, through cyber or kinetic action, the ability of our foundational transport layer to absorb damage and dynamically re-route traffic is paramount to mission success especially in degraded, intermittent, and denied conditions. This effort is well underway. In key operational theaters, DISA is leveraging commercial technology to automatically route traffic and maintain connectivity for our forces, with enhanced resiliency for key sites already completed. We will further validate this architecture at scale during upcoming exercises, including Olympus Fires 2026, confirming the network's ability to maintain operational continuity under any condition.

AN ARCHITECTURE SECURE BY DESIGN

This transformation is predicated on a modern, defensible architecture built secure by design. DISA is building security into the foundation of every capability from day one. Our approach is founded on three pillars designed to protect our users, our perimeter, and most importantly, the mission.

The foundational pillar is our operationalization of Zero Trust principles. This is the essential model that enables the agile, data-centric Mission Partner Environment, allowing us to move beyond the legacy approach of building isolated hardware-defined networks for each coalition. It provides the granular controls necessary to grant tailored data access to specific partners based on the specific mission, enabling coalition operations with unprecedented speed. By continuously validating every user and device, this "never trust, always verify" model denies adversaries the ability to move laterally—a critical defense against modern attack techniques. Achieving a truly defensible posture demands a rigorous and correct configuration. For this reason, our specific implementation, Thunderdome, is paired with a deep investment in the training required to operate this critical capability effectively.

Second, the Zero Trust architecture is complemented by a defense-in-depth strategy that begins with a formidable boundary. The volume of malicious and automated activity directed against our networks is constant and unrelenting. To counter this, DCDC forces actively manage our globally postured Internet Access Points (IAPs) as both critical defensive platforms and a unified sensor grid. In this capacity, they serve as DCDC-directed defensive chokepoints that provide the situational awareness necessary for effective command and control of the DoWIN. In lockstep, DISA is continuously modernizing these platforms with advanced capabilities like Full Content Inspection to identify and block malicious traffic. Further-

more, DISA is leveraging artificial intelligence to analyze immense volumes of data to identify and block previously unknown malware before it can impact the mission. This global defensive posture allows DCDC to defeat many automated threats at the boundary, freeing our most talented defenders to concentrate on the sophisticated, targeted intrusions that pose a genuine risk to the mission.

While protecting the user and the perimeter is a critical function, we must defend in depth, making it hard on our adversaries with a deliberate defense, gaining and maintaining contact so we can counter-strike and impose cost. The third and most critical pillar is tailored, mission-focused defense executed by DCDC. This approach applies the time-tested warfighting principle of concentrating strength on what matters most. To do this, DCDC identifies and maps mission threads to develop analytic schemes of maneuver—the specific data paths required to accomplish a warfighting function, such as generating a call for fire. Understanding precisely how a system is used in an operational context dictates how it must be defended, allowing DCDC to build a comprehensive, prioritized defense around the capabilities most critical to operational success.

CAMPAIGNING AT THE OPERATIONAL LEVEL OF WAR

To maintain our battlefield dominance, these tools must be paired with a fundamental shift in our operational mindset. We must mature beyond reactive network defense and exercise true Command and Control (C2) at the operational level of war. This represents a fundamental shift from responding to individual incidents to orchestrating a continuous, proactive campaign. Our adversaries are not launching random attacks; their actions are part of a coordinated, purposeful campaign to achieve strategic objectives. We must therefore meet them at the operational level, leveraging the deep situational awareness from our global sensor grid and coordination with intelligence to understand their objectives and direct synchronized actions across the DoWIN to disrupt them before they can achieve their effects.

The elevation of DCDC as a sub-unified command to United States Cyber Command (USCYBERCOM) was the foundational first step in operationalizing the defense of our networks, moving beyond a reactive network defense to a posture focused on gaining and maintaining contact with the enemy and imposing cost. The elevation provides a central anchor point for the Department to deliberately centralize the unity of effort required for operational-level command and control, creating the necessary conditions to synchronize defensive actions and direct forces across the enterprise to achieve strategic effects. We are moving beyond chasing individual alerts to campaigning against systemic vulnerabilities and coordinated threat actors.

The synergy created by the dual-hatted leadership of DCDC and DISA is the key to this effective C2 model, ensuring there is no daylight between the builder, the operator, and the defender. This structure seamlessly fuses DCDC's operational ability to maneuver and defend the network with DISA's deep technical knowledge of the underlying infrastructure we build and operate. As DISA fields new capabilities and modernizes the network, DCDC is fully informed and able to adjust its defensive posture accordingly. This unity of command drives priorities for mutual benefit, speeds decisions, and ensures that we design, extend, and mature our environment with operational effectiveness at the forefront.

READINESS REVOLUTION

Our transformation in architecture and mindset is powered by the readiness of our total force. Technology provides the tools, but it is trained and accountable people who win battles, which is why readiness is a non-negotiable, No. 1 priority of both the Command and the Agency. Across DCDC and DISA, we are driving a revolution to make readiness an objective, measurable, and defensible standard. This revolution is built on three core pillars: acquiring elite talent, delivering advanced training, and enforcing a framework of accountability.

Readiness begins by bringing in the right people to execute our critical mission. To do so, we have adopted a proactive and flexible hiring posture, applying targeted talent strategies and surgical hiring actions. Our focused approach is based on a proven model of direct engagement with targeted recruits. This effort is already yielding significant results. Our most recent hiring event saw over 70 percent of attendees advance in the hiring process. From this single engagement, DISA is on track to hire 32 candidates in critical cybersecurity positions in just 3 weeks. This successful model is now our template for talent acquisition, ensuring we consistently onboard the expert warfighters our missions demand.

Across DCDC and DISA, we are fostering a qualification culture focused on building the skillset of our expert warfighters to ensure the organizations they serve are

cohesive and combat ready. A complex, data-centric architecture demands an equal level of human expertise to be effective under pressure. Individual excellence is what enables our collective, organizational power. It is this enterprise-wide readiness that allows us to act as a unified whole, ensuring every echelon can execute commands with speed and precision. Crucially, this readiness includes dedicated investments in our premier cyber workforce, training them to leverage emerging technologies like artificial intelligence and machine learning to ensure the Department's advantage in the future fight. We keep our talent focused on higher order skills while technology addresses tasks that are already well understood.

To achieve this, we are looking at the problem holistically through the lens of Doctrine, Organization, Training, Material, Leadership and Education, Personnel, Facilities—Policy (DOTMLPF-P), To build the expert force required for the future fight, we are taking a comprehensive approach, ensuring our doctrine, organization, and personnel policies are fully aligned. A prime example is the unified effort between DISA and DCDC to elevate the standards for our Cybersecurity Service Provider (CSSP). By investing in a rigorous training and certification framework, we are forging a professionalized cyber workforce with the verified technical proficiency and operational readiness required to defend the DoWIN against any threat, under the most demanding conditions.

A culture of highly qualified personnel must be complemented by a framework of effective accountability. This represents a fundamental shift from mere compliance to one of deep, personal ownership at every level. In practice, accountability means disciplined execution through a robust governance framework and objective, enterprise-wide performance metrics. As a clear example, we are codifying new defensive policies that establish direct lines of responsibility and mandate common reporting standards. This consistency enables the speed and scale necessary for effective enterprise network operations and defense, ensuring that when an order is given, every echelon is ready and accountable to execute to a common high standard.

CONCLUSION

Our transformative actions are a direct response to a fundamental reality: the contest for information dominance is not a future challenge; it is a continuous, daily fight. We must build, operate, and defend systems while contesting active aggression in cyberspace. To meet this reality, we have departed from incremental change and are driving a fundamental transformation of our architecture, our operational mindset, and our force.

Chairman, Ranking Member, the security of the Department of War Information Network is inextricably linked to the security of our Nation. Our ability to project power and defend our interests across every domain—land, air, sea, and space—begins with our ability to command and control our forces through a resilient and defended network. The transformation I have detailed today is our commitment to ensuring that this foundational weapons system remains our decisive advantage in an era of persistent conflict.

At the forefront of this constant, daily fight are the dedicated men and women of DCDC and DISA. It is their vigilance, their ingenuity, and their warrior ethos that turn strategic vision into operational reality. I am immensely proud to represent this total force of soldiers, sailors, airmen, marines, guardians, dedicated civilian personnel, and our industry partners. They are our most critical asset.

With the continued support of this Committee, we will ensure the United States can deter our adversaries and, if necessary, fight and win in any domain, secure in the knowledge that their ability to command, communicate, and decide is unmatched.

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. 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. 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. With great support from Congress, we have an initiative that we reference as design, security, and resiliency. 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.

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. 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. 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 multipronged 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.

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. 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.

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. The deep assessment of replacement of that, I'm unfamiliar with right here, I can take that away as an action for you.

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. 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 followup 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 timeframe 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. No. 1.

No. 2, 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. Yes. 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. 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. 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 toward 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. 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 decisionmaking, 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. 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. Yes. Thank you, Ranking Member. In July 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. 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.

Senator ROUNDS. 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.

With that, the Subcommittee meeting is adjourned.

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

[Questions for the record with answers supplied follow:]

QUESTIONS SUBMITTED BY SENATOR JACKY ROSEN

PROVIDERS AND MANUFACTURERS

1. Senator ROSEN. We understand that the Department of Defense has not fully on-boarded all clouds from providers selected for the Joint Warfighting Cloud Capability (JWCC) that was awarded in December 2022. What is the status of cloud onboarding for all cloud providers? What is the actual utilization, not the amount awarded in ceiling contracts, for each JWCC provider?

Lieutenant General STANTON. The program management office tracks utilization through awarded task orders through our routine contract deliverables from the CSPs, which represent the utilized funds for specific cloud services. While the contract ceiling is $9 billion, the estimated utilization to date is $429 million.

All four CSPs have been awarded task orders since the contract's inception in December 2022. The breakdown of funds is as follows:

JWCC Cloud Spend Based on Actual Utilization: $429 million
Amazon Web Services: $235 million
Google Public Sector: $16 million
Microsoft Corporation: $141 million
Oracle America: $37 million

Mr. DAVIES. All four JWCC providers—AWS, Google, Microsoft, and Oracle—are fully onboarded and operational across the Unclassified, Secret, and Top Secret classification levels. While DOW currently tracks awarded task order values, the Department is aggressively improving our enterprise-wide visibility into real-time utilization and obligation data. To achieve this, DOW CIO will leverage industry-recognized best practices that the Department will use in a tailored framework for cloud cost management and optimization for better investment, budgetary and architectural decisions. The Department continues to assess the strategy and adjust course as necessary, which includes providing the granular financial transparency necessary to optimize cloud consumption. This ongoing execution ensures the Department moves beyond tracking contract ceilings to actively managing actual mission demand, maximizing the efficiency of our cloud investments for the warfighter.

2. Senator ROSEN. 10 USC 3453 establishes a preference for commercial goods and commercial services, 10 USC 2222 requires the Secretary of Defense to use "an acquisition and sustainment strategy that prioritizes the use of commercial software and business practices", and President Trump issued Executive Order 14271 titled "Ensuring Commercial, Cost-Effective Solutions in Federal Contracts." Despite these and other policy guidance, the Department continues to maintain, procure, and update non-commercial business systems that do not provide capabilities comparable to their commercial alternatives. Moreover, when the Department has procured commercial business systems, instances have occurred when they have limited the ability of original software manufacturers to advise the Department on maintaining commercial best practices. What is the Department's policy to consider replacing non-commercial business systems with commercial alternatives and seeking the

input of original software manufacturers to ensure alignment with commercial best practices?

Lieutenant General STANTON. DISA and the DOW have a strong preference for commercial goods and services as noted in, and in accordance with, the referenced U.S. Code (U.S.C.) and Executive Order. To this end, the Procurement Services Directorate (PSD) requires a Determination and Finding (D&F) to procure any non-commercial products and services on behalf of the agency. This D&F employs extensive market research to document if existing systems, subsystems, capabilities, and/or technologies are available, or could be made available, to meet the needs of the DOW in whole or in part. This D&F is subject to a rigorous review process and mandates approval by the Head of the Contracting Activity (HCA). By requiring this D&F, the Department is essentially treating non-commercial buys as the "exception" rather than the rule. Additionally, the Agency is also working through the implementation of OMB Memorandum M–26–12, which was issued on 17 April 2026, and adds additional levels of approval and scrutiny up to the Senior Procurement Executive (SPE) level.

As it relates to ensuring that commercial best practices are employed as part of all procurements, DISA conducts extensive strategic and tactical market research to engage industry partners. This process ensures that the agency is tracking general best practices and changes in the market over time as well as action-specific information that can inform the acquisition strategy on any given action. Examples of this market research include sources sought, requests for information, industry days, consultation with market experts, etc.

Specific to JWCC and commerciality/best practices, the Department, in accordance with the July 31, 2023, Department Chief Information Officer memorandum, is transitioning legacy cloud contracts to the JWCC and utilizing JWCC for all IL6 (Secret) workloads. As JWCC is a commercial contract, this aligns with the spirit of the referenced U.S.C. and Executive Order. To ensure alignment with industry's best practices, JWCC provides Mission Owners with direct access to "advise-and-assist" services from the original software manufacturers. This direct engagement provides expert architectural guidance and leverages native commercial capabilities, intentionally avoiding the historical risks and high costs associated with heavy software customization.

Mr. DAVIES. The Department's policy is to prioritize commercial software and services wherever they meet mission requirements, while limiting customization that diverges from commercial best practices. DOW CIO is strengthening governance to ensure acquisition strategies evaluate commercial alternatives early and add input from original software manufacturers to maintain alignment with industry standards and lifecycle support.

DOW CIO is also leveraging enterprise approaches, including commercially available platforms and FinOps practices, to improve visibility into system performance, cost, and utilization, enabling more informed decisions on modernizing legacy systems. This approach supports cybersecurity, reduces long-term costs, and ensures the Department benefits from ongoing innovation in the commercial sector. Under DOW CIO's leadership, the Defense Business Council has translated this commercial-first strategy into tangible Defense Business System progress, pivoting the Department away from monolithic architectures and toward rapid, secure software acquisition pathways.