S. HRG. 119–163

DEFENSE OF THE DEPARTMENT OF DEFENSE INFORMATION NETWORK

HEARING

BEFORE THE

SUBCOMMITTEE ON
CYBERSECURITY

OF THE

COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

MAY 21, 2025

Printed for the use of the Committee on Armed Services

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

U.S. GOVERNMENT PUBLISHING OFFICE
61–611 PDF WASHINGTON : 2025

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

JOHN P. KEAST, *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

MAY 21, 2025

DEFENSE OF THE DEPARTMENT OF DEFENSE INFORMATION NETWORK

WEDNESDAY, MAY 21, 2025

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

The Subcommittee met, pursuant to notice, at 2:30 p.m. in room SR–222, Russell Senate Office Building, Senator Mike Rounds (Chairman of the Subcommittee) presiding.

Subcommittee Members Present: Senators Rounds and Rosen.

OPENING STATEMENT OF SENATOR MIKE ROUNDS

Senator ROUNDS. [Unaudible] the Cybersecurity Subcommittee today.

You did an excellent job at the Army's Cyber Center of Excellence on Fort Eisenhower and it is great to see that the Army is cultivating and rewarding capable cyber operators and leaders like yourself.

Your testimony on securing and defending the Department of Defense Information Network (DODIN) comes at a critical juncture for our Nation's cybersecurity posture. Our military must maintain a ceaseless vigil against relentless attacks on our networks from sophisticated adversaries.

This is not a theoretical battle. Cyber operators actively defend our networks against State and nonState actors 24/7 365 days a year.

The fundamentals of the cyber domain present a persistent challenge. Adversaries require only a single successful breach while we must maintain perfect defensive integrity across all systems at all times.

The department has invested billions in active defense of the network that supports the entire Department of Defense (DOD). Defense Information Systems Agency (DISA), is the organization responsible for providing and running the department's secure systems and networks.

The organization responsible for protecting and securing the daily operations of those networks is an organization called the Joint Force Headquarters Department of Defense Information Network (JFHQ DODIN), and Lieutenant General Stanton oversees both, and as such is one of the many individuals across the department that is dual hatted.

The DODIN has been around for 10 years and the directive to elevate it to a subunified command represents a significant organi-

zational milestone. Making it a subunified command allows it to be task oriented underneath Cyber Command to focus on running and securing the DOD's networks and will further strengthen our defense.

DISA and JFHQ DODIN use different tools to protect DOD networks such as Thunderdome and the zero trust security program, both of which are being implemented very quickly.

Today we will hear about these two systems, which will be ready by 2027 along with other important network security programs.

Despite progress in these security programs, the road ahead demands continued focus and urgency, from securing the operational technology in end user devices and weapon systems to implementing artificial intelligence capabilities that can detect adversary activities before they approach our networks or hunt them down if they make it in.

The technological imperatives are clear. We must develop and implement emerging technologies in innovative ways securely and quickly. Our adversaries are rapidly innovating and we must do the same.

The threat of cyber attacks is not diminishing. It grows more sophisticated each day. When we examine the resources near peer competitors like China are devoting to developing their cyber forces the gravity of the threat becomes more stark.

They are aggressively pursuing technology to enhance their effectiveness in cyberspace and continue to make significant investments in artificial intelligence to build more sophisticated capabilities.

American technological superiority has historically been our asymmetric advantage and we must maintain this in the cyber domain. We cannot permit a capability gap to develop in such an all-encompassing and important domain of warfare.

The first proverbial shots to be fired will take place in this domain. Any attack in any other domain will be preceded by an attack on our vital cyber networks.

While initiatives to develop capabilities such as exquisite artificial intelligence-enabled (AI-enabled) cyber defense are underway, the timelines associated with delivery of these needed cybersecurity capabilities and environments are, clearly, too slow.

Extended deployment schedules create operational risk that our forces have to mitigate through other means. Our adversaries operate on compressed timelines. Our response capabilities much match or exceed their tempo.

Today, I look forward to understanding more of the notable achievements in securing and defending the DODIN. I am particularly interested in how DISA and JFHQ DODIN intend to accelerate delivery of these critical systems to enhance our defensive capabilities from the cell phone to the laptop to the enterprise network.

This subcommittee stands ready to provide the support needed to guarantee these vital efforts succeed in protecting our Nation's most critical networks.

I will now recognize my friend and colleague, the ranking member Senator Rosen, for opening remarks.

Senator Rosen?

STATEMENT OF SENATOR JACKY ROSEN

Senator ROSEN. Well, thank you, Chairman Rounds, and I would like to begin by welcoming our witness, General Stanton, and thanking him for joining us today to discuss the security and resilience of the Department of Defense Information Network, what we know as DODIN. So much easier to say DODIN. Lots faster.

This is a critical issue, not just for cybersecurity professionals but for every person in uniform and for every single mission around the globe. We must rely on trusted real-time access to information and communication.

As the director of the Defense Information Systems Agency and the commander of the Joint Force Headquarters, DODIN—so we have JFHQ and DODIN. We are going to be an alphabet—lots of acronyms today.

General Stanton, we are so proud. You oversee one of the largest, most complex and most targeted networks in the world, one that supports the President, the Secretary of Defense, the Joint Chiefs of Staff, and our warfighters operating across the globe.

That is no small task, sir, and I want to recognize the incredible scope of your mission and the personnel who support it.

We are operating in an era of persistent threats—cyber threats—where our adversaries are probing. They are testing our systems every single day seeking any opportunity however small to degrade our command and control, to disrupt our operations, or steal our most sensitive information.

This makes defense of the DODIN a linchpin for our national security, for our national safety, our personal security.

As a former systems analyst and computer programmer, I have seen how much the technological landscape has evolved since I began and how deeply integrated digital infrastructure has become to our operations and, frankly, every single bit of our lives.

But with that evolution comes an expanded attack surface, and as we integrate to more cloud-based services—AI tools, zero trust architectures—we also face increasingly complex security challenges.

In this hearing I hope we can explore how DISA is managing that complexity, how you are building resilience into the system, how you are attracting and retaining cyber talent, and integrating innovation into what you do without compromising our operational security.

I am also particularly interested in how your team is implementing zero trust principles across such a vast and, frankly, diverse enterprise and what this subcommittee can do to support this critical effort.

We know that the threats are evolving faster than ever and that is not ever going to change, I do not think. So must evolve our defenses to meet the ever changing threat.

So I look forward to today's discussion, to working with you, with Chairman Rounds, and our colleagues on both sides of the aisle to ensure the DODIN remains well protected, agile, and always mission ready.

So thank you, Mr. Chair, and I yield back.

Senator ROUNDS. Thank you.

Lieutenant General Stanton, you may begin if you have opening remarks. Your full statement will be in the record.

STATEMENT OF LIEUTENANT GENERAL PAUL T. STANTON, USA DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY/ COMMANDER, JOINT FORCE HEADQUARTERS, DEPARTMENT OF DEFENSE INFORMATION NETWORK

Lieutenant General STANTON. Chairman Rounds, Ranking Member Rosen, thank you for your support and the privilege of representing the men and women of the Joint Force Headquarters Department of Defense Information Network and the Defense Information System Agency.

I appreciate the opportunity to share our progress in designing, building, deploying, and defending the Department of Defense Information Network. It is a central resource and critical weapon system for meeting our Nation's objectives including defending the Homeland, deterring China, and rebuilding our military.

Our mission never rests. It is hard to imagine any aspect of planning, preparing, or executing modern warfighting that does not include data production, consumption, transport, or analysis.

Joint Force Headquarters DODIN and DISA have the responsibility of securely delivering real-time globally accessible information to the joint warfighter.

We ensure the right data is at the right place at the right time, empowering commanders to make better and faster decisions than our adversaries. We are war fighters supporting war fighting. We inculcate the warrior ethos.

Joint Force Headquarters DODIN and DISA maintain distinct responsibilities, yet support one another to balance performance and security in the context of risk.

On behalf of U.S. Cyber Command, the Joint Force Headquarters DODIN organizes, observes, and maneuvers within cyberspace to defeat enemy aggression and preserve functionality for friendly operations.

Under the direction of the DOD chief information officer DISA designs, builds, and securely operates the DODIN. Together we enable the inherently joint partner and enterprise-scale capabilities that ensure mission success.

Accordingly, our priorities to meet the urgency of our challenges are consistent for both the command and the agency.

First, we are building collective readiness across the department and with our industry partners. Success in war fighting requires forces that are manned, organized, trained, and equipped to operate effectively at both the individual and collective levels.

Cyber operations require combining skill sets such as host, network, and data analysis toward mutually supporting outcomes. Each must do his or her part with confidence and competence.

Importantly, our headquarters must also confidently issue DODIN wide orders, knowing that receiving organizations are ready to execute. The elevation of Joint Force Headquarters DODIN to a subunified command will significantly increase readiness by establishing a unified command structure that drives consistent training standards and readiness evaluations across all 45 organizations that own a portion of the DODIN battle space.

Our second priority is campaigning. We are proactively planning and prioritizing to defeat cyber adversaries and to provide functionally relevant capability to war fighters at the time and place of need.

Understanding cyberspace dependencies, the enemy's intent, the enemy's capabilities, and the potential for the enemy's capability to actually impact the mission provides focus for our defensive operations.

We prioritize our limited resources against the most critical systems and preserve our freedom of action while imposing cost on the adversary.

Just as fast as capabilities are in place they require upgrades. Our third priority is, therefore, continuous modernization. We actively field emerging technologies and iterate within our development process.

We design for extensibility with the understanding that technology and the operating environment will inevitably change. As we rebuild our military we shape the information environment according to how we intend to use it. We ensure it is always ready to meet expeditionary war fighting requirements.

Our final priority is to establish lethality. We impose cost on our enemies and provide decision advantage to our warfighters. Deterrence in the cyber domain includes raising the cost of attack beyond that which an adversary is willing or able to bear.

Thinking beyond cyberspace, all battlefield operations are subject to the proliferation of data. We must transform it to enable lethal and oftentimes kinetic action.

We are charged with sensing and transporting disparate data streams into a coherent and comprehensive picture that empowers decisionmakers at all levels.

Securing our Nation requires a robust, resilient, and well defended cyber environment. I am proud to represent the individuals serving Joint Force Headquarters DODIN and DISA, who carry out this mission every day.

With the continued support of this committee our cyber forces will remain prepared to meet the challenges of today and the threats of tomorrow.

Thank you, and I look forward to your questions.

[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 your support and for the privilege of representing the men and women of Joint Force Headquarters—Department of Defense Information Network (JFHQ-DODIN) and the Defense Information Systems Agency (DISA).

I appreciate the opportunity to share our progress in designing, building, deploying, and defending the Department of Defense Information Network (DODIN)—a central resource and critical weapon system for meeting our Nation's objectives from the tactical to the strategic.

Our mission never rests. It is hard to imagine any aspect of planning, preparing, or executing modern warfighting that does not include data production, consumption, transport, or analysis. JFHQ-DODIN and DISA have the profound responsibility of securely delivering real-time, globally accessible information to the joint warfighter in the heat of conflict. We ensure the right data is at the right place at the right time, empowering commanders at echelon to make better and faster decisions than our adversaries. We are warfighters supporting warfighting—this is a culture shift built on inculcating the Warrior Ethos.

We conduct our missions in the cyber domain where persistent threats are rapidly evolving, growing in sophistication, and constantly attempting to compromise operations across all warfighting domains. We cannot be complacent. The rate at which our adversaries are adopting new technology is staggering and unprecedented. Our advantage is that the cyber domain is manmade. As we rebuild our military, we will shape the information environment according to how we intend to use it, while ensuring it is always ready to meet expeditionary warfighting requirements.

JFHQ-DODIN and DISA maintain distinct responsibilities yet support one another to balance performance and security in the context of risk. On behalf of U.S. Cyber Command, JFHQ-DODIN organizes, observes, and maneuvers within cyberspace to defeat enemy aggression and preserve functionality for friendly operations. Under the direction of the DOD Chief Information Officer, DISA designs, builds, and securely operates the DODIN. Together, we enable the inherently Joint, Partner, and enterprise scale capabilities that ensure mission success.

The dual-hatted role as head of both JFHQ-DODIN and DISA bridges policy, acquisition, operations, and advocacy to meet cyberspace requirements of our warfighters. Effectively defending the DODIN requires a detailed understanding of how it is designed and employed; the JFHQ-DODIN must constantly coordinate with DISA as the environment continuously evolves. So, too, must DISA understand JFHQ-DODIN's view of the threats and adversarial campaigns targeting our capabilities such that we design, extend, and mature the environment with operational effectiveness at the forefront. The streamlined leadership model drives priorities for mutual benefit, speeds decisions, and consistently leverages policies and authorities to synchronize effects and efficiently apply resources to meet requirements.

Accordingly, our priorities meet the urgency of our challenges and are consistent for the command and agency. We are focused on four priorities: 1) Readiness—building collective readiness across Department and with our industry partners; 2) Campaigning—proactively planning and prioritizing to defeat cyber adversaries and provide functionally relevant capability to warfighters at the time and place of need; (3) Continuous Modernization—shaping the cyber domain to our advantage at pace with evolving technology and threats; and 4) Establishing Lethality—imposing cost on our enemies while providing the decision advantage to our warfighters.

BUILDING COLLECTIVE READINESS

Success in any warfighting domain requires forces that are manned, organized, trained, and equipped to operate effectively at both the individual and collective levels. The military servicemembers, civilians, and contractors who make up our workforce must be qualified on their respective cybersecurity weapon system and be fully confident in their ability to organize collaboratively in executing mission tasks. Cyber operations require combining skillsets such as host, network, data, and intel analysis toward mutually supporting outcomes; each must do his or her part with confidence and competence. Importantly, our headquarters must confidently issue DODIN-wide orders knowing that receiving organizations are ready to execute.

The elevation of JFHQ-DODIN to a sub-unified command will significantly increase readiness by establishing a unified command structure, ensuring consistent training standards and rigorous readiness evaluations across all 45 organizations that own a portion of the DODIN battlespace. Consistency and readiness standardization enable rapid dissemination of orders and intelligence for effective execution across a distributed footprint. Common capabilities employed in a common manner achieve both speed and scale.

Capabilities we put onto the DODIN or into the hands of the joint warfighter must be intuitive, performant, and resilient. Deployed technology will continue to evolve rapidly, demanding modifications to training and qualification standards that the force must master rapidly. DISA enhances Department-wide readiness by ensuring that industry builds solutions that can be effectively incorporated into our training models, maximizing utility and proficiency.

Our workforce will be held to a rigorous qualification process for cybersecurity standards. We are committed to building a robust training environment, including continuous learning opportunities, exchange programs, and industry engagements, to ensure our personnel can demonstrably execute their responsibilities. Ultimately, our success depends on cultivating a culture of critical thinking and self-improvement, supported by organizational resources.

As we improve tactical readiness within our formations, we must also more strategically align our readiness with Combatant Command requirements. DISA has field offices and field commands embedded with each Combatant Command so that we can remain engaged with emerging requirements and/or dependencies on cyberspace capabilities. If a Combatant Command cannot meet its mission based on a network,

data, or infrastructure limitation, then we must quickly modify our support to addresses emergent challenges. DISA's readiness is informed by and improves Combatant Command readiness.

We have recently seen our readiness materialize during the execution of a Joint Staff Globally Integrated Exercise. JFHQ-DODIN and DISA participated in Exercise ELITE CONSTELLATION together for the first time in March. We were able to move and maneuver our network operations in synchronization with demands from the Combatant Commands. We matured rapidly over a 10-day period and captured many lessons to shape our forthcoming participation in the exercise's next stage in June.

CAMPAIGNING

Key amongst our observations is that the joint force depends on operationally relevant information systems that must be consistently deployed and actively defended across the enterprise. As the combat support agency providing the foundational infrastructure and enterprise services for the Department, and as a command focused on cyber defense at operational level of war, we must plan, prepare, and execute coordinated tasks toward mutually supporting outcomes—we must campaign.

As JFHQ-DODIN elevates to a sub-unified command, we progress beyond incident response to address our adversaries' determined and coordinated approach to attacking the DODIN and we must view technical vulnerabilities at DODIN-wide scale. The enemy's actions are purposeful. Through analysis, we must recognize that an incident in one portion of the network is likely correlated to others distributed across the DODIN. We must anticipate vice react. We must understand that a technological vulnerability can be exploited across its entire deployment and drive DODIN-wide defenses vice point-in-time fixes.

Importantly, we must understand the missions of our supported commands such that we develop cyber defenses that preserve operational effectiveness. How a system is used determines how it must be defended. Understanding the cyberspace dependencies, the enemy's intent, the enemy's capabilities, and the potential for the enemy's capability to impact mission execution provides focus for defensive operations, prioritizes limited resources against the most critical systems, and preserves our freedom of action while imposing cost on the adversary.

The supported command's mission requires functionally relevant capability at a time and place that meets warfighter needs. The Department fights with Joint and Partner formations at echelon requiring integrated systems of systems available within the theater of operations. We cannot attempt to deliver individual widgets, but rather capability suites that address mission-relevant problems.

A prime example is the complex mission partner network essential to reestablishing deterrence in the Indo-Pacific. This cyber terrain, characterized by significant complexity and diversity across numerous networks and coalition partners must be integrated. We must actively build the future environment where we share information seamlessly, anticipate threats proactively, and respond to crises with coordinated precision. DISA must organize reenforcing and dependent capabilities into functional relevance delivered within the First Island Chain on timelines supporting U.S. Indo-Pacific Command. A hybrid-cloud environment secured with Zero Trust enabled by enterprise identity control and access management must be connected by resilient and encrypted transport. Nodes must be strategically placed and enabled according to the Combatant Command's plan. DISA must campaign to meet the requirements.

CONTINUOUS MODERNIZATION

As fast as capabilities are emplaced, they require upgrades with new applications, modernized security, and newly acquired data sets. Change is inevitable and we must fundamentally adjust our approach to technological advancement and the development of capabilities. The traditional approach of technical refresh, replacing our cyber terrain with simple one-for-one upgrades on a years-long predictable schedule will not keep us competitive. As we rebuild our military, we must continuously shape every aspect of the cyber terrain to our advantage at pace with evolving technology and threats.

This means actively fielding emerging technologies and iterating within our development processes. Interoperability was the baseline, but now we require integration—beyond interoperable—where information and capabilities are seamlessly exchanged across systems. We design for extensibility with the understanding that technology and the operating environment will inevitably change; our architecture must accommodate future advancements. We will build systems that are inherently

responsive to the ever-changing operating environment and capable of adapting to new challenges and opportunities.

The DODIN is a well-designed amalgamation of industry products and commercial capabilities tailored to support the unique requirements for warfighting. Industry solutions are designed for commercial markets. We must work with industry partners to provide capability that operates in extreme expeditionary environments under constant observation and attack by our enemies. Limited bandwidth over long distances pushes the bounds of physics, requiring a deep understanding of mission context to mitigate risk and build, operate, and defend for mission success. Industry is on our team accordingly.

DISA is actively transforming the Defense Information Systems Network with cutting-edge technologies, including software-defined wide area networking, next-generation transport solutions, and optimization through hybrid cloud architecture. These efforts establish a highly resilient and reliable global network core capable of supporting all DOD and partner mission requirements. Importantly, DISA works directly with the Combatant Commands to inform placement and prioritization.

Similarly, DISA works with the Combatant Commands and the Joint Staff to develop enterprise-level global decision support capability. Using a Development, Security, and Operations approach, DISA's program managers remain in contact with the user population to deliver intermediate capability on sprint cycles. This approach optimizes development and ensures that the evolving system remains nested with the dynamic mission.

DISA also remains current by adopting Capability-as-a-Service from cutting edge commercial partners. Full Content Inspection (FCI) is a good example of rapidly incorporating state-of-the-art technology into our defensive posture and leveraging contracted support for immediate execution. Directed to modernize the Internet Access Points (IAPs) in the Fiscal Year 2024 NDAA, DISA is postured for FCI integration across the 10 DISA managed IAPs by September 30, 2025. DISA and JFHQ-DODIN are also teaming to implement FCI across all DODIN boundary connections.

DISA's implementation of Zero Trust cyber defenses, Thunderdome, exemplifies a strategic shift toward continuous verification across the Department. By minimizing attack surfaces, improving interoperability, and enhancing visibility, Thunderdome has demonstrated its effectiveness with successful deployments and a perfect score on the DOD's Zero Trust Strategy assessment. Thunderdome is an integral component within the design of DODNet, DISA's ongoing effort to modernize and secure networks for all Defense Agencies and Field Activities. Importantly, Thunderdome is designed for extensibility, composability, and continuous analytic development.

ESTABLISHING LETHALITY

The design of the architecture and our approach to defenses deliver and maintain the network to deny adversaries any advantage. Deterrence in the cyber domain includes raising the cost of attack beyond what our adversaries are willing or able to bear. Our approach is proactive, leveraging deliberate planning to create and execute cyber defensive engagement areas that canalize the enemy onto terrain of our choosing, enabling full observability. Direct contact introduces opportunities to delay, deny, and degrade enemy actions in unique and dynamic ways.

Beyond cyber operations, all battlefield operations are subject to the proliferation of data that must be transformed to enable action. We are charged with sensing and transporting disparate data streams into a coherent and comprehensive picture that empowers decisionmakers at every level. Our mission includes establishing the enterprise architecture that supports global consistency and reusability that accelerates action.

Internally, we have recognized that DISA and JFHQ-DODIN require robustness in our intelligence, planning, and data analysis capacity to meet emergent demands. To that end, we have created a Data Analytics Support Cell from existing resources to transform how we process and act upon information. We are orchestrating data flows within our environment to aggregate and correlate data that answer decision-support requirements. Our team is building on-demand analytics as new decisions emerge. We are increasingly deploying AI and machine learning to bolster threat detection and leverage data as a strategic asset for Combatant Commanders and coalition partners.

DISA's Joint Operational Edge Coalition Environment (JOE-CE) represents a leap ahead approach to coordinating data exchange. Real-time data accessed at the tactical edge through a multi-cloud, data-centric architecture empowers commanders with a comprehensive operational picture for superior decisionmaking in contested environments. Built with robust redundancy and failover mechanisms, JOE-CE will

strengthen deterrence by ensuring the resilience and continuity of coalition operations, even in the face of cyberattacks and other disruptions.

CLOSING

The virtues of a Warrior Ethos transcend warfighting environments. Securing our Nation requires a robust and resilient cyber defense and I am proud to represent the individuals serving at JFHQ-DODIN and DISA who carry out this mission every day.

As we restructure our organizations for the optimization of our workforce, we are evaluating mission requirements, core competencies, and automation technologies that will drive operational effectiveness and performance efficiency.

With the continued support of this Committee, we remain prepared to meet the challenges of today and the threats of tomorrow. We are focused and dedicated to safeguarding the DODIN and defending our national interests in cyberspace. Thank you, I look forward to your questions.

Senator ROUNDS. Lieutenant General Stanton, thank you.

I will begin, and we will move back and forth in 5-minute rounds and we will do a couple of them and then if we have other members join they will be welcome to come in as well.

In April the Zero Trust Portfolio Management Office announced a 2030 timeline for full implementation of zero trust across operational technology devices and a date of 2035 for weapons systems.

Given the rapid evolution of threats targeting these systems, what interim security measures are being deployed to mitigate risks during this extended period?

Lieutenant General STANTON. Senator, I appreciate your question.

DISA has introduced Thunderdome, which is our implementation of zero trust. So we are able to look at individual systems. The individuals that are using those make informed decisions about what resources they are able to access.

We follow the zero trust principles. In fact, Thunderdome was recently assessed by a third party meeting all 132 of the 132 Department of Defense standards and activities for zero trust.

We have it in action already. We have implemented zero trust in coordination with United States Southern Command (SOUTHCOM), and in addition we have it embedded into the evolution of what we refer to as DOD.net, the modern and secure infrastructure and architecture that DISA is providing.

Senator ROUNDS. Since this is an open session let us talk a little bit about Thunderdome, and can you give us a little bit of an indication here so that folks that are listening to it and they are—it sounds interesting but just exactly how does it work?

Lieutenant General STANTON. Yes, Senator.

So we have a number of appliances and software products that are state-of-the-art provided by our commercial industry partners that we integrate into a coherent solution.

We first check to see who individuals are in the environment. We also check the State and security of the device upon which they are operating.

We put those two together to make sure that the user on the device are authorized to access resources, and then we have fine-grained controls that determine which resources they are able to access.

Senator ROUNDS. So when you are doing this for the next couple of years it really is a challenge for any defense system to actually

modernize while still maintaining that operational capability, and what you have done is taken Thunderdome and during this interim time period you have integrated into the systems and every—basically, every single user along with the platform that they are on is checked before it is authorized entrance into the DODIN.

Accurate?

Lieutenant General STANTON. Yes, Senator.

Senator ROUNDS. Okay, and successful in terms of—what do you—is it 100 percent successful? Is it—what is the probability of somebody getting around that and what is the biggest risk to it?

Lieutenant General STANTON. So another inherent principle to zero trust is to continuously evaluate the access to the resources. So it is not just getting into the DODIN but it is each time that you go to access resources you are reevaluated.

So the risk of someone gaining access that exists. We will never be 100 percent secure. However, we check and validate every subsequent access and if the enemy gained a foothold into the environment they cannot operate without impunity and we log everything to track what is happening in the environment.

Senator ROUNDS. Kind of leads me into the next question, which is the September 2024 DODIN command operational framework introduced new requirements for reporting readiness through the department's readiness tool called the Defense Readiness Reporting System, or DRRS.

What specific cybersecurity metrics—what are the metrics for being—you know, what are you capturing with that and how do these metrics provide a more comprehensive view of the DODIN operational readiness?

Lieutenant General STANTON. Senator, readiness is my number-one priority and the question you are asking is exactly what we are driving toward.

We have baseline metrics that assess the effectiveness of a cybersecurity service provider. The Joint Force Headquarters DODIN has evaluations teams that travel out to the 45 DODIN areas of operation and assess the effectiveness of their Cyber Security Service Provider Programs (CSSPs).

We record that in the Defense Readiness Reporting System (DRRS). We can do better and we are working on establishing additional metrics that can develop a more comprehensive picture for us to have confidence that all of the DODIN areas of operation can operate effectively.

Senator ROUNDS. Thank you.

Senator Rosen?

Senator ROSEN. Well, thank you. I was going to ask something different about the workforce first but I am going to build on the zero trust architecture.

I understand when you say who is the person user, who is the device. You are going to check them every time. We have that a lot in our own—in other things that regular people do with banking, other kinds of things.

But I would think—as I am listening to you I am thinking about how does the user or device get into the registry, if you will? I am thinking that that could be a point of vulnerability.

So how often—like, I know there is many ways that people gain access, understanding that you have things all around the globe. But thinking that there is a point of vulnerability because if somehow someone can put themselves as a trusted user or device then that is how one maybe big way they can get into the system, not the silent way. So how are you securing that piece, if you will?

Lieutenant General STANTON. Yes, Senator.

Enterprise Identity Credentialing and Access Management, or EICAM as we refer to it, is a central component to the effective employment of a zero trust environment.

Senator ROSEN. Yes.

Lieutenant General STANTON. So making sure that we know who you are and we have multiple different forms of validating your identity is an inherent principle.

Additionally, once we issue a certificate it authenticates you into the environment. That certificate is time bound and continuously checked and we have measures by which we can revoke it.

So in the event that we see something that is anomalous through our logging we can revoke that certificate on the spot and deny further access into the environment.

Senator ROSEN. Thank you. That answers the question for me, and I guess the question we always ask do you have the resources that you need now to continue to build out your zero trust architecture, going forward, as we are entering into the National Defense Authorization Act (NDAA) season, if you will?

Lieutenant General STANTON. Thank you, Senator.

There are two primary initiatives through which DISA is implementing zero trust. So DOD.net is our initiative to establish a modern and secure infrastructure for the defense agencies and field activities. They had independently run their networks previously. We are in the process of migrating them.

As we do we build in the Thunderdome zero trust model into that environment. Additionally, we are working with a multi-partner environment executive agent to incorporate Thunderdome into our implementation of the multi-partner environment, or MPE, as we refer to it.

We are not waiting.

Senator ROSEN. Okay.

Lieutenant General STANTON. We are moving out aggressively.

Senator ROSEN. Very good. This all leads to my first question that I was going to ask is about—well, it is kind of two part, the impacts of recent civilian workforce cuts and DODIN's ability to conduct your assigned missions.

But I think it is more than that because sometimes the workforce cuts—we understand we want to streamline, do things better. We are going to do things better with computing for sure.

But that can have an impact on both our future recruitment, retention, morale, which is key to maintaining our readiness and preparing for the future.

We know we have these issues, particularly when the public sector is—can be very lucrative for folks who work in that.

So if you would kind of speak of the snapshot of the impact of these cuts from deferred retirement, probationary employees,

planned reductions in force, and how is this really going to impact you, going forward?

Lieutenant General STANTON. Thank you, Senator.

First, I would like to acknowledge that I personally have the utmost respect for anyone that has raised his or her right hand and sworn an oath to support and defend the Constitution of the United States, as do all of our civilian and uniformed service members that operate within the Joint Force Headquarters and within DISA.

We will suffer about a 10 percent loss in terms of the numbers of individuals that are within the Defense Information Systems Agency. It is giving us an opportunity to ruthlessly realign and optimize how we are addressing what is an evolving mission.

Things like the multi-partner environment and initiatives like DOD.net are driving our workforce to perform roles that they had not previously, and so we are doing a realignment and we are going back to the Department to ask for what we refer to as a surgical rehiring.

We need to hire the right people back into the right position——

Senator ROSEN. That is my point.

Lieutenant General STANTON. —to then lead us forward.

Senator ROSEN. So we will talk about those resources.

If I can, this is my last part on this question because on April 10th there was a memo that was issued by the Secretary of Defense that announced the termination of several contracts and insourcing of Information Technology (IT) consulting and management services to our civilian workforce.

Could you provide any details to us in this open hearing? If not, we can do it in the closed. But what are your security concerns here? Everyone does take an oath but you have these public-private partnerships, and with all of this happening how is that really impacting you?

Lieutenant General STANTON. Thank you, Senator.

So reviewing contracts is a necessary part of our business in the IT world. As technology changes we have to continually evaluate whether or not we have the right industry partner performing the right mission, and so we routinely evaluate our——

Senator ROSEN. I just want to be sure it is the right—it is strategic and not—surgical, not just across the board.

Lieutenant General STANTON. That is absolutely correct, and that has been our approach and the Department of Defense has given us within the DISA the opportunity to handle it through a surgical lens.

So our contracts are aligned to the highly technical IT and cybersecurity workforce. They are not consulting contracts. These are individuals that are putting hands on keyboard, that are running fiber optic cables, that are performing server maintenance in a global footprint.

Our contracts are healthy and are in a good spot. The impetus and drive from the department is, however, forcing our industry partners to evaluate how they are presenting their technical force to us and we are gaining some efficiencies in the process.

Senator ROSEN. Thank you. I appreciate it.

Senator ROUNDS. Let us follow that up a little bit.

You not only have to have the tools but you have got to have the manpower as well. Talk a little bit about just the size and the scope of what this is to begin with.

You are protecting the Department of Defense's entire system. Talk about how big that is and about the number of people that you employ either in uniform or by contract to begin with.

Lieutenant General STANTON. Yes, Senator.

Our population size is, roughly, 20,000. Slightly more than half are contracted. About 6,800 are civilians and about 1,200 are active duty military service members.

Senator ROUNDS. Then the pipeline for bringing in individuals, what types of professional backgrounds or what types of training are you looking for for the majority of these individuals?

Can you give us a sense for the folks that are out there that are looking at it wondering whether or not some young man or young woman decided they want to be involved in this? Talk about what the qualifications are that you are looking for or that you can train for?

Lieutenant General STANTON. Senator, I will tell you that the first characteristic that we target in recruiting is inquisitiveness and the ability to innovate—someone that is going to be a lifelong learner that is going to adjust on the fly.

The technology that we put in their hands today will not be that which they are using 2 years down the road and so someone has to be willing to engage with and learn on their own so that they can incorporate new technology.

I am quite proud of our Scholarship for Service program that we have within DISA where we actively recruit highly technical folks and help pay for the remaining 2 years of their tuition in order to bring them onto our team for three to 5 years.

Senator ROUNDS. So you would actually for—okay, I will just take an example. Dakota State University in Madison, South Dakota, is known for their cybersecurity operations.

You would actually look for someone who had an interest in coming to work either in uniform or outside of uniform, bring them in and offer to pick up their costs of education, basically, for the 2-years with an agreement that they come to work for you. Is that what we are talking about?

Lieutenant General STANTON. Yes, Senator. Absolutely.

Senator ROUNDS. So what type of an appetite do you have for young men and women who want to serve? How many are you talking?

Lieutenant General STANTON. So in this past year we brought 39 individuals into our Scholarship for Service program.

Senator ROUNDS. Could you do a hundred?

Lieutenant General STANTON. Yes, Senator, we can.

Senator ROUNDS. Could you do 150?

Lieutenant General STANTON. Yes, Senator, we can.

Senator ROUNDS. Could you do 200?

Lieutenant General STANTON. Yes, Senator.

Senator ROUNDS. So for young men and women out there, this is not like a selected group only. This is to where you need more individuals that have this interest?

Lieutenant General STANTON. We do, Senator, and we recently in February published our workforce strategy within DISA and part of it is to do exactly what we are discussing. Create a pipeline. Not necessarily hire an individual and expect them to stay for 30 years and become a member of the Senior Executive Service.

Some will, and we need that, but many will stay on our team for three to 5 years, be enthused by being able to execute the mission, be in contact with the adversary, support our Nation, and then they will move on and do other things.

Senator ROUNDS. So let us just——

Senator ROSEN. Can I ask a question?

Could you talk about—like, give a job description? You talk about people going into the phone lines, hardware, software.

Could you just—if we were talking to young folks when we go back home give us a couple of actual job descriptions that you might get people—we are just sitting here chatting, if that is all right with you I would like to be able to tell some of those young folks.

Senator ROUNDS. Yes. No, let us—yes, this is—this is important because it is not just the type of a job description but the types of tools they are going to be working with as well.

Senator ROSEN. That is right. I was a software developer. I do not want to—do not make me work with the tools to put the hardware in but let me code away.

There are different kinds of things. Maybe you might give us some insight so when we talk to young people, which we do all the time, we might share with them the jobs that you are thinking about filling.

Lieutenant General STANTON. Fantastic, Senator. We need data analysts. We need data engineers. We need data scientists. We need folks that understand routing and large-scale routing, so folks that know how to configure a router securely.

We need folks that are also very willing to dive into newest cybersecurity tools and actually implement them, and when we establish a defense our intent is to gain and maintain contact with the adversary. So folks that understand host analysis and network analysis from a cybersecurity perspective are at the top of our list as well.

Senator ROUNDS. Fair to say that these young men and women that want to come and participate on this would have the opportunity to learn tools that enable or that are part of an artificial intelligence system or agent in terms of accelerating inquiries as to people trying to get into the systems?

Would be fair to also say that quantum is not far off with regards to what they would be working—the environment they would be working in?

Lieutenant General STANTON. Yes, Senator. I will start with artificial intelligence. It is central to our way forward. It is central to our current operations but absolutely central to the direction that we are headed.

Quantum is a little bit further out, but as I said previously as soon as quantum breaks and becomes a technology that is readily available it will proliferate very rapidly, and so we need individuals that can adjust dynamically to the change in the technology.

Senator ROUNDS. Thank you.

Senator Rosen?

Senator ROSEN. I am just going to build—we are just going to have a good time building on each other here.

How are you leveraging the AI? We know that the quantum is a little ways away but how are you leveraging the AI capabilities, particularly as you are modernizing, streamlining, and thinking about all of your architecture?

So just to kind of build off each other a bit.

Lieutenant General STANTON. Yes, Senator.

So, first, I will start with what I think would be obvious, large language models and chatbot capabilities across different classification levels.

I have them on all of my machines currently and I use them on a daily basis. So chatbot capabilities to help make the workforce more efficient.

We are also using AI to help us model and understand our transport network. So if you think about undersea cables as an example, if one were to be cut based off of an anchor that was dragged across the ocean floor can we do the what if analysis to understand how much bandwidth we have left so that we can dynamically reallocate how we move data from one spot to the next.

We are using AI in that context. We are also using it for network defense.

Senator, to your point earlier, we need to be able to see the enemy's campaign and not just an incident in—or an event in isolation. So being able to make correlations across very large data sets in real time is key to our success.

We are using AI inside of our Thunderdome zero trust environment so we log everything and all of those logs from every——

Senator ROUNDS. Learning from it.

Lieutenant General STANTON. Then we learn from it, absolutely, Senator.

Then, last, looking at the threat detection, again, from a campaign perspective, being able to zoom out and not just look at the incident that manifests in an alert from our cybersecurity system but how do I trace that all the way back to the enemy's infrastructure that they use to gain access?

Senator ROSEN. You mentioned something that is going to be a little bit of a hot button coming forward, and I just want to know if you have any opinion on this.

What if an anchor cut an undersea cable and how would you dynamically move things around? So we think about all this computing and, of course, we cannot do a lot of it without spectrum, right? Do you have an opinion about spectrum in this regard?

We know that there are other things that use the DOD spectrum, our airplanes and our—you know, all of our military. You know, our tanks, airplanes, radar and all of that.

But do you have an opinion about spectrum? Of course, while there is no dynamic spectrum sharing right now—we understand that. But if you would, you do not have to but I know that is not why you are here but I just know we are going to be talking about it a lot.

Lieutenant General STANTON. Yes, Senator.

So I think any discussion about spectrum has to be conducted through the lens of the military warfighting capability upon which that spectrum depends.

So if we take the—what is colloquially known as the lower three bands as an example, that is where we maintain our stationkeeping radars.

So a stationkeeping radar is required to track objects that move at mach 15. That is 15 miles per second. There is no room for error and there is no room for ambiguity or disambiguation and latency associated with that analysis.

So we need to make—be very, very clear that we understand what systems are operating within the portions of the spectrum and then be incredibly confident that we can deconflict the military operations from however it might be used commercially.

Senator ROSEN. Thank you. I know as we move a little bit closer to the NDAA this is going to be—we can maybe dig deeper in the classified but this is going to be an area for discussion so you can give us any other input that you cannot do in an open setting.

Lieutenant General STANTON. Yes, ma'am.

Senator ROUNDS. I agree. I think you were referring specifically to the 3.1 to 3.45 gigahertz portion——

Lieutenant General STANTON. Yes, Senator.

Senator ROUNDS. —which always seems to be under attack. Nonetheless, it is—just the physics of it are such that it is the best place to have the radar and a lot of our other capabilities located today and fully utilized today.

Let me go back to this just a little bit because I think the young men and women that are out there that are looking at this some of them would love to have the uniform on.

Some would say that maybe they do not want to have the uniform on but they would still love to participate and to help their country.

Can you talk a little bit about, okay, a young man, young woman, come in. They want to participate in this. Love the excitement of actually engaging with adversaries on a—you know, in the protection of our system.

But at some stage of the game industry is going to come and industry is going to look at these folks and say, you realize how valuable you are. That happens on a regular basis now.

Can you talk about how you can compete with industry that recognizes just how valuable these young, talented individuals are and what we can do to, perhaps, keep them with us for a little bit longer before they finally decide to head on out and join the business community?

Lieutenant General STANTON. Yes, Senator.

So, first, in my experience and my personal opinion the mission is the most enticing characteristic that we have to offer young men and women—old men and women, too.

Being in the game, in contact with our adversaries in defense of the Nation is exhilarating. It is challenging but it is also motivating.

So I think that there are a number of the folks that we bring in when they are young that will get that taste and stay with us. But I also think that we need to be willing to let folks go.

So the concept of a pipeline, I think, is critically important. Knowing that today's youth switch jobs readily—my daughter had her first job for a year and she already has a new job, and she has a master's degree in nursing and is quite talented.

But that is how our youth is switching jobs now. We have to be receptive of that concept and we have to acknowledge that coming to work for us, gaining security clearances, gaining operational experience, is going to make them better when they go to industry.

When we partner with industry we have to recognize that folks that learned how to fight defensively in cyberspace with us are now defending industry. I think that there is positive—there is a positive aspect to that.

Some subset of them will stay on our team and we need to make sure that we develop them effectively.

Senator ROUNDS. Do you have the resources to be able to compete enough to keep some of those top level folks there today?

Have we provided you with the authorizations and the funding to be able to do that, to make it worth their time to stay with the team?

Lieutenant General STANTON. Senator, I believe that we do and, again, it is a combination. I do not think we will ever be able to pay an individual as much as they would make in the private sector. However, we can pay them enough and we can give them the mission that is the reason why they stay.

Senator ROUNDS. For some of them we are talking not just defensive operations but offensive operations as well.

Commercial sector does not give them the opportunity to reach out and touch someone whereas within the operations here within CYBERCOM occasionally they have the opportunity to reach out and actually touch someone and make a difference. Fair enough?

Lieutenant General STANTON. Gaining and maintaining contact with the enemy is central to the evolution of defensive cyber operations. Doctrinally, the United States military goes on the defense to posture for the offense.

Why is cyberspace any different? It is not.

Senator ROUNDS. Great. Senator Rosen?

Senator ROSEN. I am going to build on this one because I speak from personal experience writing software, designing it. When you hit that enter key, boy, you are a bum or a hero. It is dynamic. It is exciting. It is challenging.

You solve problems and it is a—I speak a lot from personal experience on that. I understand the mission.

We have talked a lot about for folks in some of these very specific kinds of jobs where if you rotate out—sometimes people rotate in order to gain experience for their next promotions—you end up losing some of your skills if you do not keep them up all the time.

We have talked about not rotating certain folks so they can maintain and grow in the cyber area, and I have also set up, because I did this for a living, something that I thought of on others as well, a civilian cyber reserve.

So there is a lot of jobs in cyber security that—they could be engineering, they could be programming, linguistics—there are so many areas—that you might be a professor.

You might be someone who is a little bit older who wants to give back but does not want to quit their other job. So standing up a civilian cyber reserve so we can surge up or have people come to teach us. We have some pilot programs out there.

Just wondering if you—I know it is kind of off the cuff—how you feel about—this would allow for some of those folks that may leave to continue to stay engaged in a Reserve component, if you will, like we do in other areas of our military.

Lieutenant General STANTON. Yes, Senator.

So, first, just to nerd out for a second, I wrote my first computer program in 1985 in the Basic programming language on an Apple 2C computer. So——

Senator ROSEN. I am a little bit ahead of you because I wrote my first programs on key punch cards in Basic, okay.

[Laughter.]

Lieutenant General STANTON. But I——

Senator ROSEN. I walked around campus like that.

Lieutenant General STANTON. I absolutely share that thrill——

Senator ROSEN. It was exciting.

Lieutenant General STANTON. —of when the compiler actually completes.

Senator ROSEN. When the compiler—yes, oh yes. It is real. It is real.

Lieutenant General STANTON. Yes, Senator. But to the—I think that retaining our talent through the reserves and keeping them engaged is critical to our success and it also gives the opportunity for gaining a different perspective that is incredibly valuable for the ultimate defense of the Nation.

Someone operating, for instance, in the Joint Force Headquarters DODIN leaves and goes to industry and works at a bank or works at an oil company they are gaining a very different perspective that is certainly relevant to defense, and keeping them in the reserves allows them to bring that perspective and infuse it into our forces at the time of need. We must do that.

Senator ROSEN. Thank you.

Senator ROUNDS. We want to give you a little bit of a break. We will be going into a closed session in the Secure Compartmentalized Information Facility (SCIF) shortly and we wanted to give you a little bit of a break.

I have really appreciated your responses to these and, hopefully, we are giving folks back home a little bit of a sense of just what you do and the opportunities that are out there for young men and women to come in to help us in this very challenging environment.

Senator Rosen, do you have anything else to add before we close out?

Senator ROSEN. Oh, no. I will give you a break, and this is a topic I think both of us could talk—all of us could talk about all day. There are so many important issues.

So just appreciate—we will look forward to what we can talk about in the closed session.

Thank you, Mr. Chairman.

Senator ROUNDS. Very good, and with that, this will conclude the open portion of today's Cybersecurity Subcommittee hearing.

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 two business days of the conclusion of this hearing.

With that, the open portion of the hearing will stand adjourned.

[Whereupon, at 3:13 p.m., the Subcommittee adjourned.]