RECORD VERSION

STATEMENT BY

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

SUBCOMMITTEE ON CYBERSECURITY
COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

FIRST SESSION, 119TH CONGRESS

ON DEFENSE OF THE DEPARTMENT OF DEFENSE INFORMATION NETWORK

MAY 21, 2025

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 ten-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 FY24 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 decision-makers 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 decision-making 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.