RECORD VERSION

STATEMENT BY

HONORABLE KIRSTEN A. DAVIES

DEPARTMENT OF WAR CHIEF INFORMATION OFFICER

BEFORE THE

SUBCOMMITTEE ON CYBER, INFORMATION TECHNOLOGIES, AND INNOVATION
COMMITTEE ON ARMED SERVICES
UNITED STATES HOUSE OF REPRESENTATIVES

SECOND SESSION, 119TH CONGRESS

ON INFORMATION TECHNOLOGY POSTURE OF THE DEPARTMENT OF WAR

March 26, 2026

NOT FOR PUBLICATION UNTIL RELEASED BY THE
COMMITTEE ON ARMED SERVICES

SUBJECT: Transforming the Department of War's Technology Ecosystem and Cybersecurity Program into a Decisive Warfighting Advantage

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 FY 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. And to ensure we meet our objectives of strengthening US cyber capabilities, we are conducting a three-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.