RECORD VERSION

STATEMENT BY

MS. KATHERINE E. ARRINGTON

PERFORMING THE DUTIES OF
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER

BEFORE THE

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

FIRST SESSION, 119TH CONGRESS

ON INFORMATION TECHNOLOGY AND ARTIFICIAL INTELLIGENCE POSTURE OF DEPARTMENT OF DEFENSE

MAY 8, 2025

NOT FOR PUBLICATION UNTIL RELEASED BY THE COMMITTEE ON ARMED SERVICES

Introduction

Good morning, Chairman Bacon, Ranking Member Khanna, and distinguished members of the subcommittee. Thank you for the opportunity to testify today. I look forward to sharing the Department's progress on its digital transformation efforts.

Chairman Bacon, I look forward to working with you and this committee to reestablish lethality, readiness, and deterrence for our warfighters. Through multiple National Defense Authorization Acts (NDAA), this committee's leadership has empowered the Department of Defense (DoD) Chief Information Officer (CIO) to implement a sound, secure, and integrated DoD architecture; ensure interoperability throughout the DoD; and prescribe standards—including network and cybersecurity standards—that apply throughout the DoD. This authority includes oversight of the technology and cybersecurity budgets of each Military Department (MILDEP) and Defense Agencies and Field Activities Budget.

Department of Government Efficiency Initiatives

The DoD CIO is collaborating with the Department of Government Efficiency on several cost-saving initiatives to enhance military effectiveness and operational efficiency. These initiatives respond to the Secretary of Defense Memorandum, "Continuing Elimination of Wasteful Spending at the DoD," dated April 10, 2025, which directs departmental measures to strategically rebuild the military, restore accountability, and eliminate wasteful spending. Our focus is on improving software procurement processes to ensure warfighters have access to the mission-critical tools they need to enhance lethality and readiness while streamlining spending and reducing overall costs. We are analyzing spending patterns to identify opportunities for greater efficiency and cost avoidance. Concurrently, we are working with the Department to identify and eliminate duplicative services and streamline contracts, ultimately driving greater efficiency and resource optimization across the DoD.

Enabling Secure Warfighting IT Capabilities

The cyber threats we face today are evolving and we must keep pace to secure our national security interest. Identity Credentialing and Access Management (ICAM), Zero Trust (ZT), and securing the Defense Industrial Base (DIB) remain top priorities to secure our systems.

DoD ICAM efforts are foundational to several critical DoD initiatives, including ZT, Combined Joint All-Domain Command and Control (CJADC2), and the Mission Partner Environment (MPE). The Defense Information Systems Agency (DISA) deployed the NIPR Federation Hub in January 2024 to facilitate the adoption of enterprise ICAM service. DoD CIO published the ICAM Federation Framework in November 2024 to provide and direct the Department to an enterprise approach to Federation. DISA is onboarding partners to the Federation Hub, onboarding the Department of Army in February 2025, and currently working to onboard the Department of the Navy.

To expedite DoD ICAM adoption, the DoD CIO issued a memorandum, "Accelerating Adoption of Identity, Credential, and Access Management," in November 2024. This memorandum mandates that all financial systems designated by the Office of the Under Secretary of Defense (Comptroller) must support Internal Controls over Financial Reporting and onboard to an Identity Provider by the fourth quarter of Fiscal Year (FY) 2025. Further, automated account provisioning (AAP) must be enabled by fourth quarter of FY 2026. In alignment with the ZT Initiative, all DoD systems (both financial and non-financial) are required to onboard to an Identity Provider by fourth quarter of FY 2026 and enable AAP by fourth quarter of FY 2027.

Zero Trust

The Department continues to implement ZT throughout the Defense enterprise. In October 2024 and again in October 2025, we received updated ZT Implementation Plans from each of the DoD Components, which described how they will achieve Target Level ZT before the end of FY 2027.

In FY 2025, the Department is sponsoring 15 independent ZT Assessments to validate ZT integrated systems and whether ZT will achieve Target Level ZT strength or higher by FY 2027. The Department declared three big ZT successes so far in FY 2025. Specifically, the Department of Navy's Flank Speed, DISA's Thunderdome, and Dell's Fort Zero ZT systems all achieved Target Level ZT or higher. Both Flank Speed and Thunderdome achieved Advanced Level ZT and Fort Zero achieved Target Level ZT. These three ZT capability achievements allow the Department to choose from a variety of ZT-assessed solutions, which meet or exceed the Department's Target Level ZT requirement.

The Department is also applying ZT Target Level cyber defense solutions with allies and partners, such as within the MPE. The intent is to protect these the environment within a ZT cybersecurity framework to enable DoD to operate effectively, security, and with agility to invite or remove foreign partners as missions require. Target Level ZT capability within the MPE environment is transformative in how DoD securely exchanges information within the MPE environment.

Securing the Defense Industrial Base

In lockstep with our partners across the federal government, DoD CIO is dedicated to working with the DIB to bolster cybersecurity and better protect our warfighters and national security. In 2016 alone, the Council of Economic Advisors estimated that cyber-attacks cost the U.S. economy between $57 billion and $109 billion, both from ransomware extortion and from the theft of intellectual property. Those attacks have only increased since, in both frequency and sophistication. Adversaries target DIB information systems to steal cutting edge American innovations and defense technologies. The number of cyber incidents reported to the DoD Cyber Crime Center continues to increase. The Department released the strategy for DIB cybersecurity in March 2024. This strategy harmonizes efforts to bolster cybersecurity in the DIB and further DoD's efforts to apply appropriate levels of cyber protections to its most critical programs and technologies.

A key component of the Department's DIB cybersecurity strategy is the Cybersecurity Maturity Model Certification (CMMC) Program, which will verify that defense contractors have implemented existing information safeguarding requirements for sensitive unclassified DoD information. The CMMC Program assessments will be conducted against a scaled set of cybersecurity requirements that are based on the criticality and sensitivity of unclassified information needing protections. Over the past year, DoD has codified CMMC Program requirements in regulation and is working to finalize the revised contract clause that will make CMMC a part of DoD solicitations.

Today, companies can submit voluntary self-assessments and hire CMMC Third-Party Assessment Organizations to conduct independent assessments ahead of our contractually mandated CMMC implementation. Industry should start working now to ensure they are compliant with DoD information safeguarding requirements specified in Federal Acquisition Regulation 52.204-21 and Defense Federal Acquisition Regulation Supplement clause 252.204-7012. We've been very pleased to see the number of voluntary assessments to date – there are currently 2,600 Level 1 and over 300 Level 2 self-assessments submitted, and over 65 independent assessments reported.

The traditional Risk Management Framework (RMF), while establishing valuable fundamental principles and structured methodologies for risk identification and mitigation, is no longer sufficient. Its slow, resource-intensive nature prevents it from providing the cutting-edge capabilities and tools our warfighters need. To bring our risk management into the 21st century, we must move beyond static frameworks and adopt Artificial Intelligence (AI)-powered continuous monitoring systems, like those commonly used in industry. This cultural shift within the Department presents a unique opportunity to leverage automation, continuous monitoring, inheritance, cyber survivability, and operationalized RMF. This new approach will enable end-to-end cybersecurity management throughout the lifecycle of any capability, providing warfighters with critical insights into mission-related cyber risks. Furthermore, the Department's recent Software Fast Track (SWFT) initiative recognizes the central role of software in every weapon system. Building on the Secretary's March 6 memo, "Directing Modern Software Acquisition to Maximize Lethality," SWFT aims to transform how the Department acquires, tests, and authorizes software. Accelerating secure software delivery requires understanding and verifying the security of the software supply chain and development environment. CIO, in coordination with the Under Secretaries of Defense for Acquisition and Sustainment, Intelligence and Security, and Research and Engineering, has begun a 90-day sprint to develop a SWFT Framework and Implementation Plan.

DoD continues to employ a multi-pronged approach using established public-private collaboration to contribute to and adopt National Institute of Standards and Technology (NIST) standards, frameworks, and guidance, and work with industry on cybersecurity. The National Security Agency's Cybersecurity Collaboration Center continues to expand initiatives to share actionable intelligence with industry partners positioned to action those insights for defense at scale. In collaboration with the NIST Manufacturing Extension Partnership and the Office of Small Business Programs APEX Accelerators, Mentor Protégé, and Project Spectrum programs, DoD is working to ensure small businesses have access to the support they need to remain secure, compliant, and competitive.

Cryptographic Modernization

Cryptographic Modernization is another enduring effort essential to our intelligence, information, and warfighting systems. The potential development of a viable quantum computing capability increases the risk of our adversaries acquiring this technology to disrupt and compromise our National Security Systems. The Department must develop modern, quantum-resistant encryption solutions to outpace the threats from our adversaries. The DoD's current Cryptographic Modernization 2 initiative is designed to address a large portion of these concerns.

Modernize DoD Information Networks

The Department is expediting the DoD enterprise cloud environment, advancing modern software development approaches, and refining Defense Business Systems (DBS) rationalization to improve performance and reduce costs. These initiatives, coupled with budget certification authorities underscore the Department's commitment to adopting enterprise-wide approaches that prioritize user-centric improvements and rapid delivery of DoD systems and software. This strategy is the pivotal role of cloud computing within the Department's global information technology (IT) infrastructure.

Improving efficiency and effectiveness in IT Software Acquisition

Strategic commercial software acquisition is crucial for maintaining technological advantages and mission readiness for the warfighter. The Department has a multi-pronged approach centered on leveraging enterprise-wide agreements, robust governance, and data-driven decision-making. We will strengthen governance to implement IT Category Management best practices to standardize solutions and reduce redundancy. We will expand use of Core Enterprise Technology Agreements that leverage the Department's buying power to drive best-value solutions from commercial software providers. We are conducting analysis of commercial software procurement, demand, and usage data to optimize spending and improve license utilization. Finally, we will explore enterprise Software Asset Management programs that provide asset visibility and improve lifecycle management.

These initiatives and collaboration between DoD stakeholders and industry partners represent a strategic imperative. Optimizing commercial software licensing will streamline acquisition, reduce costs, and enhance cybersecurity to equip warfighters with the cutting-edge technology necessary to maintain a decisive advantage. This data-driven and collaborative approach ensures the DoD remains at the forefront of technological innovation.

Accelerate the DoD Enterprise Cloud Environment

Cloud computing provides the agile platform necessary for rapid data access and innovation, crucial for battlefield success. The Joint Warfighting Cloud Capability (JWCC) contract delivers commercial cloud services at all security classifications, enabling critical initiatives like CJADC2. With widespread adoption, including the Army's recent selection of JWCC as its primary cloud contract, we are actively streamlining cloud contracting and reducing sprawl. JWCC's enterprise-level delivery ensures global operational reach enhanced by expanded cloud capacity for U.S. Indo-

Pacific Command, and new capabilities that support other combatant commands. Our focus on edge computing reduces latency, enables advanced data processing, and improves operational resilience.

The DoD is accelerating the adoption of fit-for-purpose cloud capabilities, including classified environments. Our Cloud and Data Center Optimization initiative transforms the DoD's IT infrastructure by migrating applications from legacy data centers to high-performance environments, enhancing security and efficiency. Integrating advanced automation, AI, and edge computing minimizes latency and strengthens cyber resilience. This modernization effort creates a secure, scalable, and mission-adaptive IT ecosystem, supporting current operations and future needs.

DoD Modern Software Development Practices

Recognizing software's criticality to modern warfare, the DoD is committed to developing and delivering software to the user at speed. This requires transforming policies, processes, technology, workforce, and culture. The FY 2025-2026 Software Modernization Implementation Plan focuses on accelerating enterprise cloud adoption, establishing a robust software factory ecosystem, and transforming processes to achieve this goal. The plan outlines key activities and responsibilities for enhancing warfighter lethality through improved software delivery.

Recent years have seen a cultural shift toward modern software development practices. Components have established dedicated offices, inventoried activities, and developed policies and practices to foster this change. The U.S. Air Force launched a new software directorate, the Navy published guidance on optimizing its software factory ecosystem, and the Army implemented acquisition reforms and elevated its Enterprise Cloud Management Agency. These efforts, coupled with the JWCC contract and new guidance on Application Programming Interface, DevSecOps, and continuous Authority to Operate, accelerate modern software development and delivery. The DoD’s Software Acquisition Pathway is based on commercial product delivery best practices and is built for rapid innovation cycles. The Secretary’s March 6 directive on modern software acquisition further emphasizes speed and warfighter needs. It mandates the use of the Software Acquisition Pathway and innovative contracting approaches to streamline acquisition and foster greater collaboration with cutting-edge technology partners in the private sector.

The Department focus remains on executing the FY 2025-2026 plan software modernization implementation plan which prioritizes improving the DoD Enterprise Cloud Environment, scaling modern software development practices (including modernizing legacy systems and incorporating AI), and developing the software workforce under direction of the Software Modernization Senior Steering Group to ensure momentum and alignment with the overall strategy.

Cybersecurity of Artificial Intelligence

Ensuring our AI systems are both secure and effective is vital to our defense. This is a top priority, directly supported by the Deputy Secretary of Defense.

This effort is led jointly by the DoD CIO and Chief Digital and Artificial Intelligence Office

(CDAO). Think of it like this: the CIO is the cybersecurity expert, making sure all our systems, including AI, are protected. The CDAO provides specialized AI knowledge to help the CIO address the unique security needs of these advanced technologies.

We've already made significant progress and last summer, the CIO released new guidelines to help manage cybersecurity risks specific to AI. These guidelines provide a roadmap for building security into every stage of an AI system's lifecycle. We're constantly improving these guidelines, incorporating the latest lessons learned.

We're also focused on investing wisely in AI. The CIO and CDAO are working together to provide clear guidance to different parts of the DoD, ensuring that everyone's AI projects align with the overall strategy and avoid wasted resources.

Moving forward, we'll continue to develop and implement consistent security standards for AI. This is crucial for our warfighters to trust and rely on these systems.

Finally, we're exploring how AI can improve our cybersecurity. Imagine AI helping us analyze huge amounts of data to quickly detect and respond to cyberattacks. This is a game-changer. The CIO is leading an effort to bring together all the key cybersecurity players across the DoD to develop and use these powerful AI tools.

This combined approach – securing our AI systems and using AI to enhance our security – is essential to successfully integrating this transformative technology across the Department.

Defense Business Systems Modernization

DoD must deploy an enterprise approach to rationalize investments and deliver modern business capabilities in an increasingly digital landscape. Business systems, which offer common functions across organizations like health, logistics, human resourcing, and training, offer an opportunity to ensure modern and integrated business processes are in place to support the mission. We are actively working to consolidate or streamline business functions and data at the enterprise level to improve our processes, enable data integration, and reduce complex system interfaces. These enhancements will enable faster responses to mission and provide business data for holistic decision-making. Our enterprise, data-driven DBS portfolio management approach will drive rationalization across the portfolio to transform the way the Department does business. In FY 2024, we retired 115 DBS, with an additional 36 systems already retired in FY 2025. Lessons learned from these DBS retirements identified roadblocks we are working to resolve like data migration challenges, systems interdependences, statutory inconsistences, regulations, policies, and processes which hamper rationalization processes.

The Department is committed to managing DBS as a strategic asset and will use the annual certification process to ensure our DBS portfolio aligns to the strategic priorities and direction of the Department. We are driving to fundamentally transform Department processes to enable a highly efficient business environment that effectively supports our national defense priorities.

Mission Partner Environment

The Department recognizes the strategic advantage of strong alliances and is prioritizing the modernization of its MPE to enhance information sharing and collaboration with allies and partners. This modernization effort centers on transitioning to a secure, cloud-based, ZT, and data-centric architecture, enabling seamless integration across the full spectrum of military operations. This transition will provide a common operational picture and improve interoperability for more effective coalition command and control (C2).

Key initiatives within this modernization effort include developing an enterprise wide MPE for secure information exchange at various classification levels. This includes enhancing Five Eyes network federation for improved classified information sharing to support C2, planning, and operations. The DoD is also bolstering information sharing capabilities within the Indo-Pacific region, particularly through the AUKUS partnership with Australia and the United Kingdom, to promote regional stability and deeper integration of security and defense-related science, technology, industrial bases, and supply chains.

The DoD is actively experimenting with and demonstrating these modernized MPE capabilities through operational assessment events and exercises like Operation HIGHMAST and Project OLYMPUS. These initiatives emphasize data-centric interoperability and cloud-based services, focusing on globally integrated deterrence and a unified, agile architecture. Continued investment in network development, legacy system transitions, and programmatic integration is essential to fully realize the potential of the data centric MPE, ultimately empowering warfighters with enhanced battlespace awareness and enabling decisive action across all domains.

Budget Certification Authorities and the Capability Programming Guidance

In accordance with 10 United States Code (USC) §142, the DoD CIO annually executes its budget and certification authority. An annual Capability Programming Guidance (CPG) is provided to components, ensuring a clear, manageable, and repeatable process to review the proposed components' budgets for those capability areas under my statutory authority. This guidance identifies investment focus areas for the DoD CIO's assessment and is consistent with the interim 2025Interim National Defense Strategic Guidance and Defense Planning Guidance. The document continues to improve by focusing on outcome-based metrics & critical capabilities. In conjunction with the Department's broader budget guidance, the components build their budgets, which are then assessed against the priorities identified in our CPG.

The DoD CIO successfully completed seven FY budget assessments and determinations, beginning with the FY 2020 President's Budget. The certification review process identifies capability areas at risk. We then work with the MILDEPs, and other components, to address these risks areas in future budgets.

Warfighting Command, Control, and Communications

The essence of military effectiveness, particularly in planning, coordination, and control across the spectrum of the Department's missions, is fundamentally rooted in Command, Control, and Communications (C3) systems. These systems serve as the backbone, delivering the critical information necessary for the seamless execution of operations. We are at the forefront of charting

the path for the future development, implementation, fielding, and sustainment of strategic and tactical C3 capabilities. CJADC2 is improving C2 capabilities across all domains (land, air, sea, space, and cyberspace). It aims to enable a faster and more effective decision-making cycle by connecting all military services and their sensors and communications into a single network. This is exemplified through initiatives such as the Global Command and Control System, ensuring unfettered access to the Electromagnetic Spectrum (EMS), pioneering advanced EMS/IT allowing for advanced EMS Battle Management, and spearheading the integration of 5G technologies directly to the warfighter. These initiatives are not just components of our strategy; they represent critical capabilities that are prioritized within the enterprise, underscoring our commitment to maintaining and enhancing the operational effectiveness and technological superiority of our forces.

Warfighting Global Command and Control System – Joint

The Global Command and Control System – Joint (GCCS-J) is the Nation's premier system of record for the C2 of joint and coalition forces. This critical capability supports the warfighter by providing comprehensive situational awareness across all areas of responsibility, including enemy and Blue Force locations. GCCS-J integrates data from multiple sensors and intelligence sources into a single common operational picture, enabling decisive action. The system combines feeds from 46 different sensor and reporting systems, delivering correlated and augmented data to 35 visualization and analysis systems used globally across all Combatant Commands and Services at multiple echelons. GCCS-J plays a pivotal role in Joint Fires modernization, Global Integrated Operations, data synchronization with mission partners, and CJADC2.

Electromagnetic Spectrum

Military spectrum access is crucial to win wars, and achieve key presidential objectives, such as southwest border security and Golden Dome for America. Accomplishing these key initiatives will not be possible without the spectrum required to operate the military's key radar and communications systems.

At the same time, we understand the increasing commercial demand for spectrum. The Department is working with the White House, the Department of Commerce, other interagency partners, and industry to explore ways to increase commercial spectrum access without jeopardizing homeland defense and national security.

The Department relies on hundreds of air, sea, and land-based systems for a wide range of missions. The mid-band spectrum is particularly vital to DoD. As one prominent example, commercial vessels operating in the Red Sea have been attacked by unmanned systems and ballistic missiles originating from Houthi rebels in Yemen. U.S. Navy warships respond to commercial vessel distress calls, and shoot down missiles and enemy unmanned systems, utilizing the very spectrum at risk of being less available to our warfighters.

Furthermore, China has taken significant steps to challenge U.S. control of the spectrum and seeks to exploit U.S. vulnerabilities in the spectrum. China has sought aggressively to influence the International Telecommunication Union (ITU). As the international regulatory body governing

spectrum, matters before the ITU influences DoD's ability to operate a wide range of capabilities, including nearly every modern weapons system; communications systems; Global Positioning System (GPS) and other position, navigation, and timing (PNT) systems; radars across all domains; space-based and terrestrial sensors; and more. DoD's presence and robust engagement at the ITU, other international bodies, and with likeminded partners and allies is essential to countering China's aggression to ensure military spectrum access. As the Department's principal staff assistant for all matters related to spectrum and consistent with DoD CIO's authority under 10 USC §142, DoD CIO continues to focus on aligning efforts across the Department to ensure we are collectively driving towards Secretary of Defense priorities and what the warfighter needs to deter conflict, fight, and win.

Dynamic Spectrum Sharing

We are laser focused on developing a technology that will allow for dynamic, large-scale spectrum sharing between government and commercial spectrum users. From the Department's perspective, Dynamic Spectrum Sharing (DSS) presents a feasible path for commercial access to spectrum currently used by DoD without harming homeland defense and national security. We acknowledge that developing DSS at scale will be a significant engineering challenge, requiring substantial investment. However, with support from industry as well as Congress, the United States could be the first Nation in the world to develop dynamic spectrum sharing at scale.

The Department has been encouraged to see our industry partners pioneer advances in innovative spectrum sharing technologies. As spectrum reallocation choices become more and more difficult to resolve, we must look towards more towards technological solutions, such as DSS, to ensure both Federal and non-Federal spectrum needs are met. DoD is leaning in on dynamic spectrum sharing to support this.

We currently have a request for proposals out for review with industry with bids already received and expect to demonstrate the most promising technologies this November.

The Department understands it cannot achieve spectrum superiority without a whole-of-government, whole-of-industry, and whole-of-nation commitment. Accordingly, we continue robust engagement with our partners in the interagency, industry, and academia to deliver the best spectrum outcomes for the Department and the Nation. Dynamic spectrum sharing would be a game changer, unlocking significant economic and technological benefits for the Nation.

Spectrum IT Modernization

The Department continues to relentlessly focus on bringing capability to the warfighter at the speed of mission. Spectrum IT Modernization provides a shining example of where we need to apply this philosophy.

Today, spectrum operations are executed primarily through time and resource intensive processes using disparate automated and manual tools. DoD must modernize spectrum operations from a static-based approach to operationally oriented activities that are agile, automated, and resilient.

Spectrum IT modernization will enable spectrum superiority against peer and near-peer competitors contesting the spectrum and allow DoD systems to access and use spectrum in congested environments without causing or incurring unacceptable interference.

Under DoD CIO oversight, spectrum IT transformation will leverage a foundational modern cloud-based infrastructure environment with an integrated and cybersecure data fabric to improve resiliency, scalability, and rapid development to address legacy applications.

5G

The DoD CIO assumed leadership of the 5G mission and the 5G Cross-Functional Team on October 1, 2023, in accordance with the FY 2021 NDAA. In this role, DoD CIO is leading efforts to operationalize 5G capabilities and Open Radio Access Network architectures in support of the warfighter.

CIO leads 5G efforts through contributions to international standards development organizations and by identifying and providing implementation guidance for both dual-use commercial and military focused 5G technology applications that provide the optimum return on investment to the Department. CIO also continues to coordinate with the Under Secretary of Defense for Research and Engineering (USD(R&E))'s FutureG office on 5G prototypes / research and development activities. CIO's current focus is on transitioning the R&E pilots/prototypes to the Services, creating process improvements to accelerate the deployment of commercial 5G on all military installations in accordance with the FY 2023 NDAA, and advancing 5G-enabled capabilities across the Department and developing associated security policy to ensure that 5G capabilities deployed to the warfighter are reliable and secure.

Within DoD, 5G will present new cybersecurity considerations evolving from new technology; a requirement for ZT implementation; potential supply chain risks; lack of visibility; configuration weaknesses; and a vast adoption of operational technology / Internet of Things devices. 5G architectures will also expand traditional cellular connections to commercial cloud and satellite communications over time, expanding vulnerability footprints into previously disparate operational environments. The higher data speeds and lower latency of 5G will also require a keen focus on DoD data protection and availability. DoD must lean into more effective data encryption through 5G networks, adopting post quantum cryptography, managed attribution, and obfuscated devices and device locations.

The DoD is moving swiftly to guide the DoD's implementation of 5G networks through reference architecture; adoption of modern cryptography; implementing supply chain restrictions; ZT requirements and increasing defensive cyberspace monitoring and data protection.

Positioning, Navigation, and Timing

The DoD CIO is fully engaged in leading the implementation of the Department's PNT Strategy to provide robust and resilient PNT for the Joint Force and is working through the many challenges of development and integration of new PNT capabilities. Robust and resilient PNT

services are critical to enabling modern warfighting systems to maneuver, communicate, and engage, and for advanced weapons to function in today's highly contested navigation warfare environment.

The Department is focused on modernization of the GPS, the cornerstone of DoD's PNT Enterprise, which includes acquisition and fielding of GPS M-code user equipment, modernized GPS satellites to provide more powerful signals, and the next generation operational control segment to fully employ all capabilities on the more capable GPS satellites. The Department is also fully aware of the need for alternate PNT capabilities for use during periods that GPS is degraded or denied, and, using a modular open system approach (MOSA), is developing non-GPS PNT capabilities to ensure PNT services are accessible to support U.S. and coalition military operations.

The Services are beginning to field modernized GPS M-code user equipment and alternate PNT services into ground and maritime systems such as the Army's Dismounted Assured PNT System and the Mounted Assured PNT System (MAPS). The USMC is beginning to field MAPS into its ground-based platforms. Additionally, Army aviation will also begin fielding GPS M-code into its aviation platforms this year. The Navy is fielding alternate PNT coupled with GPS in their GPS-Based Positioning, Navigation and Timing Service (GPNTS), into the surface fleet. Navy has fielded GPNTS into about half of the surface fleet and anticipates fielding M-code GPS receivers into GPNTS starting in FY 2027. The Navy is also fielding an enhancement to GPNTS known as Non-GPS Aided PNT for Surface Ships which increases data integrity and accuracy in GPS contested environments by bounding inertial and clock drift.

The Air Force is developing the M-code based Embedded GPS Inertial Navigation System and the MOSA compliant Resilient Embedded GPS Inertial Navigation System to provide M-code and alternate PNT capabilities in critical DoD aviation platforms. The Navy and DISA are engaged in a joint effort to achieve global timing resiliency though the Critical Time Dissemination initiative and Defense Regional Clocks. DISA is continuing to deploy advanced clock suites and refresh initial configurations to achieve a distributed timing holdover capability. Challenges remain, but progress is being made to ensure the Joint Force has assured PNT services in the battlespace.

National Leadership Command Capability

A capability at the forefront of the Department's highest priority missions, is the National Leadership Command Capability (NLCC), which supports Presidential and Senior Leader Comms (P/SLC), Continuity of Operations/Continuity of Government Comms (COOP/COG Comms), and Nuclear C3. Our NLCC customers, to include Senior Military officials, Congress, and the President, utilize NLCC systems that provide common communication capabilities used across operational environments, regardless of location. These communications are critical to ensure our government and operations continue through any adversity.

DISA is committed to deploying an integrated Multiple Level Secure Voice and Video communications and conferencing capability in direct support of NLCC P/SLC and COOP/COG stakeholder equities and mission sets. This system will utilize new and existing IT infrastructure at all security classification levels in alignment with Department efforts to prioritize C2 through

modernization and consolidation.

Moreover, DISA is currently engineering and deploying a meshed distributed fiber-optic global infrastructure, with enhanced capacity and resiliency, that will deliver the most critical NLCC services to our National Leadership.

I am fully committed to deliver an improved, modernized National Leadership C3 System, to enable the NLCC. The substantial efforts DoD CIO, DISA, the Services, and the other DoD components are being conducted to secure and modernize our NLCC infrastructure.

Cultivate a Digital Workforce

The pivotal achievements and initiatives undertaken by the Department, ranging from user experience enhancements to software and DBS modernization, hinge fundamentally on the presence of a skilled and motivated workforce. Recognizing this critical dependency, we have embarked on a strategic mission to cultivate such a workforce through the implementation of the DoD Cyber Workforce Strategy that is designed to identify and bridge workforce gaps, ensuring that we are prepared to meet the challenges of today and tomorrow. Further amplifying our efforts to secure top talent, the introduction of the Cyber Excepted Service has significantly increased our flexibility in attracting and retaining the specialized skills necessary for our mission's success. Complementing these measures, a comprehensive outreach program has been developed, aimed at drawing in the broad range of abilities needed to fulfill our objectives. Together, these initiatives underscore our commitment to fostering a thriving workforce that can propel the Department towards its goals.

Cyber Workforce Strategy

The DoD Cyber Workforce Strategy, released in March 2023, and its implementation plan released shortly thereafter, remains a top priority for this office. Our goal is to address workforce gaps by recruiting top-tier cyber professionals, prioritizing critical roles and functions to optimize our cyber workforce, and enhancing the skills of our existing talent. This initiative is crucial for safeguarding our digital and critical infrastructures, ensuring they are operated securely to defend against cyber threats and protect our data from adversaries.

Implementing a comprehensive approach involves consistent capability assessment and analysis processes to anticipate force requirements effectively, alongside instituting an enterprise-wide talent management program aimed at aligning force capabilities more closely with present and future needs. This effort also entails cultivating a cultural transformation throughout the Department to enhance personnel management practices on a broader scale and promoting collaboration and partnerships to enrich capability development, operational efficiency, and career advancement opportunities across the organization.

To provide guidance we released the third publication in the DoD Cyber Workforce policy series to set the foundation for managing, identifying, qualifying, and upskilling our workforce according to the DoD Cyber Workforce Framework (DCWF). The manual plays a crucial role in our workforce by setting forth the qualification standards for every DCWF work

role, ensuring that personnel assigned to cyber positions possess the capability to meet mission demands effectively.

Outreach / Development / Retention

Professional development, through education and training, plays a vital role in supporting and enhancing our cyber workforce capabilities. We have several ongoing partnerships and rotation programs to provide professional development opportunities to our workforce.

The Department is working to determine the resource requirements to establish a central program office for cyber academic outreach. This office will oversee cyber-focused engagement programs, enhancing coherence, coordination, and management across the enterprise. Serving as the consolidated focal point for engagements between the department and academic institutions regarding cyber-related matters, its objective is to streamline processes and establish a clear pathway for academic institutions seeking engagement with the DoD.

In accordance with the DISA Workforce 2025 Implementation Plan, DISA is conducting outreach and shaping curricula in partnership with our academic and private industry partners, to strengthen the talent pool with training and education necessary to meet DISA and the DoD's cyber and IT mission. The agency, in collaboration with academia and industry, continues to address gaps in the areas of IT, cybersecurity, engineering, and cloud computing. In doing so, this collaboration fosters knowledge transfer to future workforce candidates of the DoD mission and opportunities available to them, as well as an advanced understanding of key skill areas necessary to be successful in achieving the DoD mission.

CIO also administers the DoD Cyber Service Academy, formerly known as the DoD Cyber Scholarship Program, which grants scholarships to students pursuing cyber-related degrees at designated institutions. Recipients of these scholarships are afforded opportunities for hands-on experience through a DoD internship, providing invaluable exposure to DoD cultures and agencies. This approach not only enhances the qualifications and capabilities of our workforce members but also initiates the clearance process for interns, ensuring that applicants are pre-cleared before commencing full-time employment.

We administer the Office of Personnel Management's Federal Rotational Cyber Workforce Program (FRCWP) for the DoD cyber workforce as well. The FRCWP enables cyber-coded government civilians to hone or develop cyber knowledge and skills through applying for, and serving in, rotational details outside their home agencies across the federal government. Rotations promote intra-agency and interagency knowledge sharing, integration and coordination of cyber practices, functions, and personnel management.

Finally, in furtherance of the Federal government's Tech to Fed initiative, DISA is partnering with private firms to modify the course curriculum to meet DISA and Joint Force Headquarters - Department of Defense Information Network (JFHQ-DODIN) requirements for cyber professionals. DISA and JFHQ-DODIN are providing technical and practical ways for veteran candidates to enroll in cyber related programs to graduate more highly qualified potential future employees for cyber related positions, with an understanding of the critical importance

specific skill areas have in bolstering our national security posture.

Conclusion

This work would not be possible without the oversight and steadfast, seamless support of this subcommittee and our partnership with Congress. I am committed to the mission of ensuring our Nation's continued leadership in the digital landscape and addressing any challenges to our national security. Thank you for the opportunity to testify this morning. I look forward to your questions.