STATEMENT BY

JOHN B. SHERMAN

DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS

ON

"Defense in a Digital Era: Artificial Intelligence, Information Technology, and Securing the Department of Defense"

MARCH 9, 2023

Introduction

Good morning, Chairman Gallagher, Ranking Member Khanna, and distinguished Members of the subcommittee. Thank you for the opportunity to testify before you today. Alongside me is Dr. Craig Martell who is the Chief Digital and Artificial Intelligence Officer (CDAO). We look forward to sharing the current progress on the Department's digital transformation efforts.

Chairman Gallagher, I look forward to working with you and this committee to achieve bold action and strengthen our position in key digital transformation areas in the 118th Congress. The leadership from this committee, through multiple National Defense Authorization Acts (NDAA), has empowered the Department of Defense (DoD) Chief Information Officer (CIO) to manage the Department's information technology (IT) portfolio, including oversight of each of the Military Departments (MILDEPs) and Defense Agency's IT and cybersecurity's budgets. Dr. Martell, the senior official responsible for strengthening and integrating data, artificial intelligence (AI), and digital solutions in the Department and myself work closely to ensure shared missions are met.

Budget certification authorities and the Capability Programming Guidance

In accordance with 10 United States Code (U.S.C) §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 National Defense Strategy 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 five fiscal year budget assessments and determinations, beginning with the Fiscal Year (FY) 20 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.

Cyber Workforce Strategy

We are continuing to develop a workforce capable of operating within the cyber domain, defending against adversaries, and supporting larger, critical CIO initiatives and efforts such as the Joint Warfighter Cloud Capability (JWCC).

A cyber workforce strategy is a priority of this office with a goal of enabling the Department to be able to close workforce gaps while expanding its cyber workforce and developing talent to securely build, operate and maintain its digital and critical infrastructures to protect and defend our data against cyber adversaries.

The recently signed DoD Cyber Workforce Strategy establishes the direction for unified management of the cyber workforce and outlines a roadmap for its advancement.
The strategy outlines four goals: 1) Execute consistent capability assessment and analysis processes to stay ahead of force needs, 2) Establish an enterprise-wide talent management program to better align force capabilities with current and future requirements, 3) Facilitate a cultural shift to optimize Department-wide personnel management activities, and 4) Foster partnerships to enhance capability development, operational effectiveness, and career broadening experiences.

To achieve these goals, we must pursue meaningful actions that reduce the talent pipeline gap, increase the quality and diversity of our cyber workforce, and prioritize professional development.

Our goals align to four key pillars: 1) Identification of needs 2) Recruitment 3) Development, and 4) Retention. First, we need to identify workforce needs and requirements. Second, it is critical we cast a wide net to attract the talent needed to meet these requirements and continually evaluate these efforts. Once the need is identified, and the talent acquired, teams and individuals must be provided the resources to be successful. Finally, incentive programs enable the Department to retain critical talent. We are using these pillars to drive the cultural shift necessary at the Department to ensure our workforce is agile, flexible, and responsive to the changing cyber domain, its threats, and its challenges.

Cyber Workforce Strategy Implementation Plan
We are shaping an agile and innovative implementation plan with clear measures of effectiveness to successfully enhance recruitment and retention of a cyber workforce.

DoD Cyber Workforce Framework Expansion
While the strategy sets the direction for unifying the cyber workforce, the DoD Cyber Workforce Framework (DCWF) provides the foundation for targeted human capital management and establishes a common data model for data-driven decision making. The DCWF has been used across the DoD to advance our understanding of cyber work roles, identify critical needs and gaps, and take action to advance a workforce capable of protecting our nation against ever evolving threats. Given its success the Deputy Secretary of Defense directed the Department to expand the DCWF. Working with the CDAO and Dr. Martell we have included new work roles for artificial intelligence, data and analytics, and software engineering. This expansion shows the utility of the framework methodology. The data driven framework is now used to assess and report on the health of the broader innovation workforce. We will continue expansion efforts to support other critical mission sets.

DoD Manual 8140
DoD Manual 8140 sets the foundation for identifying, qualifying, and upskilling our workforce according to the DCWF. DoD Manual 8140 policy series consists of a directive, instruction, and manual and was published in February of this year.

The manual is critical to our workforce as it establishes the qualification criteria for each DCWF work role to ensure personnel filling cyber positions are capable of meeting mission requirements.

Using the DCWF, the manual enhances interoperability and cyber readiness across the Department by providing a common baseline and understanding of cyber concepts, principles, and applications. The program also provides a continuing professional development mechanism for the Department to ensure the workforce maintains current knowledge and capabilities in the rapidly changing cyber domain.

Through the manual, DoD is expanding the qualification program from a population of less than 90,000 to more than approximately 225,000 military, civilian and contractor positions by establishing foundational and residential qualification criteria for each DCWF work role. Together, the strategy, implementation plan, and 8140 policy series will enable the DoD to develop and deploy an agile, capable, and ready cyber workforce.

Cyber Excepted Service

The DoD Cyber Excepted Service (CES) personnel system was established to ensure that the cyber warfighters are the first positions to be filled by utilizing a wide range of tools and program elements that is unmatched with current competitive service system opportunities. CES works in coordination with the DCWF coding of our workforce.

We are implementing a unique set of tools and programs, such as on-the-spot job offers, pay-setting flexibilities, no time-in-grade requirements, qualified-based promotions, target local market supplements, and advancement and development opportunities to achieve recruitment, retention, and development flexibilities across the Department.

Analytics

Data is key to all our initiatives. We developed an authoritative data analytics platform that provides leadership with enterprise-wide visibility into the cyber workforce using the DCWF work roles. This real-time data aggregation enables DoD leaders to make information-driven decisions to fill gaps through an enhanced way of identifying its workforce mix and conducting a more targeted analysis for fixing recruiting and retention challenges.

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.

We offer the DoD Cyber Scholarship Program (CySP) that provides scholarships to students in pursuit of cyber-related degrees at designated institutions. Each recipient is provided with a DoD internship, giving them hands-on experience and exposure to DoD cultures and agencies. This results in workforce members who are better qualified and better equipped, and it starts the clearance process with interns so that applicants are pre-cleared before beginning full-time work.

In addition, we work with the Centers of Academic Excellence (CAE) program that consists of direct relationships with over 400 universities, colleges, and community colleges with verified curriculum aligned to requirements outlined by the DCWF. CAE students work directly with grant-recipient professors to perform DoD research.

In November 2022, the DoD expanded the cybersecurity workforce by eliminating educational barriers and leveraging registered apprenticeship programs. Removing formal education barriers, combined with the use of apprenticeship programs, provides a faster pipeline to acquire talent, increases talent pool, and enhances diversity by allowing applicants to enter the workforce through nontraditional pathways. Efforts including registered apprenticeship programs enhance our cybersecurity workforce and complement the Administration's focus on diversity, equity, inclusion, and accessibility. Closing the talent gap is critical to strengthen and safeguard our Nation's cybersecurity. Moreover, removing formal education barriers and providing nontraditional skills-based pathways is a step that brings DoD closer to our goal of scaling up a workforce that are critical to mission readiness.

Zero Trust

The DoD has made great strides in establishing a strong foundation for Zero Trust (ZT) adoption and implementation. In January 2022 we established the ZT Portfolio Management Office (ZT PfMO). Last July 2022 we released the ZT Reference Architecture and subsequently, in October 2022, the ZT Strategy and Implementation Roadmap. This document provides strategic guidance, direct alignment of efforts, and prioritize resources for accelerating ZT adoption across the DoD. This includes defining capabilities and activities required to achieve Target Level ZT, which all of DoD must achieve, and Advanced Level ZT, necessary for some systems and data, applications, assets, and services. The DoD ZT PfMO hosted quarterly technical exchange meetings with the MILDEPs, Joint Staff, Unified Combatant Commands (CCMDs), National Security Agency (NSA), and the Office of the Director of National Intelligence, to ensure a clear understanding and alignment of the ZT mission, goals and objectives, and strategy roadmap. The ZT PfMO collaborated and shared updates with the Department of Homeland Security Cybersecurity and Infrastructure Security Agency, NATO, and our international partners to ensure the Federal Government and our allies and partners are moving towards successful adoption and implementation of ZT. DoD is striving to be a leader in the Federal Government on implementing ZT at scale, starting with our most critical networks and systems. With full buy-in from the DoD and its partners, this will be readily achievable.

ZT Pilots and Training Activities

The DoD ZT PfMO will ensure DoD components have the technical options available to implement ZT. The DoD ZT PfMO will initiate a series of ZT pilot scenarios in mid-2023. Additionally, we are working with NSA to develop a Native ZT Cloud which will be a government-owned private cloud designed to achieve more advanced levels of ZT.

The DoD ZT PfMO has been working with the Defense Acquisition University to develop ZT curricula and training courses. Through this collaboration, the DoD ZT PfMO published the DoD ZT Awareness Course on the DoD's Joint Knowledge Online Platform, enabling the DoD's workforce to receive foundational training on ZT. The DoD ZT PfMO is continually developing training curricula, including a Practitioner's Workshop course to upskill the DoD's workforce.

With continued intra-departmental collaboration, the DoD can be a leader in the ZT cultural shift across the Federal Government.

Identity Credential and Access Management

DoD Identity Credential and Access Management (ICAM) efforts provide key foundational support for the implementation of numerous key DoD initiatives to include ZT, Joint All Domain Command and Control (JADC2), and Mission Partner Environment. The Department established an ICAM Executive Board with the objective of empowering decision making to ensure clear direction, messaging, and prioritization of ICAM efforts across DoD. In 2022, the DoD CIO, in coordination with the DoD Comptroller, completed several pilots to see how we can leverage ICAM's capabilities to address access control and segregation of duties of financial systems and fielded several new Enterprise ICAM capabilities. DoD CIO will also require components to implement the enterprise capabilities or leverage a DoD CIO approved ICAM offering if the enterprise capability cannot meet the mission requirement. Defense Information Systems Agency (DISA) and NSA will continue to work together to develop an enterprise ICAM approach for dynamic access, which is a key capability to enable attribute-based access control that relies on user and environmental attributes for access.

Cryptographic Modernization

Cryptographic Modernization is another enduring effort essential to our intelligence, information, and warfighting platforms. The emergence of a viable quantum computing capability increases the risk of our adversaries acquiring this technology to disrupt and compromise our National Security Systems (NSS). 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.

Cybersecurity Maturity Model Certification 2.0

The Department is committed to working with the defense industrial base (DIB) and other stakeholders to achieve our shared objective of protecting national security information. In November 2021, we launched Cybersecurity Maturity Model Certification (CMMC) 2.0 to meet evolving threats and safeguard the information that supports and enables our warfighters, with a simplified approach to compliance. We are currently in the process of codifying the CMMC 2.0 program through the rulemaking process to update the Title 32 of the Code of Federal Regulations (CFR). We will be supporting the Office of the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)), as they lead the effort to update the Defense Federal Acquisition Regulation Supplement (DFARS) through the 48 CFR rulemaking process.

We understand how consequential these changes will be for DIB members whose contracts with the Department that process Controlled Unclassified Information (CUI), and we are especially sensitive to how this program might affect small and medium-size businesses. Our outreach efforts include working with DoD's Office of Small Business Programs, and which is providing resources to small businesses to improve their cyber readiness, others across the Department, to ensure that all potential partners in the DIB and academia understand the

National Institute of Standards and Technology (NIST)-based standards that already contractually apply to those who are handling CUI. We have also had industry roundtables and town halls, where our DoD Deputy CIO for Cybersecurity (DCIO(CS)) discussed how to advance DoD's and industry's shared objectives in cybersecurity risk assessment and management, information sharing, emergency preparedness, incident management, and response coordination. In addition, we continue to expand our programs for assisting industry in understanding and applying the cybersecurity practices necessary to protect themselves and DoD's sensitive information.

Implementing and Integrating Cybersecurity Guidance and Policies

The DoD CIO plays an enterprise oversight and advisory role for cybersecurity across the Department.

Strategic Cybersecurity Program

The USD(A&S) oversees the Strategic Cybersecurity Program (SCP), with an NSA program management office (PMO) performing execution. DoD CIO's role has been supporting USD(A&S) efforts, providing oversight to the NSA SCP PMO, and using CIO budget authorities to ensure components are resourcing for SCP efforts and mitigations and verifying their execution through the cybersecurity budget certification process.

National Security Memorandum-8

DoD is improving the cybersecurity of its NSS following guidance from National Security Memorandum 8, "Improving the Cybersecurity of National Security, DoD, and Intelligence Community Systems," which requires all agencies with NSS to ensure that their systems are upgraded to more rigorous, cybersecurity standards. DoD CIO published Department guidance to incorporate the NSS Checklist into components authoritative inventory tools and categorize each DoD system accordingly.

DoD Risk Management Framework

The updated DoD Instruction 8510.01 "Risk Management Framework (RMF) for DoD Systems," incorporates greater cyberspace accountability for DoD components and information systems by executive program officers, program managers, authorizing officials, and cyberspace and functional operational commanders throughout system lifecycles. It applies an integrated enterprise-wide decision structure for the RMF that includes and integrates DoD mission areas and risk governance process. Finally, it provides guidance on reciprocity of system authorization decisions for the DoD in coordination with other federal agencies to reduce redundant testing, assessing, documenting, and the associated costs in time and resources.

Mitigating Supply Chain Risk for Information and Communication Technology and Services

OMB Memorandum 22-18 Implementation

In implementing EO 14028, the Office of Management and Budget directed in M-22-18 that all Federal agencies seek attestations from software producers about secure software development practices (pending OMB's identification of minimum elements of NIST 800-218) for software in use by agencies that fall within the scope of M-22-18. The DoD CIO is collaborating across the

DoD to meet the various requirements of the memorandum, which will by necessity, require rulemaking for an anticipated Federal Acquisition Regulation, and possible DoD supplement.

Authorities to Exclude and Remove
The DoD CIO is leading the effort to address high-risk information and communication technology vendors by leveraging 10 U.S.C. §3252 and interagency engagement with the Federal Acquisition Security Council.

Implementation of Guidance
To address information and communications technology and services (ICTS) supply chain risk, NIST has updated multiple guides, to include Special Publications 800-53 Rev. 5 "Security and Privacy Controls for Information Systems and Organizations," and 800-161 Rev. 1 "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations." DoD is adopting these updated guides to drive ICTS supply chain considerations into systems designs.

Improving User Experience

The Department must take an enterprise-wide approach to improve user experience and enable the faster delivery of IT capabilities. We are committed to modernizing the digital backbone that supports the warfighter by accelerating the DoD enterprise cloud environment, modernizing business systems, optimizing networks, and buying down technical debt. These efforts will improve user experience by making critical IT infrastructure investments to reduce latency and improve cybersecurity while leveraging cloud for speed, agility, and scalability in support of emerging capabilities and mission readiness.

Accelerate the DoD Enterprise Cloud Environment

Cloud computing remains a fundamental component of the Department's global IT infrastructure and modernization strategy. With battlefield success increasingly relying on digital capabilities, cloud computing provides the IT platform needed to satisfy the warfighter's requirements for rapid access to data, innovative capabilities, and assured support.

Joint Warfighting Cloud Capability
Last December, the Department awarded the Joint Warfighting Cloud Capability (JWCC) fulfilling our commitment to deliver an enterprise-level multi-vendor, multi-cloud ecosystem to address longstanding requirements and capability gaps in support of the warfighter.

JWCC enables mission owners to contract directly with these Cloud Service Providers (CSP) to create a strategic technological advantage on future battlefields at all three classification levels – Unclassified, Secret, and Top Secret. JWCC provides foundational commercial cloud services and capabilities that enable transformational initiatives such as JADC2 and the Artificial Intelligence and Data Accelerator in coordination with CDAO. JWCC allows for streamlined provisioning of cloud services, fortified security, and commercial pricing parity. Features of JWCC include capabilities and parity of services at all three classification levels, integrated cross domain solutions, global availability inclusive of tactical edge locations, and enhanced

Cybersecurity controls. We will guide and ensure that the Department utilizes JWCC to the maximum extent possible.

Outside the Continental United States Cloud
JWCC provides enterprise-level delivery of commercial cloud services and technology from the strategic to the tactical level, to include austere and Outside the Continental United States environments. These CSPs give the Department access to multiple, global fabrics that ensure our warfighters can conduct operations anywhere in the world.

The current crisis in Ukraine and JADC2 experiments are demonstrating the need for rapid extension of enhanced edge computing capabilities globally to reduce network latency, enable advanced data processing such as AI, and improve operational resilience. The DoD CIO, CDAO, and Under Secretary of Defense for Intelligence and Security are engaged with the CCMDs, the MILDEPs, and forward deployed partners to deliver the latest cloud computing and communications technologies to meet these requirements.

Cloud and Data Center Optimization
Through strong partnership with DoD Components our Cloud and Data Center Optimization initiative is enabling the Department to achieve its vision for a more agile and resilient defense posture. We continue to facilitate the modernization of DoD application/systems, close legacy data centers, and prepare to support emerging capabilities. This initiative focuses on the migration of applications/systems from thirteen organizations to more optimal hosting environments and optimizing or closing vulnerable legacy data centers. We have successfully migrated or decommissioned over 760 systems and closed 49 data centers with plans to close 11 additional data centers by FY 2025.

DoD Software Modernization

Last February, we released the Department's Software Modernization Strategy, highlighting the Department's adaptability increasingly relies on software and the ability to deliver secure and resilient software at speed of mission while ensuring software supply chain control. Transforming software delivery times from years to minutes requires significant changes to our processes, policies, workforce, and technology. The Department is preparing to release the Software Modernization Implementation Plan that identifies key FY 2023 and FY 2024 activities, milestones, and responsibilities for driving process improvements and new capabilities to achieve the Software Modernization Strategy goals.

The JWCC award brings us closer to achieving our goal of accelerating the adoption of the Department's enterprise cloud environment, which is a core enabler of our software modernization initiatives, especially the development of Department-wide software factory ecosystem enabling advanced modern software practice such as Development, Security, and Operations (DevSecOps). DevSecOps allows for continuous monitoring of the DoD network and enables us to integrate the cybersecurity and cloud-native technologies into the DoD computing platforms used to integrate software development and system operations for accelerated capability delivery. Our workforce and process transformation are aiming to expand the DoD

CES approach to offer flexibilities for the recruitment, retention, and development of software professional across the Department.

4th Estate Network Optimization

Today's challenges require that we implement a digital enterprise that maintains pace with commercial innovation and delivers IT efficiently. Through 4th Estate Network Optimization (4ENO), the Department is modernizing DoD IT infrastructure and streamlining the digital enterprise. 4ENO converges the 26 networks that the Defense Agencies and Field Activities (DAFAs) independently own, operate, and manage to a single unclassified network domain and a single classified network domain while eliminating redundant networks, and supporting global access that reduces barriers for joint information sharing, strengthens cybersecurity, and improves end user experience.

To date, four DAFAs completed their migration to the Global Service Desk (GSD) and three DAFAs have migrated 700 users across six sites to the new single service network known as DoDNET. This resulted in the consolidation of six legacy networks and a refresh of network hardware. Between FY 2023 and FY 2026, 4ENO aims to migrate an additional 96,000 users from over 470 sites and transfer nearly 800 more FTEs to the GSD. While 4ENO is a long-term effort, it reflects the Department's commitment to enhance efficiencies, modernize capabilities, and improve operational effectiveness.

Defense Business Systems Modernization

DoD must deploy an enterprise approach to deliver modern business capabilities throughout the Department 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 that modern and integrated business processes are in place to support the mission. We are actively working to identify opportunities to consolidate or streamline business functions and data at the enterprise level by improving our processes, enabling data integration, and reducing complex system interfaces. These enhancements will lead to a faster response to mission and provide business data for holistic decision-making. Our enterprise, data-driven Defense Business Systems (DBS) portfolio management approach will drive rationalization across the portfolio to buy-down technical debt, and enhance user experience across the Department, ultimately transforming the way the Department does business.

The Department is committed to managing DBS as a strategic asset. We have successfully transitioned business system responsibilities to DoD CIO, including the annual certification, as the result of the repeal of the Chief Management Officer. The Department will use functional and technical criteria to lead a more data-driven annual certification process per 10 U.S.C §2222 authorities and ensure our DBS portfolio aligns to the strategic priorities and direction of the Department. We are driving to fundamentally transform processes to enable a highly efficient business environment that effectively supports our national defense priorities.

Warfighting Command Control and Communications

Command, Control, and Communications C3 systems are fundamental to all military operations to deliver the critical information necessary to plan, coordinate, and control forces and operations across the full range of Department's missions. DoD CIO is leading the way ahead for future development, implementation, fielding, and sustainment of strategic and tactical C3 capabilities. The critical capabilities in this portfolio are a priority for the enterprise.

Electromagnetic Spectrum

Electromagnetic spectrum (EMS) is important to every DoD mission, in every domain. Spectrum not only provides the critical connective tissue that enables all-domain operations but represents a natural seam and critical vulnerability across Joint Force operations. China and Russia have taken significant steps to challenge U.S. control of the spectrum and seek to exploit U.S. vulnerabilities in the spectrum. Ensuring the U.S. military can train and operate in the spectrum—both at home and abroad—is a strategic imperative.

As the Department's senior official responsible for coordinating across the EMS Enterprise, we are employing and refining our governance processes to ensure synchronization and harmonization of all developments and activities necessary for the successful implementation of the 2020 Electromagnetic Superiority Spectrum Strategy (EMS3). The C3 Leadership Board and the EMS Senior Steering Group has broad participation from stakeholders across the Department, and work to drive towards the EMS3 vision of achieving freedom of action within the EMS at the time, place, and parameters of our choosing while denying the enemy the same.

The Department acknowledges it cannot achieve spectrum superiority without a whole-of-government, whole-of-industry, and whole-of-nation commitment. Accordingly, we also continue robust engagement with our partners in the interagency, industry, and academia to deliver the best spectrum outcomes for the Department and the Nation.

Spectrum Sharing

The DoD supports efforts to ensure U.S. dominance in 5G and next-G development. Previous DoD success in making spectrum available for commercial use through the Advanced Wireless Services -3, Citizens Broadband Radio Service, and America's Mid-Band Initiatives Teams are testaments to this commitment. DoD maintains numerous operational equities throughout the spectrum which must be preserved to enable DoD the ability to protect the homeland, test equipment, train for overseas contingencies and operate in all domains. As I testified during my confirmation hearing before the Senate Armed Services Committee in 2021, "Spectrum sharing must be our watchword going forward" for the U.S. to maintain both its global leadership position and the capabilities of our armed forces.

The Department remains committed to making mid-band spectrum available for industry while meeting our mission requirements. Within the 3100-3450 band, the DoD relies on hundreds of air, sea, and land-based radars for a wide range of missions. It would be untenable for DoD to outright vacate these systems from the parts of the spectrum in which they currently operate. To do so would take decades, cost hundreds of billions of dollars, and cause significant mission impacts to

the Joint Force's warfighting readiness and capabilities.

We continue to make strong progress in the spectrum sharing study of the 3100-3450 band, our as required by the Infrastructure Investment and Jobs Act (IIJA). To inform this study, DoD is coordinating closely with the Department of Commerce and leveraging the technical expertise of government, industry, and academia. We will report our findings to the Department of Commerce by September 2023 as required by the IIJA.

Our efforts build on previous sharing initiatives led by the Department. We are committed to helping maximize U.S. 5G and Next G dominance while also ensuring that the Joint Force can both train and conduct operations in and near the continental U.S. where use of terrestrial, airborne, and sea-based radars operating in the mid-band are critical for success.

5G

The DoD CIO continues to work on 5G through contributions to international standards development organizations, and through participation in the Under Secretary of Defense for Research and Engineering (USD(R&E)) led 5G Cross Functional Team (CFT), to identify and provide implementation guidance for both dual-use commercial and military focused 5G technology applications that provide the optimum return on investment to the Department. Our current focus is on the development of required enterprise capabilities, and associated security policy/infrastructure to support the MILDEPs in their implementation of 5G Information and Communications Technology across all military installations in line with the FY 2023 NDAA. Finally, in accordance with the FY 2021 NDAA, the DoD CIO is preparing to assume leadership of the CFT on October 1, 2023, and will continue to work in close coordination with USD(R&E) and USD(A&S).

Positioning, Navigation, and Timing

The DoD CIO is fully engaged in leading the implementation of the Department's positioning, navigation, and timing (PNT) Strategy to provide robust and resilient PNT for the Joint Force. This is critical to enabling advanced weapon systems to function in today's highly contested navigation warfare environment. Current efforts are focused on modernization of the Global Positioning System (GPS), including acquisition and fielding of GPS M-code equipment, modernized GPS satellites, and the next generation operational control segment. In order to ensure that PNT is accessible to support international U.S. and coalition operations, resilience efforts also concentrate on alternative and complementary capabilities to GPS to provide multi-source PNT in a modular open system approach (MOSA).

To date, the Services accomplishments include the fielding of GPS M-code ground receivers in key systems that include the Army's Mounted Assured PNT System or MAPS which is in the Patriot System, currently in South Korea. The Navy has started fielding the GPS-Based Positioning, Navigation and Timing Service, known as GPNTS, and Non-GPS Aided PNT for Surface Ships or NoGAPSS into the surface fleet. The Air Force is developing the MOSA compliant Resilient Embedded Global Positioning System Inertial Navigation System (REGI) for use in critical DoD aviation platforms. In a joint effort by the Navy and DISA, global timing resiliency is being achieved though the Critical Time Dissemination initiative and Defense Regional Clocks.

Enterprise Satellite Communications Modernization
The DoD is rapidly accelerating its satellite communication (SATCOM) services modernization, with particular focus on our international and commercial partnerships. The Department is nearing the conclusion of a ground teleport sharing arrangement with Australia that will offer both participants increased operational capacity and resiliency. As the Department shifts to a Future SATCOM Force Design, diverse commercial and military services will be blended into a single operational enterprise, achieving more agile and scalable communication transport.

Recently, the Department released its Enterprise SATCOM Management and Control Reference Architecture, Implementation Plan, and SATCOM Terminal Reference Architecture for delivering automated SATCOM resource allocation to the warfighter quickly. We are now implementing a solution that establishes cloud-based enterprise services and secure automated resource allocation across military and commercial SATCOM communication service provided networks.

Following commercial SATCOM industry's lead, we are changing decades old analogue business and operational processes used to allocate SATCOM and creating the necessary rules-based processes to deliver machine-to-machine information flows allowing SATCOM resource allocation in minutes and seconds.

As the Department integrates commercial SATCOM, we must stay focused on protecting our infrastructure and networks from adversarial threats. The Department worked with industry over the past two years and issued the "Information Assurance – Pre" program where commercial solutions are assessed and graded on the ability to protect the Departments information streams.

SAP IT
The Deputy CIO for Special Access Program (SAP) IT is responsible for policy, oversight, and governance of all need to know SAP IT programs and cybersecurity activities across the Department. The office has made significant progress in establishing, enhancing, and maturing SAP IT policy and governance. Working closely with the team in the DISA, we have implemented repeatable and reliable approaches for managing, coordinating, and protecting SAP IT. These efforts include modernization of the legacy stand-alone "Chinstrap" desktop hardware system. The Compartmentalized Enterprise Desktop (CED) is DoD's new cloud-based virtualized desktop. CED installation and Chinstrap decommissioning is underway and is on track to be completed by the end of the month of March 2023.

Conclusion

It would not be possible to continue all this work without the consistent and dedicated support of this subcommittee and partnership with Congress. I am committed and I know Dr. Martell is dedicated in our combined mission of ensuring that our nation continues to be a leader in the digital landscape and combat any challenges to our national security. I look forward to continuing to work with you all. Thank you for the opportunity to testify this morning, I look forward to your questions.