STATEMENT BY

JOHN B. SHERMAN

DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER

LT GEN ROBERT J. SKINNER

DIRECTOR, DISA
COMMANDER, JOINT FORCE HEADQUARTERS-DEPARTMENT OF DEFENSE INFORMATION NETWORK

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 22, 2024

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 Lt Gen Robert Skinner, Director of the Defense Information Systems Agency (DISA) and Commander of Joint Force Headquarters-Department of Defense Information Network. 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. 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.

Lt. Gen. Skinner, who serves in a dual-hatted role, as Director of the DISA and Commander of Joint Force Headquarters-Department of Defense Information Network (JFHQ-DODIN), oversees a global network and leading nearly 19,000 personnel across 42 countries to provide joint, interoperable command and control capabilities and defend enterprise infrastructure in support of various entities including the President and combatant commanders, while also directing unified actions to secure, operate, and defend the Department of Defense' information networks (DoDIN).

Together we provide strategic guidance, oversight, and technical expertise to enable secure warfighting IT capabilities, modernize DoD information networks, enhance Warfighting Command Control and Communications, and cultivate a digital workforce.

Enabling Secure Warfighting IT Capabilities

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

The Department is moving forward on implementing ZT throughout the Defense enterprise and with Allies and Partners. In January 2024, we received implementation plans for each component within the Department and my teams are working hard to help shape, support, and recommend solutions to successfully meet Target Level ZT requirements. These plans included acquisitions, technology, funding, and major milestones.

In 2023, DISA deployed Thunderdome ZT network access capabilities to 15 sites on their classified and unclassified cyber terrain. This supports DISA's DoDNet deployments for Defense Agencies and Field Activities to ensure their common IT infrastructure aligns to ZT architectural principles. In 2024, DISA will accelerate deployment to 60 sites and will also begin to support the U.S. Coast Guard and USSOUTHCOM. In addition to ZT alignment, these deployments are critical to our Department's migration from our legacy Joint Regional Security Stacks (JRSS) capabilities.

DoD ICAM efforts provide foundational support for the implementation of numerous critical DoD initiatives to include ZT, Combined Joint All Domain Command and Control (CJADC2), and Mission Partner Environment (MPE). 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 FY23, DISA launched a self-service portal for customer on-boarding enabling Component systems and applications to leverage ICAM's capabilities to address access control and segregation of duties for financial systems. DoD CIO provided specific guidance on how to adopt enterprise capabilities or leverage a DoD CIO approved ICAM offering if the enterprise capability cannot meet their mission requirements.

Cryptographic Modernization is another enduring effort essential to our intelligence, information, and warfighting platforms. 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 (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.

Securing the Defense Industrial Base

The Department remains committed to collaborating with the defense industrial base (DIB) and other stakeholders to protect our national security information and its own intellectual property. DoD CIO published the Proposed Rule for CMMC in 32 Code of Federal Regulations (CFR) with specific requirements of the Cybersecurity Maturity Model Certification (CMMC) Program and its associated ecosystem to be codified in federal regulation.

The CMMC Program will provide a mechanism for the Department to validate DIB compliance with the implementation of previously established cybersecurity requirements on their unclassified information systems that process, store, or transmit federal contract information (FCI) or controlled unclassified information (CUI). 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 protection.

Departmental outreach efforts, available through the Cyber Crime Center (DC3) and the NSA Cyber Collaboration Center, include robust programs that ease regulatory burdens, particularly for small- and medium-sized businesses. The Office of Small Business Program's (OSBP's) Project Spectrum and the Air Force's Blue Cyber also support small businesses with free consultation on National Institute of Standards and Technology (NIST) Special Publication 800-171 compliance. In collaboration with the NIST Manufacturing Extension Partnership (MEP) and the OSBP's APEX Accelerators programs, DoD is working to ensure small businesses have access to the support they need to remain secure, compliant, and competitive.

Modernize DoD Information Networks

The Department has dedicated considerable effort to enhancing user experiences, expediting the DoD enterprise cloud environment, advancing DoD Software modernization, and refining Defense Business Systems Modernization. These initiatives, coupled with budget certification authorities

and Capability Programming Guidance, underscore the Department's commitment to an enterprise-wide approach that prioritizes user-centric improvements and the swift delivery of IT capabilities. Central to this modernization strategy is the pivotal role of cloud computing within the Department's global IT infrastructure. We have also stood up the Customer Experience Officer (CXO) Portfolio Management Office in CIO specifically to address this challenge. The DoD's Software Modernization Strategy and the creation of the CXO further emphasizes the critical importance of software in adapting to new challenges, highlighting the necessity of delivering secure software quickly to meet mission demands and maintain software supply chain control.

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.

Following our award of the Joint Warfighting Cloud Capability (JWCC) contract in December 2022, DoD Components now have access to commercial cloud computing at all three security classifications, from the headquarters to the tactical edge, which is critical to enabling Combined Joint All-Domain Command and Control (CJADC2) and other important efforts, such as modern software development and artificial intelligence. In the first year of execution, the team was focused on helping Mission Partners through the acquisition process and adopt JWCC. To date, JWCC has awarded more than 47 Task Orders. We published guidance for the use of JWCC and cloud rationalization to streamline cloud contracting and reduce contract sprawl across the Department.

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 (OCONUS) environments. Working with Cloud Service Providers (CSPs), the Department now has access to multiple, global fabrics that ensure our warfighters can conduct operations anywhere in the world. Additionally, DISA has expanded Stratus Private Cloud to OCONUS to enable hybrid cloud deployments overseas.

The current crisis in Ukraine and CJADC2 experiments demonstrate 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 Combatant Commands (CCMD), the MILDEPs, and forward deployed partners to deliver the latest cloud computing and communications technologies to meet these requirements.

In the last 12 months, the DoD CIO, in partnership with DISA, successfully deployed the initial OCONUS commercial cloud capability in support of INDOPACOM missions. This OCONUS cloud capability will establish the OCONUS portion of the global, resilient, and secure information environment that supports the National Defense Strategy's (NDS) top priorities. Specifically, the OCONUS cloud enables warfighting and mission command, resulting in improved agility, greater lethality, and improved decision-making at all levels.

The Department continues to accelerate the use of fit-for-purpose cloud capabilities to meet mission requirements, including capabilities in the classified environment. DoD continues its partnership with the Federal Risk and Authorization Management Program (FedRAMP) in the use of commercial CSPs at the moderate or Impact Level 2. Beyond Impact Level 2, the Department provisionally authorized more than 50 cloud service offerings for use with CUI, NSS, or classified data, the results which can be leveraged by mission owners DOD-wide to accelerate cloud capability adoption.

Through strong partnership with DoD Components our Cloud and Data Center Optimization initiative enables the Department to achieve 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.

DoD Software Modernization

The Department's Software Modernization Strategy highlights our ability to adapt 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 released the Software Modernization Implementation Plan in March 2023, identifying key activities, milestones, and responsibilities for driving process improvements and new capabilities to achieve the Software Modernization Strategy goals.

The Command & Control Software Factory (C2SF) became DISA's first accredited Development, Security, and Operations (DevSecOps) platform on the NIPR and SIPR Commercial Cloud Fabrics. To date, C2SF has onboarded over 1000 users across 10 PMO's, facilitating large enterprise programs through their complicated modernizations. C2SF has transformed the way our programs partner with industry to deliver modern capabilities to the warfighter. C2 software development teams can vet their new products incrementally every sprint as a tenant inside the DISA managed environment. The teams are provided real-time security & functional vetting of their products, as well as an integration region mutually accessible by the DISA JITC testers and Government cyber authorities. The software releases performed inside the factory track with the DoD Risk Management Framework.

The Department continues to accelerate the adoption of the Department's enterprise cloud environment through enterprise cloud contracts such as JWCC, which is a core enabler of our software modernization initiatives, the expansion of the software factory ecosystem enables advanced modern software practice such as DevSecOps. DevSecOps allows for continuous

delivery of software capability while monitoring for any changes in security 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 change the DoD approach to offer flexibilities for the recruitment, retention, and development of software professionals across the Department and give them an ecosystem like what they would find in industry to deliver the capabilities we need in DoD. The Department is more than halfway through the FY23-24 Software Modernization Implementation Plan and is beginning development of the follow-on plan for FY25-26.

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 identify modernization and drive rationalization across the portfolio to transform the way the Department does business.

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.

The DISA Business Systems Portfolio has embarked on a multi-year modernization effort to align the portfolio with the tenets of the Business Enterprise Architecture (BEA), initially focusing on alignment to the Procure to Pay (P2P), Budget to Report (B2R) and Order to Cash (O2C) processes and will expand to additional processes in the coming years. Additionally, as DISA modernizes DISA Storefront, DISA is reinvigorating it's focus on the User Interface and User Experience (UI/UX), to provide a more streamlined, customer friendly experience when ordering services. DISA's modernization efforts with the modernized DISA Storefront have already succeeded in the processing of $1.2B in FY24 customer Defense Information Systems Network-Integrated Services (DISN-IS) and Organizational Messaging Service (OMS) subscription services payments.

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 six fiscal year (FY) budget assessments and determinations, beginning with the 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.

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. This leadership is exemplified through initiatives such as the Global Command and Control System, ensuring unfettered access to the Electromagnetic Spectrum, pioneering advanced Electromagnetic Battle Management strategies, 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.

Global Command and Control System – Joint (GCCS-J)

DISA's GCCS-J program continues to support the warfighter by providing situational awareness in all areas of responsibilities across enemy and Blue Force locations, GCCS-J is a primary data integrator supporting Joint Fires modernization, Global Integrated Operations, and data synchronization with Mission Partners. GCCS-J is at the forefront of designing the enterprise COP data model which fuses intelligence objects with the DoD sight picture in support of CJADC2's data driven decision making philosophy.

Electromagnetic Spectrum

Spectrum is vital to our national security and essential to mission effectiveness. Aligned with the National Spectrum Strategy, we understand the increasing federal and commercial demand for spectrum; at the same time, it is critical that we preserve the military's access to spectrum required for the capabilities it needs to defend the Nation. We are working with the White House, the Department of Commerce, other interagency partners, and industry to explore ways to do that without jeopardizing national security.

The Department relies on hundreds of air, sea, and land-based radars for a wide range of missions. Turning on the news you can see how this mid-band spectrum is vital to DoD. Commercial vessels operating in the Red Sea have been attacked by drone-launched and ballistic missiles originating from Houthi rebels in Yemen. Currently, U.S. Navy warships are subject to drone attacks, respond to the commercial vessel distress calls, and shoot down drones, utilizing the very spectrum at risk of being less available to defense users.

Spectrum provides the critical connective tissue to that enable all-domain operations and 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.

Spectrum Sharing

We are laser focused on developing a technology that will allow for dynamic, large-scale spectrum sharing, which poses a significant engineering challenge but is achievable for the nation. We partner across industry, government, and academia to drive forward viable next steps to safeguard domestic military radar to safeguard military capabilities and sharing options.

As the Department's senior official responsible for coordinating across the Electromagnetic Spectrum (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 DoD supports efforts to ensure U.S. dominance in 5G and next-G development. Previous DoD success in making spectrum available for shared commercial use, including the ground-breaking Citizens Broadband Radio Service, are testaments to this enduring 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.

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.

Electromagnetic Battle Management (EMBM)

Developing robust EMBM capabilities is a key objective in the DoD's 2020 EMS Superiority Strategy to monitor, identify, characterize, and adapt to the operational environment, while providing dynamic control of real-time operations in the EMS via machine-machine and human-machine collaboration. DISA, in partnership with USSTRATCOM, is developing EMBM Joint (EMBM-J) which is a suite of web-based applications, systems and data management services that work together to gather and arrange electromagnetic spectrum, or EMS, data into a comprehensive visual display to generate command, control, and communications information.

Robust EMBM capabilities require complete and accurate data to meet CJADC2 and current Spectrum Superiority objectives. The legacy enterprise EMS IT systems (e.g., DISA's Global Electromagnetic Spectrum Information System) designed for capturing, producing, and provisioning data require modernization to meet evolving EMBM and CJADC2 objectives. DISA is working with DoD CIO and mission partners to resource the modernization of data capture and EMS resource management tooling.

5G

The DoD CIO assumed leadership of the 5G mission and the 5G Cross-Functional Team (5G CFT) on October 1, 2023, in accordance with the FY 2021 NDAA. In this role, CIO is focused on guidance, fielding and implementation of mature 5G capabilities to 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. 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 FY23 NDAA, advancing enterprise capabilities and associated security policy and infrastructure, and addressing resourcing requirements to support the MILDEPs in their implementation of 5G information and communications technology on installations and in tactical and expeditionary use cases.

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. 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. 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.

Enterprise Satellite Communications Modernization

As the Department increases the diversity of the SATCOM systems it uses, we must recognize and address the expanded infrastructure and networks which we must protect from adversarial threats. The DoD CIO works to ensure appropriate monitoring and protections are in-place through our Cyber Security Directorate and by continuous coordination with the NSA, with USCYBERCOM and DISA, and with the Space Force.

The DoD is rapidly accelerating its satellite communication (SATCOM) services modernization, with particular focus on our international and commercial partnerships. We issued CPG for the

development of hybrid terminals capable of operating in multi-band, multi-waveform, and multi-orbital service offerings to enable heavier integration of commercial SATCOM services. The DoD CIO is assisting the Space Force, in conjunction with all the Services, in identifying the total resources required over the balance of the current decade to properly operate and sustain our existing capabilities, including the ground infrastructure which DISA manages, and the Services operate, as well as resource the transition to the more diverse capabilities of the Broadband portion of the Future Space Data Network Force Design.

The US Space Force working with DISA has begun the implementation of the Enterprise Satellite Communications Management and Control (ESC-MC) Reference Architecture; they are coordinating closely on the implementation and on hosting the resulting services within the JWCC to optimize security as well as enabling authorized access. Their focus will result in an initial roll-out of capability during FY 2025. The implementation requires 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.

National Leadership Command Capability

I want to emphasize a capability at the forefront of the Department's highest priority missions. This three-part capability is the National Leadership Command Capability (NLCC), comprised of 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 Congress and the President, utilize C3 systems that provide common capabilities used across operational environments. 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 to provide direct support to the NC3 community. This system will utilize existing IT infrastructure at all security classification levels in alignment with Department efforts to prioritize command and control thru modernization and consolidation.

I am fully committed to deliver an improved, modernized National Leadership C3 System, to meet the needs of all NLCC customers. The substantial efforts DoD CIO, DISA, the Services, and the other DoD components are conducting 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 defense business systems 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 diverse 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 in August 2023, remains a top priority for this office. Our goal is to address workforce gaps by recruiting top-tier cyber professionals, expanding 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.

Cyber Excepted Service

The Department appreciates Congress' recognition of the need for increased flexibilities in attracting, hiring, and retaining quality cyber personnel. Section 1599f of Title 10, U.S. Code, authorized the Cyber Excepted Service (CES) personnel system for civilians supporting the U.S. Cyber Command, providing pay flexibilities to mitigate recruitment and retention challenges. The CES features a mission-focused occupational structure, qualification-based professional development, and advancement opportunities without time-in-grade requirements, along with agile recruitment and retention strategies, recruitment incentives, and market-based compensation.

The Cyber Workforce Health Report is designed to provide leadership with enterprise-wide insights into the cyber workforce through the lens of DCWF work roles, enabling them to identify workforce gaps and address recruiting and retention challenges more strategically and quickly. This platform reports on the state of the civilian and military cyber workforce, manage the CES Targeted Local Market Supplement (TLMS) incentive and provide local commanders with a means of identifying and mitigating workforce health challenges before they impact mission readiness.

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 of Defense 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 DISA and DOD mission and opportunities available to them, as well as an advanced understanding of key skill areas necessary to be successful in achieving the DISA and DOD mission.

CIO also administers the DoD Cyber Service Academy, formerly known as the DoD Cyber Scholarship Program (DoD CySP), 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 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

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 and Lt Gen Skinner 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.