STATEMENT BY

JOHN SHERMAN

DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER, Acting

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS

ON

" Department of Defense Information Technology, Cybersecurity, and Information Assurance for Fiscal Year 2022"

JUNE 29, 2021

NOT FOR PUBLICATION UNTIL

RELEASED BY THE HOUSE ARMED SERVICES COMMITTEE

Introduction

Good afternoon Mr. Chairman, Ranking Member, and distinguished Members of the Subcommittee. Thank you for this opportunity to testify before the Subcommittee today on the current efforts underway pertaining to the Department's information technology (IT) and cybersecurity. I am John Sherman, the Acting, Department of Defense (DoD) Chief Information Officer (CIO).

As you know, the DoD CIO serves as the principal advisor to the Secretary of Defense for information management; IT; cybersecurity; communications; positioning, navigation, and timing (PNT); spectrum management; senior leadership communications; and command, control, and communications (C3) matters. This portfolio is unlike that of most CIOs in both scope and scale. During this time of transition, we have made it a priority to maintain the momentum in transforming the foundations of the Department's digital capabilities, while innovating at scale to bring new initiatives, such as Zero Trust (ZT) and DevSecOps, into wide scale use across the Department. This is essential to support both our forward deployed forces and global capabilities that our nation's adversaries have shown the will and capability to target. These efforts are focused by the President's Interim National Security Strategic Guidance and the Secretary's Message to the Force priorities memo.

The DoD CIO coordinates on a daily basis directly with the DoD Principal Cyber Advisor (PCA), U.S. Cyber Command, the Joint Staff J6 counterparts at the Military Departments (MILDEP), and various Defense Agencies and Field Activities (DAFA) at leadership and staff levels. Additionally, the CIO holds a bi-weekly meeting of MILDEP CIO principals to coordinate initiatives, and a monthly meeting of DAFA CIO principals to achieve the same goal.

The DoD CIO annual budget review and certification authority, in accordance with section 142 of Title 10, United States Code, as amended by the National Defense Authorization Act for Fiscal Year 2018, provides a critical avenue for a more strategic and methodical approach to prioritize resources toward capability requirements within the areas I am responsible for. To ensure a clear, manageable and repeatable scope for the review of the proposed DoD budget, my office issues annual programming guidance to the DoD Components identifying the investments of focus for the CIO assessment of their fiscal year budget, consistent with the National Defense Strategy and Defense Planning Guidance, for strengthening and accelerating the modernization of the Department's IT and Cybersecurity digital capabilities. Components are asked to build their budgets consistent with the CIO guidance, and as part of the Department's broader budget guidance and deliberations. My office assesses their budget submissions against our priorities and the guidance. DoD CIO has successfully completed three fiscal year budget assessments and determinations beginning with the FY 2020 President's Budget. The Department is making consistent progress toward increasing the focus and priority toward transforming the foundations of the Department's digital capabilities, which I will discuss in more detail today. I recognize that not all priorities can be satisfied in each budget, so part of the certification process is to identify areas where the budget is adequate but still present some risk to transforming the Department's digital capabilities. Focus for future budget certifications will continue to be these modernization efforts, working with the Military Departments and other DoD Components to address areas of concern in future budgets.

The DoD FY 2022 Information Technology/Cyberspace Activities (IT/CA) Budget Request is $50.6B, including $12B in cyber/ classified IT/CA investments and $38.6B in unclassified IT investments. The FY 2022 request reflects an overall 4% increase from the DoD FY 2021 enacted IT/CA Budget.

Today I would like to speak to you on a number of critical initiatives that exemplify the key elements of the Department's effort to transform and innovate in support of the warfighter globally. First, I'd like to discuss our activities in the areas of cloud computing, software modernization and network optimization. Second, I'll provide a brief assessment of our cybersecurity posture and discuss key initiatives including ZT, the Strategic Cybersecurity Program (SCP), Risk Management Framework (RMF), and Industrial Control Systems (ICS). I will provide an update to earlier testimony on initiatives related to the Department's Cyber Workforce as well. Then I'd like to discuss critical initiatives in the Department's ongoing effort to develop a more resilient PNT capability to support warfighting in degraded environments, spectrum sharing, our work on 5G, and updates to leadership communications. Finally, I'd like to provide you a brief overview of the actions underway to make data a strategic asset and increase its availability for leaders across the Department, from the boardroom to the battlefield.

Cloud-Enabled Warfighting

Cloud computing is 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.

The Department continues its commitment to cloud computing with the $1.48 billion total FY22 budget representing a 10% increase in cloud investments from the prior year. This growth includes continued investment in cloud services (infrastructure, platform, and software), application and system migrations, and additional cybersecurity measures to protect DoD data in the cloud. Progress includes DAFA cloud and data center optimization reform with 90% of planned migrations and closures expected by 4QFY21 and the remaining to complete in FY22 for a total of 926 systems migrated or decommissioned and 42 data centers closed. While making progress, work remains to drive accelerated modernization and adoption. In addition to the 10% growth in the FY22 budget, the Department continues to require double-digit growth in the future years to maintain this momentum.

The Department remains committed in its drive toward a multi-vendor, multi-cloud ecosystem with FY22 cloud investments representing over 50 different commercial vendors, including commercial cloud service providers, and system integrators. With the ongoing delays associated with the JEDI enterprise cloud contract acquisition, optimizing the Department's cloud acquisitions remains challenging. However, centralized cloud contracts issued by MILDEPs and the enterprise-level milCloud 2.0 contract help fill the gaps and provide a more streamlined and cost-effective approach to DoD cloud adoption.

Software Modernization

The Department continues to learn from its modernization efforts and to gain a better understanding of the IT requirements for the future battlespace. Based on this understanding, the Department is focused on Software Modernization, an initiative that builds upon cloud with the vision of delivering resilient software capability at the speed of relevance. Extending the cloud with capabilities such as DevSecOps and enterprise services, and incorporating a focus on delivering cyber resilient systems, Software Modernization provides for the full integration of technology, process, and people needed to deliver next-generation capabilities.

The FY22 budget includes investments to enable Software Modernization with cloud services as the foundation. As one example, the Air Force's Platform One provides multi-tenant capabilities to critical weapon and business systems that include the F-35 fighter, the Advanced Battle Management System, and the B-21 bomber. Platform One's latest demonstration was the edge deployment of Artificial Intelligence/Machine Learning (AI/ML) capability to the U-2 reconnaissance aircraft in just 12 days. The Department will continue to place emphasis on Software Modernization with the publication of a strategy later this summer, building on DoD DevSecOps guidance already developed and early implementation success of that guidance by the Military Departments.

Network Modernization

Today's joint warfighter requires a globally-accessible and adaptable network infrastructure that provides resilient data transport in real-time across Service, operational domain, and security classification boundaries to joint, allied, and other mission partners. We must have the ability to rapidly collect, analyze, and share information from multiple tactical, operational and strategic locations and make decisions in real time.

In response to the COVID-19 pandemic crisis, the Department rapidly deployed Commercial Virtual Remote (CVR) a commercial based collaboration capability to enable the remote work force and lessen the demands on the Department's networks. CVR, intended as an interim measure until a more secure and enduring platform was deployed, was decommissioned on June 15. The Department recently implemented DoD365, a platform that represents a more secure collaboration environment and more comprehensive integrated suite of office productivity tools (Email and MS Office). The DoD365 planning and deployment efforts were led by the DoD CIO and CDR, USCYBERCOM. Informed by limited deployment and cybersecurity testing, the initial capability provides users with Direct Internet Access through a Web Browser into the DoD365 environment. The intent is to increase capability over the next 12 months with Components developing and testing solutions to deliver managed and unmanaged Bring Your Own Approved Device with internet based access to DoD365. To date, the initial deployment of DoD365 has reached nearly ~2.2 m users of the targeted ~2.8m user base.

Cloud access and remote work introduces a significant burden to the DoD networks. To counter that demand, DoD365 enables Direct Internet Access through a web browser now and is working to incrementally deliver direct internet access on managed and unmanaged mobile and desktop devices. During the COVID-19 pandemic the Department was able to sustain day to day

operations by greatly expanding the VPN capacity and by providing a large number of additional VPN services.

Additional modernization efforts underway or planned will reduce the number of network connections needed at any given Base/Post/Camp/Station by optimizing to an all-Internet Protocol (IP) infrastructure that can be virtualized for specific mission needs and cybersecurity protection. The Department's network modernization efforts will deliver greatly enhanced bandwidth capacity and increase network resiliency to enable advanced warfighting initiatives. It will also support the use of DoD-wide services and consolidation of critical IT systems, applications, and services from local installations to core data centers and the DoD enterprise cloud environment. To this end, the Department is conducting experiments with industry partners to determine how they can help DoD enhance the resilience and performance of its IT infrastructure. These experiments will also identify ways to improve base and wide-area connectivity required to meet the increased network demands resulting from operations in the Commercial Cloud.

Tomorrow's war fighter will require the ability to collect and fuse information in new ways and make that information available instantaneously across geographically-separated forces spanning the strategic to tactical levels of combat. In spite of the enterprise infrastructure successes, more needs to be done to eliminate vulnerable network systems, implement mandated Internet Protocol version 6 (IPv6) capabilities for next generation network management, and establish resilient, high speed capabilities to support Joint All Domain Command and Control (JADC2) and cloud access at DoD locations.

The Department's many network modernization efforts will provide the ability to fully harness the cloud and compute capabilities, as well as establish an efficient and effective information technology environment.

Cybersecurity

The cybersecurity posture of the Department is a complex quantity to assess. The Department of Defense Information Network (DoDIN) is a massive infrastructure supporting multifarious missions each having a range of threat actors, and consequences of failure. At the same time both the technologies comprising the DODIN and the capabilities of threat actors is evolving at an ever increasing rate.

In this complex and dynamic context, any posture assessment must look at risks across the current fight and into the future across the spectrum of conflict. In this regard, the Department has established powerful cyber defensive technologies and operational capabilities that have proven capable in the past, and appear capable in the present fight; however, with ever decreasing margins. It is the context of the future fight that it is most challenging to assess. As we pivot from counter terrorism to near peer competition the risks increase, as they do for every war fighting capability.

It is clear, that for the future fight, the steps being taken in technology and operations will be fully sufficient for the low-tier threat actors of tomorrow while their margin against near-peer competitors will remain slim and uncertain. The steps being taken by DoD, for instance, to

achieve ZT across all mission capabilities of the DoDIN, the modernization of DoD cryptography, and to operationalize defensive cyber operations are in the large placing DoD in the right posture for future conflict. The success of these programs and their ability to maintain critical margins depend on resourcing decisions made across the Future Years Defense Program (FYDP).

The Secretary previously discussed the Department's investment in cybersecurity and cyberspace operations to maintain the momentum of the Digital Modernization Strategy. Expanding on those comments, the Department's ZT framework assumes that the DoDIN is compromised, and employs existing and emerging cyber defense capabilities to derive a data, applications, and systems-centric security model that "denies by default." The $5.6B FY22 DoD Cybersecurity budget maintains enhanced funding levels established in FY20 and FY21 for key enterprise cybersecurity capabilities, including Identity, Credential, and Access Management (ICAM); endpoint security, including comply to connect (C2C) and Automated Continuous Endpoint Monitoring (ACEM); and User Activity Monitoring (UAM) have enabled DoD to begin to implement the ZT framework across the DODIN.

New investments to our IT and cybersecurity infrastructure will also be necessary to achieve a robust implementation of ZT. Some examples include software defined environments, continuous multi-factor authentication, micro-segmentation, artificial intelligence/machine learning (AI/ML), and user behavior monitoring. Once fully implemented, the DoD ZT framework will provide a new hardened architecture for the DoDIN which will significantly enhance resiliency and cyber defenses, requiring the adversary to invest considerable offensive resources to gain exceedingly limited access, if any at all, to data and resources.

Risk management will continue to be a key pillar of the DoD security program, and the DoD Risk Management Framework (RMF) assessment and authorization process ensures the Department designs, evaluates and monitors IT system compliance with ever improving security requirements. The DoD is starting to implement the Continuous Authority to Operate (cATO) within its Risk Management Framework to ensure that the IT systems connected to DoD's networks maintain the appropriate level of cybersecurity controls in light of a dynamic cyber threat environment. cATO allows us to continually monitor and respond to changes in the risk in our systems much faster. This results in fielding capabilities quicker for our warfighters, but also allows the Department to respond to the constantly changing cyber threats that we are facing.

As we look to further manage risk, DoD is working to mature the Strategic Cybersecurity Program (SCP) that addresses the requirements of the FY 2018 NDAA Section 1640 and FY 2021 NDAA Section 1712 to ensure that the DoD is always able to conduct the most important military mission of the Department. It is achieving these requirements through close collaboration of DoD CIO, USD(A&S), NSA and the DoD PCA. The DoD is undertaking pathfinders for twelve critical fielded systems. DoD will apply a seven step process that performs mission-based, threat informed risk reduction planning through a focus on the mission impacts of system vulnerabilities and the ability for adversaries to exploit them.

Encryption and Cross Domain Solutions (CDS), foundational cybersecurity capabilities, continue to be a high priority for the DoD. Building on enhancements in FY20 and FY21, the Department

continued to increase investment in cryptographic modernization by funding next generation cryptographic algorithm development. Additionally, the Department has continued sustaining investment in CDS modernization, driving implementation of the CDS Raise the Bar (RTB) strategy.

Industrial Control Systems (ICS) has been a frequently overlooked technology across the government and industry. As the lead for control systems cybersecurity, DOD CIO is working hard to address risks in these systems. The Department has clarified that ICS is covered under our cybersecurity program and the cybersecurity standards that we have for traditional systems apply to control systems. We have published guidance to help ICS systems implement cybersecurity programs. Additionally, the Department is working to build cybersecurity expertise in our Cyber Workforce and are developing capabilities to monitor ICS systems. This is a tough problem that requires the DoD CIO to work with new partners. We are working with the National Institute of Standards and Technology (NIST) and the Cybersecurity and Infrastructure Security Agency (CISA) to develop cybersecurity standards for these technologies. We are strengthening our working relationships with the mission and system owners for these system to help them understand the threats and risks; and develop mitigations. The cyber vulnerability assessments the Department conducted of Defense Critical Infrastructure in response to FY2017 NDAA, Section 1650, have helped identify the nature of cyber vulnerabilities that are associated with our most important critical infrastructure. We have a significant amount of work left to do, but we've implemented many of the foundational principles and are moving to maturing our practices and capabilities.

Defining the Cyber Workforce

The Secretary discussed the importance of developing a diverse workforce that draws on "the full range of talent that the United States has to offer." Nowhere is this truer than in cyberspace. The Department must continue to modernize our approach to recruit, retain, and maintain Cyber Workforce talent. In the modern cyber environment, the race to recruit and retain the most innovative individuals with high-demand skillsets is a top priority for government and industry leaders alike. Emerging cyber talent are faced with an abundance of employment opportunities across the private sector where lucrative incentives are available to those with high-demand skillsets. To maintain a viable cyber-talent pipeline, the DoD CIO is focused on a strategy and key initiatives to attract these workers while encouraging increased diversity. The CIO is developing seven key initiatives to advance the Cyber Workforce.

First is the 8140 Policy Series to facilitate strategic Cyber Workforce management activities. This series will drive implementation of the vision for a robust and trained workforce necessary to meet our current and future cyber challenges. These policies accomplish this goal by providing a targeted, role-based approach to identify, develop and qualify cyber personnel leveraging the Defense Cyber Workforce Framework (DCWF).

Second is the Cyber Excepted Service (CES) mission-focused personnel system that supports the human capital lifecycle for civilian employees engaged in or in support of cyber-related missions. This program offers flexibilities for the recruitment, retention and development of cyber professionals across DoD. CES applies to ~9,000 civilian positions with ~6,500 positions converted to the program. CES includes a monetary compensation tool called the Targeted Local

Market Supplement (TLMS). It is used to incentivize critical work role coded positions that are faced with excessive vacancy and attrition rates. TLMS functions similarly to Locality Pay, where a predetermined percentage of pay is added to an employee's base pay, though the TLMS is scoped to work role coded positions and not occupational series or localities. This feature helps DoD be more competitive with industries and agencies hiring individuals with similar skill sets.

The third initiative is our ongoing series of Zero-Based Reviews (ZBR) of the workforce as required by section 1652 of the FY 2020 NDAA, which tasked DoD components to conduct a ZBR of cyber and IT positions. This review includes providing resource, technological, and funding information, as well as providing recommendations to improve capability and resource efficiencies. The DoD Tri-Chair (DoD CIO, PCA, and OSD P&R) created a funded course of action (COA) to accomplish the review that scoped down the level of effort while keeping with the intent of the congressional requirement. The Marine Corps was the first component to initiate the ZBR (phase 1), while the remaining components have recently initiated their efforts (phase 2). A ZBR interim update to Congress on initial observations from the Marine Corps will be provided in the coming days.

Fourth is an initiative we are calling Cyber 101, which utilizes the DC3 Cyber Training Academy to develop training to provide DoD personnel with a foundational understanding of the six common core knowledge, skills, and abilities (KSAs) required for each of the 54 DCWF work roles. This program will establish foundational cyberspace training to assist Components/Services in qualifying the workforce to DCWF positions and standards of DoD Manual 8140 "Cyberspace Workforce Qualification & Management Program."

Fifth, the DoD CIO has a goal to develop tools to assess cyber aptitude and differentiate/predict current employees and potential candidates' abilities or skills to perform cyberspace work. Aptitude testing enhances DoD's recruitment ability by identifying individual potential while predicting performance, behavior, and attrition. This will allow the Department's current Cyber Workforce to keep pace with technology trends and reskill the non-Cyber workforce to close mission critical cyber skill gaps. The DoD CIO partnered with Army Research Institute (ARI) to broaden validation efforts for the Common Cyber Capabilities (C3) Test. This partnership is enabling the DoD to leverage ongoing work to deliver a government-owned solution for use with personnel across the four Military Services. The DoD CIO was able to fund roughly $500K for this initiative in FY21, however additional funding is required to first, maintain current delivery and second, ensure the Department can leverage a viable platform for administration of the assessment planned through FY22.

The sixth initiative uses the Advanced Analytics platform known as ADVANA to better understand the workforce. We are developing a series of interactive dashboards through the platform to enable flexible, transparent and meaningful analysis of DoD's Cyber Workforce. These Cyber Workforce dashboards will merge data pulled from authoritative manpower and personnel systems and generate the real-time data required for managing the civilian Cyber Workforce. This initiative will use the data gathered from the Services and Components to enable the generation of a suite of Key Performance Indicators (KPIs) as well as real-time trend and predictive analysis.

The final initiative is the Cyber Workforce Strategy, our team in DoD CIO, in conjunction with colleagues in USD(P&R), will publish a new Cyber Workforce strategy by March 2022. The workforce strategy will shape the future Cyber Workforce to incorporate emerging technologies (AI, Data, Control Systems, and Machine Learning) and provide an authoritative foundation for digital workforce talent management. In order to ensure future workforce development capabilities, the DoD Cyber Workforce Strategy will increase diversity by expanding how talent is acquired and leverage developmental and educational programs. Our focus will be on innovative and creative personnel practices to increase entry level opportunities while adopting flexible retention models. The intent is to provide alternatives to the traditional 30-year career.

Command, Control, and Communications

Command, Control and Communications (C3) is part of the DoD CIO portfolio that makes the office unique and differentiates it from a civilian CIO position. While all divisions in the CIO, and aspects of the Digital Modernization Strategy, support warfighting, it is C3 that is most closely linked to the warfighter on the ground, sea and airspace. The critical capabilities in this portfolio are a priority for the enterprise.

The PNT enterprise is an essential contributor to cybersecurity and a critical element for any advanced weapon system to operate effectively in today's competitive environment. As the Secretary noted in his posture hearing, "modernization of all segments of GPS [Global Positioning System] to ensure precision and availability" is a priority for the Department. The investment that the Department requested in the FY22 budget will enable our progress in this area. It will fund GPS, including related "M-Code" modernization in DoD platforms/systems, as well as other complementary and alternative resilient PNT capability efforts. The Department understands the reality that while GPS remains the revolutionary cornerstone for worldwide PNT services to the Joint Force, it has increasingly become a target for disruption and denial by adversaries. Accordingly, the Department has been developing alternatives and complements for fielding in order to increase resiliency and survivability of the force. The Implementation Plan (I-Plan) for these PNT capabilities and applications addresses the FY 2021 NDAA Section 1611, *Resilient and Survivable PNT Capabilities*.

DoD CIO is also the Department's lead for the Electromagnetic Spectrum Enterprise (EMSE) and the designated senior official for the long-term implementation of the 2020 Spectrum Superiority Strategy. This strategy includes five high-level goals that will drive policy harmonization, I-Plan and workforce oversight, and enterprise governance. In accordance with the strategy, the Electromagnetic Spectrum Operations (EMSO) Cross Functional Team (CFT) developed an Electromagnetic Spectrum Superiority Strategy (EMSSS) I-Plan. Our team in DoD CIO will assume the EMSSS I-plan oversight from the EMSO CFT, in keeping with my role as the Principal Staff Assistant (PSA) for EMS and EMSE, subsequent to the Secretary's approval of the I-plan.

DoD continues to work with interagency partners to make available mid-band spectrum to support U.S. leadership in 5G. The Department has already made available the 3450-3650 MHz band for 5G and, under the new Emerging Mid-Band Radar Spectrum Sharing (EMBRSS) effort,

has already begun the process of assessing the feasibility of sharing the 3100-3450 MHz band. DoD cannot vacate the 3100-3450 MHz band without significant mission and operational impact; however, the Department is studying opportunities and procedures to share this critical national resource. DoD will be assessing different courses of action based on different sharing frameworks that inform the Administration, federal regulators, and DoD senior leadership decision on the best way forward.

During his recent testimony, the Chairman spoke of a vision of future warfighters using "local and expeditionary 5G networks" to gain and maintain an information advantage in conflicts though connected sensors and weapons in resilient battlefield networks. We in the DoD CIO continue to work with USD(R&E) on a variety of 5G pilots to advance this vision for the future. These pilots explore the use of 5G technology in the areas that include standards, security, networks, and spectrum. Additionally, we're actively participating in the USD(R&E) CFT, which will transition leadership of 5G initiatives to us in CIO by 2024.

Finally, leadership communications in a denied, disrupted, intermittent and limited (DDIL) environment is of paramount importance during competition, crisis and conflict. To this end we have placed great emphasis on preparing to provide our leaders with the right information at the right time under all conditions. The FY22 budget includes $14.5M to continue the Pentagon and Raven Rock Information Technology Modernization efforts. This year we continue to modernize and update the locations' network access points and active directory as well as consolidate and modernize the servers that support multiple networks at both locations.

Data

Data is the ammunition of the future. Under Secretary Austin's leadership, the Department has prioritized ensuring the timely, secure, and resilient access to data that enables advanced warfighting capabilities needed for military advantage in all-domain operations. While data management is not directly tied to specified program elements in the FY22 budget request, we are identifying, assessing, and tracking our data-related investments as part of the budget certification process that I lead. The Department must measure, manage, and modernize its data assets to create new operational advantages and remain effective against near-peer competitors. Becoming a data-centric organization is a top priority for DoD.

The Department is aggressively implementing the actions described in the recent DoD Data Strategy and the Deputy Secretary's recent guidance entitled "Creating a Data Advantage." The Data Strategy provides a clear vision, principals, objectives, and focus areas for data management. We need to make DoD data visible, accessible, understandable, linked, trusted, interoperable and secure. The recent guidance from the Deputy Secretary helps accelerate this transition by via a series of five "Data Decrees" to guide the force in the transition to an open data standard architecture and strategic use of data.

Last fall, the CDO established a Data Council composed of all the Department's data leaders, and he also meets regularly with data leaders from across the Combatant Commands, our interagency teammates, and our "Five Eyes" (FVEY) partners. The CDO's office has also established key data related policies, guidelines, and processes on topics such as data cataloging, sharing and protection.

The DoD is implementing the ability to use live data to inform senior leader decision-making. Forums such as the Deputies Management Action Group (DMAG) now use data-driven analytics and metrics to track progress on all the Department's top priorities. The signal from the top, including frequent emphasis by the Vice Chairman, is that all organizations need to provide, manage, and share decision-quality data. Components are getting the message and treating data as a resource.

Similarly, the warfighting community is collaborating to solve the interoperability challenges posed by Joint All Domain Operations and new operational concepts. CDO is partnering with Combatant Commanders, Services, Joint Staff, and international partners to enable JADC2 and provide the warfighter with data whenever and wherever needed. This shift to a data-centric approach is urgent, underway, and already leaving a lasting impact on the Department.

Conclusion

I'd like to note the importance of our coordination and partnership with Congress in all of these areas and many others. Today we have discussed key initiatives in the areas of cloud enabled warfighting, software and network modernization, cybersecurity, the Department's Cyber Workforce, C3 and data. I look forward to continuing to work with Congress through the authorization and appropriation process and beyond as we continue to evolve to maintain the Department's information advantage. Thank you for the opportunity to testify this afternoon, and I look forward to your questions.