STATEMENT BY

JOHN B. SHERMAN

DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER

DEPARTMENT OF DEFENSE CHIEF DIGITAL AND ARTIFICIAL INTELLIGENCE 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 2023"

May 18, 2022

NOT FOR PUBLICATION UNTIL

RELEASED BY THE HOUSE ARMED SERVICES COMMITTEE

Introduction

Good morning Chairman Langevin, Ranking Member Banks, and distinguished Members of the Subcommittee. Thank you for the opportunity to testify before you today. Alongside me is Dr. Kelly Fletcher, the Principal Deputy Chief Information Officer and Ms. Margie Palmieri who is the Deputy Chief Digital and Artificial Intelligence Officer (CDAO). We look forward to sharing the Department's ongoing efforts with regard to information technology (IT), cybersecurity, command, control and communications (C3), and artificial intelligence (AI).

Before I begin, Chairman Langevin, I would like to thank you for your 22 years of serving our nation in Congress, our women and men in uniform, and the civilian workforce at the Department of Defense. Under your leadership, cyber issues have moved from the fringes to the forefront of our national security landscape. I look forward to working with you and this Committee to achieve bold action and strengthen our position in these key areas as you complete your term in the 117th Congress.

I appear before you today as the now-confirmed DoD Chief Information Officer (DoD CIO), and as the Acting CDAO. I serve 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 C3 matters. Additionally, the leadership from this Committee, through multiple National Defense Authorization Acts, has empowered the DoD CIO to manage the Department's information technology portfolio, including oversight of each of the Military Department and Defense Agencies IT and cybersecurity's budgets.

We are excited about the establishment of the CDAO. The Department has made significant strides to unlock the power of its data, harness AI, and provide digital solutions for the Joint Force. As we face China as a pacing threat, an increasingly aggressive Russia, and as our adversaries adapt to technological innovation, it is clear to us that there is a need for stronger alignment and synchronization to accelerate decision advantage and generate advanced capabilities for our warfighters.

The CDAO will work closely with DoD CIO and other components within the Department to ensure it meets its intended mission of serving as the Department's senior official responsible for strengthening and integrating data, AI, and digital solutions in the Department. While the DoD CIO will continue to lead on core infrastructure, including cybersecurity, cloud, transport, and networks, the CDAO will help set requirements and provide policy and guidance for the data, analytics, and adoption of mature AI. Since February 1 of this year, the CDAO has been operating in an initial operating capability (IOC) and will reach full operating capability (FOC) by June 1.

Budget certification authorities

In accordance with section 142 of Title 10, United States Code (U.S.C), the DoD CIO annually executes its budget and certification authority. Annual programming guidance is provided to components ensuring a clear, manageable, and repeatable process to review the proposed components budgets for those 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. With this guidance, and in conjunction with the Department's broader budget guidance, the components are able to build their budgets, which are then assessed against the priorities identified in our guidance. The DoD CIO successfully completed four fiscal year budget assessments and determinations, beginning with the FY20 President's Budget. The certification review process identifies capability areas where modernization may be at risk. We then work with the Military Departments and other components to address these risks areas in future budgets.

The DoD FY 2023 information technology/cyberspace activities (IT/CA) budget request is $58B, including $12.8B in cyber/classified IT/CA investments and $45.2B in unclassified IT investments. The FY 2023 request reflects an overall increase of 2.5% from the DoD FY 2022 enacted IT/CA budget.

Defining the Cyber Workforce

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. To address the numerous workforce challenges DoD faces, we must take a unified and coordinated approach that takes meaningful action to reduce the talent pipeline gap, increase the quality and diversity of our cyber workforce, and prioritize the personal and professional needs of our cyber practitioners. The DoD CIO is currently in the process of developing the DoD CIO Cyber Workforce Strategic Action Plan (CWSAP) in response to these identified challenges. The CWSAP is derived from the DoD Cyber Strategy and provides specific actions to be taken to remediate shared challenges impacting the Department.

The first initiative is the update and maintenance of the DoD Cyber Workforce Framework (DCWF). The DCWF describes the extent of cyber work performed by the DoD. We developed the DCWF to enhance the interoperability of cyber forces within the Department and with foreign and domestic partners. Leveraging the framework, we began coordination with partners from the newly established CDAO and in the office of the Undersecretary for Acquisition and Sustainment (USD(A&S)). This collaboration will expand the framework to include a broader range of AI, machine learning, data science, and advanced software development work roles.

Second, we are leading the development of the 8140 Policy Series to facilitate cyber workforce management activities. These policies provide the structure for a standardized, role-based approach to identify, track, and report on the Department's cyber workforce leveraging the DCWF. The forthcoming manual in this series will provide guidance for role-based qualification and continued development of the subject workforce.

The third initiative 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, meeting statutory criteria in section 1599f of Title 10, U.S.C, offers flexibilities for the recruitment, retention, and development of cyber professionals across the Department. The ability to employ monetary tools such as the Targeted Local Market Supplement (TLMS) is crucial to the program's ongoing success. Since approval of the TLMS in

FY21, the TLMS has reduced attrition rates in targeted work roles from eight percent to three percent. To fully leverage the flexibilities afforded in the CES Personnel System the Department approved a validation process for non-CES components to petition for inclusion. The process requires non-CES components to conduct a position-by-position review for determining a "qualified position".

Fourth is the Emerging Technologies Talent Marketplace (ETM). In FY21, our team in DoD CIO provided CES organizations access to the AI-enabled ETM platform, which contains a broad Federal Occupational Database with position classification standards and assigned DCWF work role codes. ETM serves as an open talent marketplace with a candidate-centric design, focusing on the needs, objectives, and point of view of the diverse and sought-after cyber talent the Department needs. Further, ETM expedites position classification and leverages alternate talent resources outside of USAJobs to streamline the recruitment, hiring and onboarding processes.

The fifth initiative is our ongoing Zero-Based Review of the cyber and IT workforce required by section 1652 of the FY20 NDAA. The review yielded invaluable data to support workforce planning for readiness and retention. The final congressional report, for which we're on track to deliver by June 2022, will detail the key strategic findings from participating stakeholders and outline a repeatable process for future workforce reviews.

The sixth initiative leverages DoD's authoritative data analytics platform, Advana, to drive enhanced visibility of the cyber workforce and deliver analytic capabilities. We are spearheading the development of interactive cyber workforce dashboards through Advana to enable adaptable, transparent, and meaningful analysis of the Department's cyber workforce. These dashboards merge data from authoritative manpower and personnel systems and enables the generation of a suite of Key Performance Indicators for vacancy rates, recruitment, retention, and development. Additionally, Advana is generating the Cyber Workforce Health Report (CWHR) which provides leadership an enterprise-wide visibility into the workforce along with planned expansion to include the military. This capability will bring efficiency in generating actionable data for decision-making, improved data quality, and user-friendly, self-service visualizations that allows users to interpret and evaluate data specific to their mission needs.

The final initiative is an array of developmental programs intended to provide prospective and current cyber talent an avenue to explore diverse jobs during their career. This includes opportunities to gain valuable industry experience through participation in programs like the Cyber and Information Technology Exchange Program or the Cyber Talent Initiative. Similarly, we will kick off a Cyber Workforce Rotation Program in May, allowing participants an opportunity to work in other CES organizations. We also offer a retention scholarship under the Cyber Scholarship Program and we are working to build a partnership program with the Department of Labor and the Department of Veterans Affairs. Lastly, we continue to pursue cyber aptitude assessment capabilities to differentiate and predict current employees and potential candidates' abilities or skills to perform work in or in support of the cyberspace domain.

Zero Trust

The DoD has made great strides in establishing a strong foundation for Zero Trust (ZT) adoption and implementation. In 2021, the Department accomplished numerous foundational tasks, to include the publication of the DoD ZT Reference Architecture (ZT RA) v. 1.0, the submission of the DoD's initial response plan to Executive Order 14028, and the analysis of the DoD CIO's first data call for ZT. On January 31, 2022 the DoD formally established the DoD ZT Portfolio Management Office (ZT PfMO) to provide strategic guidance, direct alignment of efforts, and prioritize resources for accelerating ZT adoption across the DoD. The ZT PfMO hosts a quarterly technical exchange meeting with the Military Departments, Joint Staff, CCMDs, National Security Agency and the office of the Director of National Intelligence, to provide a clear understanding of the ZT mission, its goals and objectives, and its strategy roadmap. Through sharing insights, exchanging ideas, strengthening partnerships, and refining practical implementation across the DoD, the office energizes the grassroots level around this new opportunity to improve DoD's cybersecurity. ZT adoption can be successful only with full buy-in from all of DoD. DoD is striving to be a leader in the federal government on implementing ZT at scale, starting with our most critical networks and systems.

Strategy, and the ZT Reference Architecture

The DoD will release its initial strategy for ZT around July 2022. The strategy will promote interoperability and specify requirements without being overly prescriptive. This approach will allow each component in DoD to implement ZT capabilities in the way that is most appropriate for its particular needs, while still maintaining compliance with issued guidance—namely, the ZT RA. ZT RA focuses specifically on data-centric security designs, conditional access, and segmentation of critical assets.

Cybersecurity Maturity Model Certification 2.0/DIB Cybersecurity

The Department is committed to working with the defense industrial base (DIB) and other stakeholders to protect national security information. Last November, we launched Cybersecurity Maturity Model Certification (CMMC) 2.0 to enhance DIB cybersecurity to meet evolving threats and safeguard the information that supports and enables our warfighters. Other internal efforts include working with DoD's Office of Small Business Programs, and across the Department, to ensure that standards are understood by all potential partners in the DIB and academia. DoD also partners externally with the Department of Homeland Security (DHS). Industry outreach efforts include cybersecurity roundtables and townhalls, where our DCIO for Cybersecurity 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. We understand how consequential these changes will be for DIB members whose contracts with the Department include Controlled Unclassified Information, and we're especially sensitive to how this program might affect small and medium-size businesses.

The DCIO for Cybersecurity oversees programs to protect the Department's critical infrastructure against advanced persistent threats and by coordinating cybersecurity standards, policies, and procedures with other federal agencies, coalition partners, and industry.

Strategic Cybersecurity Program

Led by USD(A&S) and with strong support from our team in DoD CIO and our partners in NSA, Principal Cyber Advisor, and Joint Staff, the DoD Strategic Cybersecurity Program (SCP) is entering its second year of system evaluations and mitigations to identify and assess critical vulnerabilities. Ultimately, these efforts ensure that the Department's weapon systems will succeed in a cyber-contested environment against a near-peer adversary. Senior oversight boards have begun to review program's mitigation plans for critical vulnerabilities. SCP's ability to provide platform owners continuous intelligence on the evolving threat environment throughout system life cycles, in addition to a snapshot risk assessment, will help to ensure that our warfighters have cyber-resilient systems. Using this methodology and in accordance with legislation and operational priorities, we have prioritized the DoD's key warfighting platforms and weapon systems to evaluate.

Improving Cybersecurity Posture (E.O. 14028)

DoD is executing compliance with Executive Order 14028, "Improving the Nation's Cybersecurity." These tasks include the DoD's publishing its ZT architecture plan and formalizing its agreement with DHS to exchange each agency's incident response orders. DoD is improving the cybersecurity of its national security systems (NSS) following guidance from National Security Memorandum 8, "Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems," that requires all agencies with NSS to ensure that their systems are upgraded to more rigorous, cybersecurity standards. These efforts will improve both DoD and the NSS cybersecurity across the entire federal government.

Software Modernization

Compute

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.

The Department continues its commitment to cloud computing, and we saw a 19 percent increase in cloud spend from FY21 to FY22. This growth includes continued investment in cloud capabilities for infrastructure, platform, and software as a service, including the Department's transition to DoD365, which is the culmination of a multi-year effort to ensure the Department's unclassified e-mail, voice, video, and chat communication tools are best of breed.

The Department remains committed in its drive toward a multi-vendor, multi-cloud ecosystem in line with the Digital Modernization Strategy. Following our cancellation of the Joint Enterprise Defense Infrastructure enterprise cloud acquisition last year, we launched the Joint Warfighting Cloud Capability as our principal cloud contract to enable the transformational activities of Joint All Domain Command and Control (JADC2) and AI and Data Acceleration (ADA). The acquisition began in 2021 and will provide unmet enterprise cloud capabilities at three classification levels: unclassified, secret, and top secret, along with providing the ability to bring cloud computing to the tactical edge. We issued a direct solicitation to four major cloud service

providers (CSPs): Microsoft, Oracle, Amazon Web Services (AWS), and Google, and are currently reviewing the proposals received from the CSPs to ensure they meet DoD requirements, with a planned award date of December 2022. We thought that we could have made the awards in April 2022 but as we reviewed the proposals, we realized that we needed more time to ensure we conducted all the necessary due diligence with the four vendors. I've personally told the team that while we need to move with a sense of urgency, we also need to get this right and to take the time to perform all the key tasks in the procurement.

Collaboration Capabilities

The DoD365(IL5) cloud environment solution replaced the Department's temporary rapid response of Commercial Virtual Remote, the commercial based collaboration capability in 2022 that enabled the remote workforce during COVID-19. DoD365(IL5) provides a more secure and enduring platform, a comprehensive integrated office suite, and collaboration tools with additional capabilities, including managed/unmanaged devices, being assessed for full scale implementation.

The Department is working towards a DoD365(IL6) environment by reaching across DoD to gain an understanding of requirements and applications. The proposed approach is the establishment of a single, joint DoD365(IL6) tenant. The Department is analyzing and conducting testing to determine whether a single O365 tenant can support multiple components and their specific requirements. With successful completion of analysis and testing efforts, migration into the DoD356(IL6) environment is expected to begin in FY23. We're focusing our initial efforts on IL6 with CCMDs and Defense Agencies and Field Activities (DAFA). We're working closely with the Military Departments on how and when they might proceed with this capability.

The Department's transition into the cloud, and more specifically the DoD365 environment, is a journey with our industry partners. Collectively, we are working to identify, prioritize, and address capability gaps to improve the user's experience, enhance cybersecurity protections, and increase collaboration within the DoD and with mission partners.

As the DoD increasingly relies on software, the ability to securely and rapidly deliver resilient software capability is a competitive advantage that will define future conflicts. To that end, the Deputy Secretary of Defense (DSD) signed the Software Modernization Strategy in February 2022. This joint effort led by the DoD CIO, USD for Research and Engineering (USD(R&E)) and USD(A&S) aims to achieve three major goals: accelerate the DoD enterprise cloud environment, establish a department-wide software factory ecosystem, and transform processes to enable resilience and speed. In the coming months, the Department will release an implementation plan that will outline the initiatives underway to achieve these three strategic goals.

Warfighting C3

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 the lifeblood of operations and is critical to all warfighter domains, especially as the Department ensures the Joint Force is prepared to operate against peer and near-peer challengers in a highly-contested environment. As the Department's lead for the Electromagnetic Spectrum Enterprise (EMSE), we are providing oversight and governance to ensure the long-term implementation of the 2020 Electromagnetic Spectrum Superiority Strategy (EMS3). DoD CIO reformed its governance structure and realigned the C3 Leadership Board and the EMS Senior Steering Group to support enterprise-wide stakeholder engagement. These bodies provide governance, oversight, strategic direction, prioritization, policy execution, and resourcing recommendations that are necessary to ensure successful implementation of the EMS3. Current active participation reflects a strong consensus that an enterprise-wide approach is needed to realize the EMS3 vision of achieving true freedom of action within the EMS, at the time, place, and parameters of our choosing while denying the enemy the same. Through these efforts we will be fully positioned to fulfill our obligation as the Principal Staff Assistant (PSA) for the EMS and the EMSE.

Spectrum Sharing

The Department is committed to making mid-band spectrum available while meeting our mission requirements. The Infrastructure Investment and Jobs Act (P.L. 117-58) authorized $50 million for DoD to conduct a sharing study of the 3100-3450 MHz band to enable an auction by the Federal Communications Commission (FCC) in late 2024. Our Emerging Mid-Band Radar Spectrum Sharing (EMBRSS) effort will provide viable options for how this spectrum can be shared by August 2023. DoD is focused on sharing this spectrum as vacating the 3100-3450 MHz band would significantly impact mission and operations.

DoD is confident that the band can be shared. We have a long track record of reaching shared solutions that work for the nation without compromising our mission demonstrated by the 3450-3550 MHz band that was auctioned for 5G earlier this year. 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 United States where use of terrestrial, airborne, and sea-based radars operating in the mid-band are critical for success.

Advancing innovative spectrum sharing technologies and frameworks is critical as we continue to fulfill the objectives of the EMS3 and our work to advance DoD's JADC2 initiative. Key to this is connecting the battlefield, 5G and other emerging technologies.

5G

The DoD CIO continues to work with USD(R&E) on a variety of 5G test programs which explore dynamic spectrum sharing, augmented training, security, and operational support. In accordance with section 224 of the FY21 NDAA the DoD CIO is preparing to assume leadership of the 5G Cross Functional Team (CFT) led by USD(R&E) and continue to work in coordination with USD(A&S). Our current focus is determining the value and prioritization of potential functional applications; developing the optimum underpinning governance; and assessing

centralized versus federated network implementations. In addition, the Department is identifying the necessary enterprise infrastructure and resources and applying the necessary policy and enforcements to ensure the security of 5G telecommunication networks.

Positioning, Navigation, and Timing

Resilient and survivable PNT is critical to enabling advanced weapon systems to function in today's highly-contested navigation warfare environment. The PNT enterprise incorporates modernization of all segments of Global Positioning System (GPS) and its integration with complementary capabilities to ensure PNT continuity throughout mission execution. The DoD CIO is fully engaged in leading implementation of our DoD PNT Strategy to provide resilient PNT for the Joint Force. The FY23 budget funds GPS modernization, including acquisition and fielding of M-code GPS equipment, and modernized GPS satellites and next generation control segment capabilities. It will also advance the Department's efforts to develop and field alternative, multi-source PNT capabilities in flexible, affordable PNT applications to ensure resilient and survivable PNT is available to support worldwide coalition operations by the U.S. and our allies. Both elements are essential to our continuing military success, as our adversaries have studied the role GPS plays as the cornerstone for PNT service to the Joint Force, and they target it in attempting to achieve an asymmetric advantage over the United States. Consequently, a full range of multi-source PNT capabilities is necessary to complement GPS and enable enhanced resiliency and survivability for all military operations.

Commercial Satellite Communications

The DoD recognizes that commercial SATCOM communication (SATCOM) services, particularly those offering high-throughput and non-geostationary orbit capabilities, are altering the use of the space domain. These technologies enable the use of applications that were previously limited to terrestrial networking.

These technologies offer unique opportunities in warfighting applications and an increased resilience and flexibility in our DoD SATCOM enterprise, it is imperative that that DoD retain the necessary degree of protection and interoperability to meet future operational and JADC2 requirements. The Department is working closely with the USSF and commercial industry to digitally modernize the DoD's SATCOM enterprise to make this possible.

The Department is implementing an Enterprise Management and Control (EM&C) solution architecture that establishes cloud-based enterprise services and secure, resource allocation across military and commercial SATCOM communication service provided networks. The Department is in the final stages of developing a digitally system engineered Terminal Reference Architecture to help industry build to terminal specifications and standards that meet EM&C and other DoD security protocols.

To ensure the protection of the Department's NSS that may rely on these hybrid, integrated SATCOM communication networks, the Department is working closely with the USSF on a program known as Infrastructure Assessment Pre (IA-PRE). IA-PRE will make it easier for the Department to leverage the use of commercially owned and operated network management systems by publishing and certifying a pre-approved list of commercial provided services that meet a defined set of cybersecurity and other risk management protocols. Throughout all these

processes, DoD CIO is also working closely with USSF and the Military Departments to ensure requirements are incorporated into the SATCOM way-ahead.

SAP IT

The newly established Special Access Program (SAP) IT office within DoD CIO establishes, enhances, and matures SAP IT policy and governance. Working closely with the team in the Defense Information and Systems Agency (DISA), this office is implementing repeatable and reliable approaches for managing, coordinating, and protecting SAP IT. These efforts include Chinstrap modernization, help desk responsiveness, reliable and secure infrastructure with federated solutions, and enabling SAP/Compartmented Access Program (SAP/CAP) co-mingling efforts. The Compartmentalized Enterprise Desktop (CED), is DoD's new cloud-based, virtualized desktop, developed by the DISA Compartmented Enterprise Services Office in support of DoD SAP users. CED is replacing the legacy "Chinstrap" desktop hardware system. CED installation and Chinstrap decommissioning is underway and will be completed by the end of June 2022. By moving from traditional, individually configured desktop computers to CED's cloud-based desktops, we are able to provide a more reliable and secure operating environment for the DoD SAP user community.

CDAO

Over the past few years, the Department has made significant strides in applying data, analytics, AI, and digital solutions to inform decisions from the boardroom to the battlefield. Such actions are essential for the Department to retain decision advantage relative to our pacing challenge, China. Department-wide responsibilities on digital and AI were divided across several organizations, to include the OUSD(R&E), Advancing Analytics, or Advana platform, Chief Data Officer (CDO), Defense Digital Services (DDS), and the Joint AI Center (JAIC).

At this stage in the Department's digital maturation, there is a clear opportunity for stronger alignment and synchronization to accelerate decision advantage and generate advanced capabilities for our warfighters. In December 2021, the DSD established a CDAO who will serve as the Department's senior official responsible for strengthening the integration of data and AI functions across the Defense enterprise. Transitioning and integrating CDO, JAIC, DDS, and Advana into CDAO is a multi-step process that began on February 1, 2022, when CDAO organization achieved its IOC and will be complete prior to CDAO reaching FOC on June 1, 2022.

The principal purpose for creating a CDAO is to elevate the importance of the issue set to the Secretary, Deputy Secretary, and other PSAs while also ensuring unity of mission and strategic alignment in the Department's enterprise-level data, analytics, digital solution, and AI efforts.

CDAO will achieve this mission by performing several critical functions:

- Lead and oversee DoD's strategy development and policy formulation for data, analytics, and AI;

- Break down barriers to data and AI adoption within appropriate DoD institutional processes;
- Create enabling digital infrastructure and services that support components' development and deployment of data, analytics, AI, and digital-enabled solutions;
- Selectively scale proven digital and Al-enabled solutions for enterprise and joint use cases; and
- Provide a sophisticated cadre of technical experts that serve as a de facto data and digital response force able to address urgent crises and emerging challenges with state of the art digital solutions.

CDAO will perform these functions in close collaboration with USD(A&S), USD(R&E), DoD CIO, Joint Staff, Military Departments, and other digital leaders. CDAO will also need to work closely with industry, interagency, and international mission partners.

Our planning has incorporated extensive feedback from a wide-range of stakeholders internal to the Department, including the Under Secretaries, Military Departments, Joint Staff, CCMDs, and DAFA. It also reflects input from numerous external stakeholders in Congress, academia, and industry.

The CDAO's form follows function. It reflects the leadership the Department needs to accelerate its progress in harnessing information within a rapidly changing technology landscape. Moreover, a top priority is to tap the unique strengths of the CDAO's component organizations while creating greater performance from the sum of their parts.

The CDAO budget is fully informed by the President's vision, policies, and strategies, including the Interim National Security Strategic Guidance and the National Defense Strategy.

Ultimately, the value of creating a CDAO is about empowering the warfighter. Going fast requires a focused effort with clear priorities. The CDAO will have an immediate impact by providing several concrete deliverables this year.

First, CDAO will review and more tightly integrate the Department's policy, strategy, and governance of data, analytics, and AI. This will include an integrated data, analytics and AI adoption strategy as well as further establishing a Responsible AI Ecosystem.

Second, CDAO will provide the enterprise-level infrastructure and services that enable efforts to advance adoption of data, analytics, and AI. This will include an expanded and more accessible enterprise data repository and data catalogue, including designated authoritative data sources, and common data models for enterprise and joint use cases, as well associated coding and algorithms to serve as a public good as Department stakeholders put data on the offensive.

Third, CDAO will solve and scale enterprise and joint use cases. This will include executive analytics to measure progress on implementation of the National Defense Strategy, a common operational picture for Combatant Commanders from the operational to the strategic level as part of the ADA initiative, and better tools and analytics to assist the Department's senior leaders and Combatant Commanders with dynamic campaigning.

This is an ambitious effort but we are well on our way. The urgency of the situation means we cannot afford to slow delivery while we constitute the CDAO.

AI and Data Acceleration Initiative

In June 2021, the DSD launched the ADA initiative. ADA is a three-year effort (FY22-24) to accelerate the deployment of data-enabled automation platforms and development capabilities to each CCMD. It is designed to transform how CCMDs conduct globally-integrated data management, including both warfighting and business decision analytics, and provide a data foundation to enable workflow and C2 automation capabilities.

ADA is a campaign of learning to identify data and JADC2 operational needs, discover obstacles to implementation of modern capabilities, and develop joint solutions. Following discovery, ADA will seek to build the people and partnerships to solve data, process, and infrastructure challenges at scale. ADA will accomplish this via onsite data personnel to augment CCMD capabilities, access to AI experts to deploy tailored process solutions, deep reach back to DoD enterprise services, and close integration with the JADC2 experimentation community.

ADA seeks to learn fast and scale outcomes broadly. As effective solutions are developed in one CCMD, they will be made available across the enterprise for further development and implementation. ADA is not solely focused on capability delivery, but designed to address both materiel and non-materiel challenges to data management. Discovery efforts across a range of capability areas including workforce development, acquisition practices, software modernization, IT infrastructure, and outdated processes are included. The ADA team will provide recommendations to the CDAO, JADC2 partners, and other governance bodies as appropriate.

The CDAO leads ADA with support from USD(R&E), OUSD Intelligence and Security, DoD CIO, and JADC2 CFT.

DoD is already experiencing real benefits from ADA contributions, specifically in response to the crisis in Ukraine, whereby ADA elements at the Joint Staff, USEUCOM, and USTRANSCOM, are providing data, AI, and digitally-enabled insights and enhancements on areas like U.S. force deployments into USEUCOM and refugee flows into Eastern Europe.

Acquisitions

CDAO is posturing the Department to support four critical needs: AI expertise, joint synchronization, agile contracting, and stronger relationships with industry and academia.

The CDAO is offering the DoD a suite of five innovative, decentralized procurement vehicles that allow for rapid AI delivery and purchasing of key AI services and enabling tools.

1. The T&E Blanket Purchase Agreement (BPA) Request for Proposal offers multiple-award BPAs for rapid orders of conflict-of-interest-free T&E and independent verification and validation services in line with responsible AI development practices. This offering was released in February 2021 and is currently available throughout DoD.

2. The Data Readiness for AI Development (DRAID) Blanket Ordering Agreement allows for the rapid ordering of data services to address common DoD data issues, and allow for components to become "AI Ready." DRAID was released at the end of March 2021 and is currently available throughout DoD.

3. Tradewind leverages an Other Transaction Authority or OTA to quickly and repeatedly identify, acquire, and operationalize critical AI technologies from traditional and non-traditional DoD partners. Tradewind and its supporting business process guides DoD through the AI-tailored agile delivery process, from ideation to transition. Tradewind is available throughout DoD and has successfully awarded contracts to multiple services and components.

4. The TryAI Commercial Solutions Opening is a merit-based, competitive, bid-selection model used by federal contracting officers to acquire innovative commercial items through AI demonstrations.

5. The AI Talent BPA provides highly qualified AI advisory and assistance support through multiple-award BPA's, so DoD customers can procure these advisory and assistance services with the necessary skills and experience to achieve their unique AI goals. The AI Talent Contract Support vehicle was released in September 2020 through the Air Force and is currently available throughout DoD.

Conclusion

It would not be possible to continue all of this work in both the DoD CIO and CDAO portfolios without the consistent and dedicated support of this Subcommittee and partnership with Congress. I am committed and I know each of my colleagues here are dedicated in our combined mission of ensuring that our nation continues to be a leader in these areas and we are able to effectively maneuver 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, we look forward to your questions.