STATEMENT OF
DR. CRAIG MARTELL, CHIEF DIGITAL AND ARTIFICIAL INTELLIGENCE
OFFICER

REGARDING
HOW FEDERAL AGENCIES ARE HARNESSING ARTIFICIAL
INTELLIGENCE

BEFORE THE
HOUSE OVERSIGHT COMMITTEE ON CYBERSECURITY, INFORMATION
TECHNOLOGY, AND GOVERNMENT INNOVATION
SEPTEMBER 14, 2023

CHIEF DIGITAL AND ARTIFICIAL INTELLIGENCE OFFICER
Statement for the Record
House Oversight Committee
Subcommittee on Cybersecurity, Information Technology, and Government Innovation
September 14, 2023

Chairwoman Mace, Ranking Member Connolly, and distinguished Members of the Subcommittee, thank you for the opportunity to testify before you today. I look forward to sharing the ongoing efforts of the Chief Digital and Artificial Intelligence Office (CDAO) and the broader Department of Defense (DoD) related to the responsible use of data, analytics, and artificial intelligence (AI)-enabled technologies to accomplish our mission of national defense.

DoD Chief Digital & Artificial Intelligence Office

The Deputy Secretary of Defense (DSD) established CDAO in December 2021, bringing together the authorities and resources of previously separate DoD organizations, including the DoD Chief Data Officer (CDO), Joint Artificial Intelligence Center (JAIC), Defense Digital Service, and Advancing Analytics Office.

In February 2022, DSD charged CDAO with the mission of ensuring DoD becomes a digital and AI-enabled enterprise capable of operating at the speed and scale necessary to preserve military advantage. This includes the following functions:

- Lead and oversee DoD's strategy development and policy formulation for data, analytics, and AI
- Work to 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 AI-enabled solutions for enterprise and joint use cases
- Surge digital services for rapid response to crises and emergent challenges

The National Defense Strategy identifies four top-level defense priorities DoD will pursue: defending the homeland, paced to the growing multi-domain threat posed by China; deterring strategic attacks against the United States, allies, and partners; deterring aggression while being prepared to prevail in conflict when necessary; and building a resilient joint force and defense ecosystem. Data, analytics, and AI play a role in all of these priorities. They are core capabilities underpinning DoD's operational and business analysis and decision-making in support of the Secretary of Defense's priorities to Defend the Nation, Take Care of Our People, and Succeed Through Teamwork. To that end, CDAO aligned on five strategic initiatives focused on using data, analytics, and AI to advance DoD's priorities:

- Improved Data Quality
- Business Performance Metrics
- AI Scaffolding

- Combined Joint All-Domain Command and Control (CJADC2) Data Integration Layer
- Digital Talent Management

Additionally, a 2021 DSD Memorandum recommitted to implementing Responsible AI, specifically outlining Responsible, Equitable, Traceable, Reliable, and Governable as ethical guiding principles for the design, development, deployment, and use of AI capabilities.

Improved Data Quality

Quality data is CDAO's foundational priority. We are focused on improving the quality of "core concept data", the fundamental data that enables most DoD use cases. Having CDOs and a digital workforce, while also establishing more effective data governance, is key to improving core concept data. In support of the Office of the Secretary of Defense (OSD), CDAO is providing data teams to Principal Staff Assistants to improve their ability to access, use, and improve data among functional communities. To accelerate the adoption of data, analytics, and AI within the Combatant Commands (CCMDs), CDAO is embedding digital teams through the Accelerating Data and AI (ADA) initiative. These CDAO-provided ADA teams provide CCMDs with resources to develop digital solutions and enable access to enterprise tools and data to accelerate decision-making across multiple domains, including financial management, logistics and supply chain, workforce and personnel, global force management, and executive decision support. ADA teams are helping CCMDs understand and resolve challenges in advancing their digital readiness. Digital Readiness Assessments at each CCMD help reveal the existence of any cultural, bureaucratic, and technical barriers that prevent responsible adoption of data-driven technologies. Additionally, we are working closely with U.S. Cyber Command on the development and implementation of their five-year AI roadmap for rapidly adopting and acquiring AI systems applications, and supporting data and data management processes for the Cyberspace Operations Forces.

Business Performance Metrics

CDAO, in partnership with DoD Performance Improvement Officer (PIO), is defining and data-enabling the metrics DoD will use to assess and manage its performance of the Secretary of Defense's priorities and the implementation of the National Defense Strategy and the Strategic Management Plan. CDAO works to ensure that metrics are outcome-based and measurable, improves data access and quality to inform those metrics, provides analytic tools, and grows the digital talent pool to derive insight and improves DoD decision-making.

AI Scaffolding

Enterprise AI scaffolding consists of the robust environments and tooling that enable industry-trending environments for development of machine-learning and AI capabilities, testing, and assurance. CDAO works with DoD Components to assess their level of readiness to adopt AI-enabled capabilities and provides the technical and non-technical enterprise services, infrastructure, data, tools, contracting mechanisms, and best practices they need to accelerate secure, reliable and responsible AI development, adoption, and operational sustainment.

<u>Combined Joint All-Domain Command and Control Data Integration Layer</u>

Considering Combined Joint All-Domain Command and Control (CJADC2) as data-centric command and control for the 21ˢᵗ Century, and not a product to be delivered, CDAO will enable warfighter capability federation by developing a data integration layer to improve access to, and interoperability of, joint data at the strategic, operational, and tactical levels. CDAO, along with technical and operational stakeholders, will iteratively demonstrate and assess this capability via a series of Global Information Dominance Experiment (GIDE) events focused on Joint Warfighting Concept key operational problems.

<u>Digital Talent Management (DTM)</u>

In partnership with the Under Secretaries for Personnel and Readiness, as well as Research and Engineering, CDAO is building the Defense Digital Workforce, beginning with coding existing DoD talent capable of executing roles in data, analytics, AI, and software. As the Functional Community Manager of the Data, Analytics, and AI workforce, encompassing 11 work roles, CDAO is investing resources to establish a digital workforce that is globally identifiable, accessible, and available for DoD use. CDAO has built a robust team to systematically analyze DoD's digital workforce and promote their education and management as a unified cohort. Ultimately, CDAO will develop the data, analytics and AI workforce so that DoD has the necessary talent for organic development, delivery, and implementation of digitally-enabled capabilities. The Defense Digital Workforce will lead DoD's adoption of data and AI from classroom-to-combat.

Use-Case Driven AI

AI is not a singular, monolithic technology or one-size-fits all-solution. "AI" represents a collection of individual, use-case-based applications of a set of technologies. For example, talking to your phone, making shopping suggestions, matching you with the driver most likely to get you home quickly, or guessing the documents you are most likely to click on when searching. The same is true for DoD: computer vision to understand the environment; natural language processing to navigate DoD's policies and requirements; and many other types of machine learning algorithms to support predictive maintenance, modeling and simulation, and virtual and constructive training.

In each of these cases, there are different algorithms, different success criteria and metrics, and different data necessary to train the models underpinning that particular technology.

Responsible AI in DoD

AI-based technologies can help take advantage of opportunities and improve our capabilities and effectiveness. However, they also pose significant challenges and risks that require careful oversight, management, governance, and accountability. DoD is committed to developing and deploying AI technologies in a manner that upholds our Constitution, laws, policies, and values. We will lead in the global AI field thanks to our democratic principles, not in spite of them.

In 2020, DoD adopted five AI Ethical Principles: Responsible, Equitable, Traceable, Reliable, and Governable. These principles are founded on the U.S. Constitution, Title 10 of the U.S. Code, the Law of War, privacy and civil liberties protections for individuals, and long-standing international norms and values. The AI Ethical Principles operationalize these policies and values into the context of the critical AI sector. To this end, DoD released the Responsible AI Strategy & Implementation Pathway in June 2022, which outlines the Department's comprehensive, coordinated, and structured approach to building responsible artificial intelligence (RAI) capabilities. This pathway reinforced the five DoD AI Ethical Principles and laid out a plan for operationalizing them throughout DoD. The plan designates roles and responsibilities for 64 separate lines of effort, which are organized under six tenets: RAI Governance, Warfighter Trust, AI Product and Acquisition Lifecycle, Requirements Validation, Responsible AI Ecosystem, and AI Workforce.

DoD recognizes that responsible AI use is not only a matter of internal governance, but also a matter of external collaboration and engagement. DoD is committed to working with other Executive Branch agencies, our allies and partners, academia, industry, civil society, and other stakeholders to promote responsible AI design, development, acquisition, and use.   DoD is also involved in efforts to establish international norms and standards for responsible AI use that are consistent with our values and interests, and actively engages with partners and allies on this topic through the U.S.-led AI Partnership for Defense, international organizations like NATO and the United Nations, and through engagements with countries interested in furthering the goals of RAI including AUKUS and FVEY countries. CDAO and DoD more broadly welcome the opportunity to work with any like-minded nation on RAI, and actively do so on a regular basis.

As we embed AI in many other aspects of our mission — from battlespace awareness, cyber and reconnaissance, to logistics, force support and other back-office functions — we are mindful of the potential risks of AI-enabled technologies, which we are determined to understand and address. This includes establishing processes to design and employ a human fail-safe during the AI development lifecycle and post-AI system deployment, empowering our warfighters with the skills and tools to notify and report changes in capability performance, outcomes, unpredicted behavior, and/or disengagement in accordance with existing DoD processes.

By putting our values first and playing to our strengths, the greatest of which is our people, we have taken a responsible approach to AI that will ensure America continues to come out ahead.

Unintended Bias in AI

CDAO prioritizes a future DoD in which the data used to train and deploy AI and statistical models is accurate, reliable, and representative of the real-world scenarios and populations that the models will affect. DoD has committed to avoiding unintended bias in AI models as part of its AI Ethical Principles. To meet that commitment, DoD and CDAO are implementing several strategies, such as establishing data governance policies and standards that promote data quality, security, and responsible use across the DoD enterprise, and developing

data literacy and awareness programs that educate DoD personnel on the potential sources and impacts of bias in data and AI technologies.

Supporting CDAO's priority for data quality improvement, DoD is creating validation and verification processes that check data for errors, inconsistencies, and class imbalances before and after using it for AI and statistical model development. DoD is also exploring and developing methods that provide for traceability and accountability for the AI models' decisions and outcomes. These strategies are important because unintended bias in AI and statistical models can have serious consequences for DoD's mission and values.

Conclusion

In conclusion, I would like to reiterate DoD's commitment to ensuring responsible and ethical use of AI-enabled technologies in our missions and operations. AI technologies can enhance our national security and defense capabilities while reducing risks to our personnel and civilians. DoD has adopted a set of ethical principles for these technologies, and CDAO is working to further operationalize those principles across the Department. DoD is also engaged in collaborative efforts with various stakeholders to promote trust, transparency, and accountability in AI development and use. We look forward to working with Congress and this Subcommittee on these issues, and others, as we enable DoD's current and future use of data, analytics, and AI-enabled technologies for national security.

Thank you, and I look forward to answering your questions.