[H.A.S.C. No. 117–93]

HEARING

ON

NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2023

AND

OVERSIGHT OF PREVIOUSLY AUTHORIZED PROGRAMS

BEFORE THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES
ONE HUNDRED SEVENTEENTH CONGRESS

SECOND SESSION

SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS

ON

DEPARTMENT OF DEFENSE INFORMATION TECHNOLOGY, DIGITAL DEVELOPMENTS, AND ARTIFICIAL INTELLIGENCE FOR FISCAL YEAR 2023

HEARING HELD
MAY 18, 2022

U.S. GOVERNMENT PUBLISHING OFFICE
48–653 WASHINGTON : 2023

SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS

JAMES R. LANGEVIN, Rhode Island, *Chairman*

RICK LARSEN, Washington
SETH MOULTON, Massachusetts
RO KHANNA, California
WILLIAM R. KEATING, Massachusetts
ANDY KIM, New Jersey
CHRISSY HOULAHAN, Pennsylvania, *Vice Chair*
JASON CROW, Colorado
ELISSA SLOTKIN, Michigan
VERONICA ESCOBAR, Texas
JOSEPH D. MORELLE, New York

JIM BANKS, Indiana
ELISE M. STEFANIK, New York
MO BROOKS, Alabama
MATT GAETZ, Florida
MIKE JOHNSON, Louisiana
STEPHANIE I. BICE, Oklahoma
C. SCOTT FRANKLIN, Florida
BLAKE D. MOORE, Utah
PAT FALLON, Texas

JOSH STIEFEL, *Professional Staff Member*
SARAH MOXLEY, *Professional Staff Member*
PAYSON RUHL, *Clerk*

CONTENTS

DEPARTMENT OF DEFENSE INFORMATION TECHNOLOGY, DIGITAL DEVELOPMENTS, AND ARTIFICIAL INTELLIGENCE FOR FISCAL YEAR 2023

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS,
Washington, DC, Wednesday, May 18, 2022.

The subcommittee met, pursuant to call, at 10:07 a.m., in room 2118, Rayburn House Office Building, Hon. James R. Langevin (chairman of the subcommittee) presiding.

OPENING STATEMENT OF HON. JAMES R. LANGEVIN, A REPRESENTATIVE FROM RHODE ISLAND, CHAIRMAN, SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS

Mr. LANGEVIN. The subcommittee will come to order.

I want to welcome everyone to today's "Department of Defense Information Technology, Digital Developments, and Artificial Intelligence for Fiscal Year 2023" hearing.

Some housekeeping things before I give my official opening statement. We have obviously convened this as a hybrid hearing, so just to—for formality, members who are joining remotely must be visible on screen for the purposes of identity verification, establishing and maintaining a quorum, participating in the proceeding, and voting.

Those members must continue to use the software platform's video function while in attendance unless they experience connectivity issues or other technical problems that render them unable to participate on camera. If a member experiences technical difficulties, they should contact the committee staff for assistance.

The video of members' participation will be broadcast in the room and via the television internet feeds. Members participating remotely must seek recognition verbally, and they are asked to mute their microphones when they are not speaking.

Members who are participating remotely are reminded to keep the software platform's video function on the entire time they attend the proceeding. Members may leave and rejoin the proceeding. If members depart for a short while for reasons other than joining a different proceeding, they should leave the video function on. If members will be absent for a significant period, or depart to join a different proceeding, they should exit the software platform entirely and then rejoin if they return.

Members may use the software platform's chat feature in communication—to communicate with staff regarding technical or logistical support issues only.

Finally, I have designated a committee staff member to, if necessary, mute unrecognized members' microphones to cancel any inadvertent background noise that may disrupt the proceeding.

With that, today we are joined by Mr. John Sherman, the DOD [Department of Defense] Chief Information Officer [CIO] serving concurrently as the interim Chief Digital and Artificial Intelligence Officer. He is joined by Ms. Margaret Palmieri, the Deputy Chief Digital and Artificial Intelligence Officer; and Dr. Kelly Fletcher, the Principal Deputy Chief Information Officer.

I welcome our witnesses today.

The position of the Chief Digital and Artificial Intelligence Officer is a new one at the Department of Defense, effective as of February. The CDAO will serve as the Department's senior official responsible for strengthening, integrating data, artificial intelligence, and digital solutions, and at its outset assumed responsibility for the three preexisting entities that our members will be familiar with—the Joint Artificial Intelligence Center, or the JAIC; the Office of the Chief Data Officer; and the Defense Digital Service.

While Mr. Sherman has appeared before us previously, he did so in his CIO capacity, and today marks the inaugural appearance of the CDAO in front of Congress.

For as long as I have served on this committee, there has been a bicameral and bipartisan push to elevate the role technology plays in the Department and to disassemble the artificial stovepipes that exist within the sprawling bureaucracy.

In bringing the CIO and CDAO together today, the committee is making clear precisely how important of a role of technology plays in warfare and that no single leader can manage it all. So from data to operationalizing artificial intelligence, to building resilience in our networks, these topics are just too vital to be foisted onto a single official's already full plate.

So I here—I applaud the Department's leadership for taking this first step in creating the CDAO.

Next comes that vital pivot when the Department moves from concept to execution. And as long—as the saying goes, the devil really is in the details. So the lion's share of the CDAO duties were previously held by the Chief Information Officer. The future success will depend in part on the clear delineation of responsibilities between the CIO and the CDAO.

These are positions whose responsibilities will persistently sit adjacent to one another. It is critical that these lanes of the road are clear not only to one another, but [to] the Department, the rest of the executive branch, congressional oversight committees, and our international partners and allies.

In addition to this delineation, I am eager to hear how the CDAO will organize its efforts. In inheriting three separate entities in the JAIC, Defense Digital Service, and the Chief Data Officer, the CDAO is poised to develop exciting new constructs and build expertise across teams that have previously been siloed.

For instance, we have seen how critical good data principles are to building useful artificial intelligence models. Hence, it only

stands to reason that the CDAO would be thinking about new ways to align the teams that had previously worked these problems in separate silos.

So, finally, I hope to hear how both the CIO and the CDAO will be working with the services. While we finally have empowered CIOs within each of the military departments, there are not—there are not natural parallels for the CDAO. So will the CDAO's engagement with the services be directed at their CIOs or are there other more suitable positions for the CDAO to work with?

There are many historical comparisons to show that all of the best efforts within the Office of the Secretary of Defense can be quickly stymied without commensurate efforts by the services.

Again, I am excited to hear about all of these matters and more. But before proceeding, I want to remark briefly about Mr. Sherman and his CIO team. So here I want to stay that when he was with us last year, I put a spotlight on the frustration that the subcommittee was dealing with, specifically in transparency on the budget request and information technology matters with his office.

So in the year since, under John's leadership, we have seen a remarkable transformation when it comes to transparency, increased responsiveness to congressional inquiries, and the timely delivery of products required by law.

Too often it falls on Congress to point out the shortfalls or failings of the Department of Defense. But when deserved, we should also acknowledge its successes, and I commend John and his team for its track record over the last year, and I thank you for your efforts.

So with that, I want to thank our witnesses for appearing before us today, and I will turn now to Ranking Member Banks for his remarks.

[The prepared statement of Mr. Langevin can be found in the Appendix on page 23.]

STATEMENT OF HON. JIM BANKS, A REPRESENTATIVE FROM INDIANA, RANKING MEMBER, SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS

Mr. BANKS. Thank you, Mr. Chairman, and thank you to the witnesses who are here with us today and for joining us on short notice.

Mr. Sherman, as CIO for the Department of Defense, you are responsible for a significant number of programs—cloud adoption, IT [information technology] networks, data policies, spectrum management, cybersecurity, and more. All of these things are critical to the warfighter, and we don't take that lightly.

Secure, effective technology can revolutionize how the Department conducts its business, but investments in IT infrastructure are necessary to do so.

I am encouraged by the progress that you have made in the last year, but I fear there is still a long road ahead. I also have been disappointed in the delays to award contracts in the Joint Warfighter Cloud Capability program.

I think the creation of the Chief Digital and Artificial Intelligence Officer was a wise move to help the Department better use and deploy AI at scale, but the value of that move won't be realized

for months as Dr. Martell is not yet in place. With an enterprise as large and diverse as the DOD, modernization and security is a difficult task. You need the buy-in not just from the highest levels of the DOD but everyone who logs onto a DOD network.

You also need a capable workforce to acquire and deploy it, as well as train the rest of the workforce on how to use it. Without strong investments, strategic vision, diligence in implementation, and accountability, we risk weakening the Department's security, which is unacceptable.

I look forward to our conversation today about how to continue the progress that you have made and to expand upon it.

And with that, thank you. I yield back.

Mr. LANGEVIN. Very good. Thank you, Ranking Member Banks, for your remarks.

As a point of order, while we have three witnesses joining us today, we will have Mr. Sherman deliver opening remarks, and during the question portion we will ask that he turn to his colleagues as he sees fit for remarks and answers.

With that, I will turn it over to Mr. Sherman for 5 minutes of remarks. Your full statement can be submitted for the record, and I ask you to summarize your remarks for 5 minutes.

Mr. Sherman, please proceed. We need to have your microphone on. Mr. Sherman, I can't hear you. Nothing yet.

Okay. I am going to have to ask staff to intervene here and figure out the technical issues here.

STATEMENT OF JOHN SHERMAN, CHIEF INFORMATION OFFICER AND ACTING CHIEF DIGITAL AND ARTIFICIAL INTELLIGENCE OFFICER, OFFICE OF THE SECRETARY OF DEFENSE; DR. KELLY FLETCHER, PRINCIPAL DEPUTY CHIEF INFORMATION OFFICER, OFFICE OF THE SECRETARY OF DEFENSE; AND MARGIE PALMIERI, PRINCIPAL DEPUTY CHIEF DIGITAL AND ARTIFICIAL INTELLIGENCE OFFICER, OFFICE OF THE SECRETARY OF DEFENSE

Mr. SHERMAN. Chairman Langevin, all right, it looks like we are hot now.

Mr. LANGEVIN. We have got it. Yes. Please proceed.

Mr. SHERMAN. Thank you very much, sir.

Good morning, Chairman Langevin, Ranking Member Banks, and distinguished members of the subcommittee. Thank you for the opportunity to testify before you today. As you noted, with me is Dr. Kelly Fletcher, our Principal Deputy Chief Information Officer, who can help provide insight on our resources and budget, among other topics; and Ms. Margie Palmieri, our Deputy Chief Digital and Artificial Intelligence Officer, who will help me speak on the standup of this exciting new office.

Chairman Langevin, I would first like to thank you for your past 22 years——

Mr. LANGEVIN. Mr. Sherman, if you can please pause for a minute. We are having some technical difficulties here.

Mr. SHERMAN. Okay. We are hot again.

Chairman Langevin, I would first like to thank you for your past 22 years of public service to our Nation. Your leadership has posi-

tively impacted all of the Department of Defense from the civilian workforce to our women and men in uniform.

I appear before you today as the DOD CIO and the Acting CDAO. With your support, we have made strong progress since I testified before you last June, and I look forward to updating the subcommittee on our achievements and the recent establishment of the CDAO.

Moreover, as we discuss investments today, I want to assure you that both the CIO and CDAO budgets are fully informed by the President's vision, policies, and strategies, including the Interim National Security Strategic Guidance and the Department's National Defense Strategy.

The Department has made significant strides to unlock the power of its data, harness AI, and provide digital solutions to the joint force. Going forward, there is a need for stronger alignment to accelerate decision advantage and generate advanced capabilities for our warfighters as we face China as a pacing challenge, an increasingly aggressive Russia, and as our adversaries adapt to technology innovation.

In December 2021, Deputy Secretary of Defense Hicks established a CDAO to serve as the Department's senior official responsible for strengthening and integrating data, AI, and digital solutions across the defense enterprise. Integrating the standalone data and AI organizations into the CDAO is a multi-step process that began on the 1st of February and will reach full operating capability on the 1st of June.

While the DOD CIO will continue to lead core infrastructure functions, including cybersecurity, cloud, transport, and networks, the CDAO will help set requirements and provide strategy, policy, and governance of data, analytics, and AI. This office will provide enterprise-level infrastructure and services that enable efforts to advance adoption of these critical areas.

The CDAO will work closely with our team in CIO and other components within the Department to ensure mission success. As the CDAO focuses on organizing and carrying out their mission, I will continue my attention as a CIO on enterprise-level priorities, such as cybersecurity, cloud computing, software modernization, and warfighting command, control, and communications, or C3.

We have been able to move forward in these areas through robust governance and teamwork, to include with the military departments. In cybersecurity, I am committed to ensure protection of the Department of Defense Information Network, or DODIN, implementing zero trust, hardening the SIPRNet [Secret Internet Protocol Router Network], addressing 20-plus years of technical data on our systems, securing the defense industrial base, and enhancing our cyber and digital talent.

Of course, cloud computing remains a fundamental component of the Department's global IT infrastructure. To that end, I will ensure that we provide modern enterprise cloud capabilities to enable everything from software modernization to enhanced user experience at every classification level.

Finally, turning to C3, I remain driven to modernize our positioning, navigation, and timing, or PNT, capabilities; lead the Department on the electromagnetic spectrum operations, or EMSO,

development; move forward on 5G while ensuring DOD equities remain protected, and also providing economic opportunities for U.S. industry, strengthening transport, and ensuring national leader command capabilities.

In closing, I thank this subcommittee for its consistent and dedicated support in these and countless other areas. It would truly not be possible without your strong partnership and guidance.

Thank you for the opportunity to testify this morning, and we look forward to your questions.

[The prepared statement of Mr. Sherman can be found in the Appendix on page 26.]

Mr. LANGEVIN. Very good. Mr. Sherman, thank you very much for your remarks.

With that, we will now proceed with questions. Each member shall be recognized for 5 minutes, beginning with myself.

With that, Mr. Sherman, can you speak to the efforts underway, not only to define the role and responsibilities of the Chief Digital and Artificial Intelligence Officer but also to account for and revise historical policies and directives that may designate or outline roles for the CIO, which may now more appropriately be handled by the CDAO.

Mr. SHERMAN. Yes, sir. I will start with this, and then turn to Ms. Palmieri for some amplifying comments. We have had a robust effort underway since IOC on the 1st of February to bring the new organization together, identifying leaders, ensuring employees know where they go in the new structure, and really getting the most synergy out of this new AI, data, digital services alignment together with this.

A lot of work, sir, has gone into this in terms of defining roles, getting our workflow together, and using real-world opportunities such as with the operation supporting the Ukraine crisis to bring things like the Advana team to bear, to supporting U.S. Transportation Command and U.S. European Command. So real-world operations to drive the way ahead on that.

Additionally, working with the Director of Administration and Management, or DA&M, at the Pentagon under Mr. Mike Donley, former SECAF [Secretary of the Air Force], doing all of the pick and shovel work, updating the policies, updating the paperwork that identified CIO previously on some areas, to put CDAO in the right parts of the documentation, and then also looking at things like the finances in terms of some of the former historical relationship with the Joint AI Center and DISA [Defense Information Systems Agency], and so on, and making sure we do the blocking and tackling to align and empower the new CDAO organization.

And, sir, with that, I would like to turn to Ms. Palmieri briefly, and hopefully your mic is hot there. If not, I will give you mine.

Ms. PALMIERI. Let's see. Yep. Thank you, sir, for the question. As part of the CDAO standup, we have established a governance working group, and they are looking through over 40 different foundational documents that reference either the preexisting organizations before CDAO or other roles and responsibilities that CDAO is taking over. And so we are looking at holistically and looking at governance specifically in all the different working groups in the Department.

I think we found about 21 that had oversight on some of our issues. We have been able to streamline those in the near term and take them down, actually reducing the level of bureaucracy around some of these issues and getting some more clarity on them.

Thanks.

Mr. LANGEVIN. Very good. Thank you.

So in my opening remarks, I noted questions about how the DOD CIO and the CDAO will collaborate together and deconflict their work with the military services. So can you elaborate on that more? Can you speak to your initial thoughts on this matter, and specifically who the right interlocutors are within the military departments for the CDAO?

And, you know, if it is the services' CIOs, then how can the CIO and the CDAO proactively think through how to minimize the potential for OSD overload given the service CIO's relatively small size?

Mr. SHERMAN. Yes, sir. So as a first step is to capitalize on the very well-established relationships we already have through CIO channels, as you note, sir, with the services and MILDEP [military department] CIOs, to be able to use our established governance processes, the teaming we have, certainly not to overload them, but to use the very well-established processes we have in place. Matter of fact, we were doing something this week on coordinating some material with the CIOs.

The other thing, the Chief Data Officers who work for the service CIOs have a very established relationship on the data side of things through data governance councils that we can tap into.

Now, with the AI aspect, this is probably an area that we need to reinforce. There is a lot of AI going on in the services under the military departments, that we have some established governance there, much of which goes through the CIOs but not all of it, and that is an opportunity for us and we need to tighten that up as well.

So, in a nutshell, working through the CIO so far has given us a successful ingress point. But when Dr. Martell gets here, working with Ms. Palmieri, these are the—this is an area that, as we really get up on our skis with this, need to refine a bit, ensuring, as you note, sir, that we don't overload a process and that we are getting to the right humans in each of the components to get the answers we need on whether it is operations or responsible AI or unlocking the power of the data.

Margie, would you add anything to that?

Ms. PALMIERI. No. I think that hits it very accurately. I think the other piece about this is, you know, mission owners are across the Department and not just within the data or CIO lane. And so a lot of the work that Mr. Sherman talked about that we have been able to do in support of Ukraine has been with the Joint Staff, J4, and the logistics community or with EUCOM's [U.S. European Command's] team on logistics.

And so the partnerships with the mission owners is also very critical, and I think we will—we have gotten great support from people that want to use data and analytics as we work the broader issues through the CDAO and CIO channels.

Mr. LANGEVIN. Thank you for those answers.

I am going to hold. I have additional questions. Hopefully we will get to a second round or I will submit them for the record.

But for right now, I want to yield to Ranking Member Banks for his questions.

Mr. BANKS. Thank you, Mr. Chairman. A few years ago, Vladimir Putin proclaimed that "Artificial intelligence is the future. Whoever becomes the leader in this sphere will become the ruler of the world."

While there have been some useful but limited AI programs, such as Project Maven, that have gotten to some scale and now transition, the DOD still needs a scalable enterprise capability for the integrated deployment of AI technologies for joint warfighting missions.

Ms. Palmieri, what are your plans as Deputy CDAO to accelerate, scale, and transition an AI-enabled warfighting capability?

Ms. PALMIERI. Yes, sir. Thanks for the question. Part of the [inaudible] of the CDAO is to look at both the enabling infrastructure, the analytic tools, and the tools that people will use to develop AI, and then the responsible AI ethics and testing and evaluation processes to make sure that the United States is doing this in accordance with established ethical considerations.

So much of our budget in the fiscal year 2023 cycle and fiscal year 2022 cycle is focused on bringing that core enabling enterprise capability, so that includes the computing platform, the tools, and then the data policies that will enable us to access different data from across the Department to really bring that together and enable either analytics or ultimately artificial intelligence to be able to support decisionmakers with decision advantage.

And so one of the key initiatives under that is the Secretary—the Deputy Secretary of Defense's AI and Data Acceleration initiative, or AIDA. This is an area where we have put significant investment in both talent and money to go out to the combatant commanders and some of the principal staff assistants inside of the Department in charge with business operations and support them with experts, digital experts, data experts, as well as bringing some of our established capabilities.

In Advana, this is our business health system, and in Project Maven on the AI side, and scale that up to combatant commanders more broadly, share those lessons across COCOMs [combatant commands], and then bring that back to identify the barriers that we have to enable across the Department.

Mr. BANKS. Very good.

Mr. Sherman, as I mentioned in my opening statement, I am concerned by the delays in awarding contracts for the JWCC. Has the Department considered using a rolling date for compliance for providers instead of one set date, the end of December?

Mr. SHERMAN. No, sir. We have not considered a rolling date, but I can assure you getting this right and getting this done by the end of this calendar year is among my very top priorities.

Sir, I think you are referencing we had—when I rolled this out, when I was the acting last year, that we were aiming for April for an award date, but part of this—and I will own this here—was we haven't done this at this scale, and when we had—did the initial

review, that we had four vendors make the cut, that we had estimated too quickly on the date.

So December, working with the team between our team in CIO, DISA, Washington Headquarters Services, with support from Acquisition and Sustainment, with all of the advice on the procurement experts, and the way we are proceeding with the awards aiming for December, but, sir, we recognize this is critically important. We appreciate the committee's support here recognizing with the JEDI [Joint Enterprise Defense Infrastructure] cancellation and how important this is for the CDAO efforts, for Joint All-Domain Command and Control, and so much of what we are doing for warfighting.

So, sir, I will assure you we are getting—we are getting after this with alacrity.

Mr. BANKS. Can you talk a little bit more about the task order process that you envision for JWCC?

Mr. SHERMAN. Yes, sir. The way that we are going to do this, there will have to be on each of—depending upon how many vendors do make the cut on this, to be able to have—there will be individual task orders that will have to go in, but the upshot of what we did learn from JEDI was a process that our Hosting and Compute Center team, HACC, up at the DISA headquarters came up with to be able to expedite this, so users do not have to take an incredibly long time to compete task orders against whichever kind of best athlete cloud they want to use.

It is called ATAT [Account Tracking and Automation Tool], is what they call it. So we do have an established process there to use these IDIQ [indefinite delivery, indefinite quantity] contracts, but to be able to have expedited task orders to depend on what the workload and mission is for that, sir.

Mr. BANKS. Okay. Just a couple more questions. Can you provide an example of a commercial technology solution that the Department has adopted that has been successful?

Mr. SHERMAN. I think we have had plenty. I think a lot of is in the cybersecurity realm, sir. I will start there, but I could go to others, such as with Comply-to-Connect, such as what we are doing for endpoint security, such as what we are doing on software-defined networks, not only for security matters but on areas like 5G.

I think there is a number of areas on command and control I could go into on spectrum hitting on that that have been commercial technologies we have been able to use, and cloud already exists extensively in the Department at the service level, such as with Cloud One, cARMY, Black Pearl in the Navy. There has been a lot of commercial innovation there, and as well as with software, quite a bit of commercial software usage across the Department.

My job as CIO is not only to encourage and cultivate that but to make sure we can make this work at an enterprise level, such as with JWCC, such as supporting CDAO. But, sir, there have been a number of key technologies we have rapidly integrated and employed for our warfighter and other support.

Mr. BANKS. Just one final question. Our national security depends on resilience across the defense industrial base [DIB]. I know you know that because your office has rightfully taken on an increased role in this arena. How are you leveraging AI to grapple

with the size and scale of the DIB attack surface and the speed at which we need to identify and remediate vulnerabilities?

Mr. SHERMAN. So that is one area that with the CDAO now standing up that I want to work with Dr. Martell and work with Ms. Palmieri on. I can tell you at an unclassified level there are—some of this is we work with our colleagues at CYBERCOM [U.S. Cyber Command] and NSA [National Security Agency] employing AI capabilities to be able to get after some of this.

But this is an area, as we look at big data platform, as we look across an enterprise—now you are talking about DIB, not the DODIN, so I need to make sure I focus my remarks on that. These are areas that we look at the 220,000 companies in the DIB, and particularly as we look at cyber maturity model certification employment, I want to make this understandable and usable, particularly to small and medium businesses.

So while not [inaudible], we are looking at areas to where we can possibly use some government cloud capabilities to be able to put data in from these companies if we can do this properly and with the proprietary considerations to be able to help these companies out where we can run analytics and lessen the burden on the small and medium-sized companies out across the United States and not make this too cumbersome on them.

So this is an area we need to work on, sir, but it is definitely on my radar to do so.

Mr. BANKS. Thank you. I yield back.

Mr. LANGEVIN. Thank the Ranking Member.

The chair now recognizes Mr. Moulton for 5 minutes.

Mr. MOULTON. Great. Thank you, Mr. Chairman. I would like to pick up with Ms. Palmieri. In answering your questions to—the questions of Ranking Member Banks, you mentioned that when you bring forward new AI capabilities you have to ensure their employment meets our ethical norms and standards. This is, of course, exactly what we would expect.

But do you believe that our adversaries adhere to the same ethical standards?

Ms. PALMIERI. Yes, sir. Thanks. Not in all cases. We know that there are nations that do not respect the privacy of citizens and do not necessarily use that information that they get in a way that meets our ethical principles.

Our five ethical principles are that we use AI responsibly; that we take steps for it to be equitable, which means we minimize unintended consequences associated with our capabilities; that our methods are traceable. This means that we can audit them. We know how the AI was developed. It is reliable, that there are well-defined use cases and we know what the AI is good at and what it is not good at, and we have a testing and assurance cycle associated with that. And that it is governable, and that we know that it does its intended functions, and if it doesn't do those intended functions, we can either deactivate the system or take it offline.

Those are very important to us. We are working on a responsible AI strategy right now in the last few weeks of coordination across the Department, where we are going to take those principles and actually put them into implementation action and so——

Mr. MOULTON. I will tell you that, I mean, as fellow Americans, we certainly agree with those ethical standards, and this is what we would expect of you and of us. But I think it is patently obvious to all of us that China and Russia, our principal adversaries, are not going to adhere to these standards. They don't, and we can see this playing out in Ukraine every day.

And, therefore, their AI won't as well. I am confident that their AI is being trained to do heinous things or at the very least pay little regard for civilian casualties and collateral damage, which will almost certainly make their AI more deadly and effective.

Everything you just described is the right thing to do, but there are constraints on these AI weapons. So in an AI versus AI battle, they will have a massive advantage because they won't constrain their weapons in the ethical ways we do. So the point that I am making is that we have to do work on developing an international agreement to codify these standards, so it is not just us who are following them, and then we at least have some hope of ensuring our adversaries' worst instincts are at least to some degree constrained.

Now, not every nation abides by the Geneva Convention, but we know across the world that it does matter and it does help. So just as when the world came to terms with the horrors of chemical weapons in World War I, and the Geneva Convention was the result, I think this is a second Geneva Convention moment.

Now this is not your responsibility. I get that this is the—basically falls under the State Department. But I don't think enough people in State appreciate how important this is. And as one of the leaders in our government on the use and employment of AI, I would strongly encourage you to help mount an effort to work on this broader problem.

Do you have any comments on that?

Ms. PALMIERI. Yes, sir. Absolutely. In fact, we have a partnership for defense organization right now with 16 nations. They include our Five Eyes partners, many of our partners out of NATO, and some others like Israel, Finland, Sweden. This is absolutely an interest area of all of those nations that we have started with, but absolutely take your point on a broader effort, and that is worth pursuing. Thanks.

Mr. MOULTON. I mean, this is one of the principal recommendations that came out of the Future of Defense Task Force that Representative—Ranking Member Banks and I co-chaired.

And, look, ultimately, if you do this right, we are not only doing the right thing in terms of humanity, but we are figuring out ways that we do this to our advantage, because I think, as I have just described, we are at a disadvantage right now because our adversaries will not be so constrained.

I had another question coming from the results and the recommendations of our Future of Defense Task Force report on the need to update our acquisition process for this new era of technology where we are not just acquiring hardware but acquiring software. And our acquisition system is really not built to acquire software. It is a different animal.

We won't have time to answer that question right now, but that is something that I would like to take for the record and look forward to your response.

Mr. Chairman, with that I yield back.

[The information referred to was not available at the time of printing.]

Mr. LANGEVIN. Thank you, Mr. Moulton.

Mr. Franklin is now recognized for 5 minutes.

Mr. FRANKLIN. Thank you, Mr. Chairman, and thank you to our witnesses for being here today. Actually, my line of questioning was going to be right along with what Representative Moulton was starting to get into there with the acquisition process.

And, Mr. Sherman, I notice in your testimony you talked about the CDAO offering five decentralized procurement vehicles for rapid AI delivery and purchasing of key AI services and enabling tools, a mouthful but sounds like a lot of new ways to try to improve this process.

We know, as has already been noted, AI is so integral to the future, our future success, it cuts across all areas of DOD, but the struggle is, how do we innovate fast enough to keep up with the threat? And we don't have—traditionally, our acquisition system just is not tailored to that.

I would love for you to take the time that I have here to—you and your team—maybe expand on these five different vehicles and help us understand that this is a good thing and we are not just creating more bureaucracy.

And particularly for small businesses, because I speak with a lot of them who have great ideas, but it is just so difficult to navigate the process that by the time they could get something to market it has already passed them by.

Mr. SHERMAN. Sir, I will start with that and then turn to Ms. Palmieri and Dr. Fletcher for amplifying comments. Software acquisition and working on that, of course, it is both within the CIO and CDAO realm to be a driver for that, but it really is going to be a team effort, working with Acquisition and Sustainment, Research and Engineering, with our colleagues in the military departments and services. But to use the authorities that Congress has already granted us in terms of how we can use kind of different approaches to this, but also how we think differently about employing software, acquiring software, developing software ourselves, moving to development, security operations, DevSecOps, approaches, leveraging open source software, and moving at pace; as you have noted, sir, to not have historic ways of coming at this but to be able to move at high speeds.

And then, really, what I see sitting up at OSD, there is so much innovation occurring within the Department, in the military services, at the commands, to jump on that, not try to recreate the will but elevate that. And there has been so many great examples we have seen.

Out at the very tip of the spear, too, out in—out at the sub-unified commands, and so on. So that is one thing we are trying to do is not over-govern this but take these great examples of this.

And looking from the acquisition optics, sir, as I mentioned earlier on Ranking Member Banks' question about small and medium

businesses, this keeps me up a lot, making sure not to take away from the "bigs," but those companies out—all throughout the United States and not to have high barriers of entry, where we can get their products, their capabilities into the system quickly. So this is a priority for me as CIO.

If I can, I would like to turn to Ms. Palmieri briefly from the CDAO optic on the five areas, sir, you were noting.

Margie.

Ms. PALMIERI. Yes, sir. First of all, thank you very much for section 808 in the NDAA [National Defense Authorization Act] that gave acquisition authority to the JAIC. That is now inherited by CDAO. We owe an implementation plan to Congress which will come this summer on how we are going to go after that.

But the five vehicles that the JAIC created were specifically focused on the areas of data and AI, all with an agile approach, and this idea that organizations outside of CDAO could come and leverage these contracts, these enterprise contracts.

And so real briefly, the first one is at Tradewinds. It is another transaction agreement which gives us a very agile approach to focus on mission capabilities. We have about 63 percent of those awardees right now that are either small business or non-traditional defense contractors.

There is another one for data readiness, that's specifically on data engineers, data labelers. This one is really great because you can customize the different performance work statements based off of your needs, and we see about 50 percent of those awardees right now being small business or non-traditional.

There is a vehicle on test and evaluation that provides simplified acquisition procedures for test and evaluation, and we have about, you know, 40 or so—about 50 percent small business versus large business there.

We have a contract vehicle for acquiring contract talent to support AI development, six vendors on that one. It is relatively small now—all small businesses—but we have a lot of interest there, and so we are looking at how to scale up that vehicle.

And then the last one is a commercial solutions offering, which is generally no money involved, but it allows businesses across the board to come in and pilot or demo their capabilities on government data, which is a huge asset to small companies. The government is able to provide feedback on their capabilities, and they get access to our data to test out their ideas.

We have about 4,000 different companies that are eligible for those types of contracts, and then we are doing more with outreach and partnering with non-profits to try to do a better set of market research on who is out there, so we are not just going to the same vendors.

Mr. FRANKLIN. Mr. Chairman, I yield back.

Mr. LANGEVIN. Thank you, Mr. Franklin.

Mr. Moore is now recognized for 5 minutes.

Mr. MOORE. Thank you, Chairman. Thank you, witnesses, for being here. Thanks for your context. I think we can all agree that artificial intelligence is rapidly transforming our world, even sometimes without our knowledge. Industry is on the cusp of some very

key scientific breakthroughs. These will disrupt our daily lives, and disruption in a good way should be celebrated.

Autonomous vehicles, smart homes, all this type of stuff, this is going to be ubiquitous. And while much of it gives us something to look forward to, there is an inherent risk that can be mitigated if the United States—if we are the global leader in AI, we can—we can mitigate the risk that is essentially going to come from this. And just don't trust other nations to properly fill this role.

Mr. Sherman and Ms. Palmieri, welcome comments from either of you. America's greatest strategic advantage against near-peer competition, one of the major advantages is that we remain a country that—the world's number one destination for immigrants and a strong immigrant workforce. As long as talented people want to come here, and to innovate and start their businesses, the U.S. can't be beat.

While primarily technology focused organizations, the CIO and CDAO require that people are proficient in policy, economics, ethics, data science, and the law. How do both organizations ensure they are optimally staffed, considering increased competition in recruitment and retention?

Mr. SHERMAN. Thank you, sir. I will start with that, and then I will ask Ms. Palmieri to chime in.

So, looking at digital and cyber talent writ large, which all is kind of coming together on this, both between CIO and CDAO, as I mentioned to this committee last year, recognizing talent is so critical. I launched a new cyber talent strategy, which we are aiming to publish in the August/September timeframe of this year, which will have a close nexus to CDAO.

It is going to help us think differently about not only using the authorities this committee and the rest of Congress has granted to us on areas like cyber excepted service and also capitalizing on what we have done to think about our current workforce through the defense cyber workforce framework and using our 8140 policy series and doing all of this blocking and tackling behind the scenes work we need to do.

But also, as we have a more dynamic workforce that is going to come in and out of government in a way that may not go to a 30-year career, how do we compete with industry partners with whom we need to have a partnership on to be able to have digital advantage to very sophisticated adversaries as you note in a near-peer and peer competitor fight.

So that is what we are doing from the CIO side. CDAO specifically is going to be looking at AI, data, and digital talent in that regard, so it is going to be a close partnership with CIO.

So for that I would like to turn to Ms. Palmieri to talk to what we are doing on the CDAO front.

Ms. PALMIERI. Sure. Absolutely. So the CDAO, as it has brought together these different organizations across the Department, is about 200 to 300—it is about 250 people total, more than half of whom are technical in some way. They have digital services expertise, computer scientists, or some level of AI or data science background.

And so I am actually very excited about where we are right now as an organization and the talent that we have in that organiza-

tion. On the military side as well, we are leveraging existing communities like the operational research community, which is heavily data and analytic focused, but then we also have an element of our team that is specifically looking at talent management for the entire Department and how we go after talent management there, things like how we first train and educate our people to be, you know, data literate, but then also develop skills and developing analytic and AI skills as well.

But then, also, how do we track them throughout the Department and work that into promotions and the things that we value for opportunities for leadership. Thanks.

Mr. MOORE. And can you also touch on, does the DOD and the intelligence community have adequate information about—obviously, we are in a—we are in an open setting, so it is not a classified setting, but do we have adequate information about the state of foreign military AI applications and the ways that those could be harmful to U.S. national security?

And are we—and, more importantly, are we investing in ways to defend us and defend our Nation against these applications?

Mr. SHERMAN. Sir, at a high level, as you noted, an unclassified session, I can say that working with our colleagues, and Intelligence and Security, in I&S under Honorable Moultrie, and with the intelligence community, this does remain a key topic and robustly focused on. That is what I can say with that.

And in terms of working with adversary—or not working with, but defending against adversary capabilities, that is something that is very much on our radar, both on the CDAO side, but as I implement on the CIO side, things like zero trust cybersecurity and getting after technical debt that is critical, that is very much something we focus on.

And our partnership with the intelligence community, for example, working with my colleague General Nakasone at NSA and CYBERCOM, is something that is very prominent in our discussion. So we do work on this a lot together.

Mr. MOORE. Awesome. Thank you.

Thank you, Chairman.

Mr. LANGEVIN. Thank you, Mr. Moore.

Is Mr. Kim there?

Okay. So that is our first round of questioning. I am going to go to a second round in concurrence with the ranking member. So with that, let me recognize myself.

With regards to structuring the CDAO, can you speak to initial views on possible constructs, how much is notional at this point, particularly with the incoming CDAO? Mr. Martell is reportedly only a few, you know, weeks from starting, what are your thoughts on that?

Mr. SHERMAN. Sir, our organization is pretty solid at this point. And, actually, it doesn't look terribly dissimilar from CIO where we have deputy CIOs. We have—in addition to Ms. Palmieri as the Principal Deputy CDAO, we have five deputy CDAOs organized functionally on areas like acquisition, policy, enterprise capability, warfighting support, and digital services. Those are the five, as well as a separate unit under Dr. Pinelis just looking at responsible AI, artificial intelligence.

And then this is bringing these organizations together—CDO [Chief Data Officer], the Joint AI Center, Defense Digital Services—and then organizing functionally on these areas. We have already begun to do this with the officer, the employees, going to their new integrated units to get after some of the things Ms. Palmieri talked about on support to the Ukraine crisis.

So actually, sir, we have a pretty well-honed organization now. We are still working on some final pieces of that, but the organization has come together. And, again, the point that Dr. Martell and Ms. Palmieri will be working is creating a team of teams.

It is a new organization, breaking down some institutional barriers we had, bringing folks together, and we are seeing this, for example, with the AI and Data Accelerator, the AIDA, teams that Ms. Palmieri noted, supporting the commands and also back at the Pentagon.

So the wheels are turning on this, and we do have a very strong foundation for the new organization.

Margie, anything you would like to add?

Ms. PALMIERI. No. I think that is great. Thanks.

Mr. SHERMAN. Thank you.

Mr. LANGEVIN. Very good. So I know we talked about cloud in some of the line of questions that you touched on. Is there anything else you want to do in terms of give us some sense of where we are to creating and shifting over to an enterprise cloud system, obviously, since, you know, the JEDI failure to execute, you know, to come up with a final decision there and now we are moving into something hopefully similar but without the challenges and protests and all of that. But anything you want to add there?

Mr. SHERMAN. Sir, only that—just to amplify what I said. This is so critical. Sir, you brought this up from here and your position. We have gotten that message loud and clear. And also, not only would—not having protests, but a multi-cloud/multi-vendor approach, which is more consistent with industry standard at this time.

And then, once we have the procurement completed, using it, using the capabilities, using the tasking mechanism that Ranking Member Banks asked me about for the task orders, and really having something that spans the entire enterprise, from the continental United States to the tactical edge, and having that compute capability to support warfighting needs as well as AI and other needs on that with world-class capabilities from U.S. vendors, which I really do see as a national advantage for the United States, whether it's in an INDOPACOM [U.S. Indo-Pacific Command] scenario or EUCOM or anywhere else, to get this in place and really figure out all the capabilities.

And this will be a little bit of a journey of learning, same as our intelligence community partners are doing in their multi-cloud environment with whom we are working closely on lessons learned and how that is working. So this is critically important, sir.

Mr. LANGEVIN. Good. Well, it is a higher priority for me and the subcommittee, and I know it is for you. So I look forward to following the progress on this over time.

If I could, over the last few years, the cybersecurity maturation model certification, or CMMC, received significant public attention.

However, in the last year, we haven't heard much about the program's development. So can you please update us on where CMMC stands and how it is progressing?

Mr. SHERMAN. Yes, sir. I will make one brief comment, and then I would like to turn to Dr. Fletcher because she has been instrumental in helping guide this. We realize we are at what is called CMMC 2.0, which we launched last fall after the initial startup of this.

One of my main goals as CIO is to make sure this is rationalized, understandable, and back to the earlier points that Representative Franklin and others brought up about small and medium businesses all across the U.S., to make this understandable, so this is not overly burdensome, but also is able to protect the controlled unclassified information, CUI data, in contracts.

Dr. Fletcher, would you like to add to that, please?

Dr. FLETCHER. Yes, sure. Thank you, sir. So right now we are reworking the rules. So there is a lot of work happening, but it is behind the scenes. Those rules will go to OMB [Office of Management and Budget], and then they will be available for public comment in March of 2023. So folks will have the opportunity to say, you know, this is onerous or this is about right. And then we may see CMMC in contracts as early as summer of 2023.

Thank you.

Mr. LANGEVIN. Thank you, Dr. Fletcher. Appreciate that.

So for my final question, I am concerned that the Department is not adequately focusing on electromagnetic spectrum operations. I think it's a concern for many. The fiscal year 2022—I am sorry, the 2022 NDAA required the Department to designate a senior official to be responsible for the electromagnetic spectrum superiority strategies implementation plan.

Can you tell us, what is the status of that implementation plan and the leadership structure? And what barriers do you see to the strategy's successful implementations?

Mr. SHERMAN. Yes, sir. So within CIO, we took the baton on this from Joint Staff last fall in terms of being the overall integrator and lead in the Department. But as you note, EMSO, electromagnetic spectrum operations, is so critical for near-peer and peer competitor fights, as we potentially have to ready our forces to fight in highly contested environments—that we haven't had to do for many years—and also, bringing together the electronic warfare community and the spectrum operations community into a very necessary integration.

So to your question, what we are doing from our Deputy CIO for Command and Control, Communications, as the overarching lead on this, to make sure we are looking at governance, funding, standards, very important as we are working with this, but this is a team of team efforts, very diverse here.

Working with the services, the weapons platform leaders and owners, and then, for example, working with U.S. Strategic Command. I was just talking to Admiral Richard about this very topic last week about how we need to be hand in glove working together, given his combatant command responsibility on this.

So, sir, we have moved out on this. We are setting the governance structures in place and making sure that we have all the dif-

ferent wheels turning. This will—this necessarily can't be hypercentralized, but we do need someone to quarterback this, which will be us. But it is going to require extensive coordination, to include with Joint Staff as well, to make sure all of these different pieces—and, again, the marriage of EW [electronic warfare] and spectrum operations—which I don't think we have really ever quite done at this level—get fully implemented.

Mr. LANGEVIN. Very good. I appreciate that, and thank you for those answers and the testimony here today. Those are the questions that I had at this point.

So with that, let me just thank you, Mr. Sherman, Ms. Palmieri, and Dr. Fletcher. Appreciate the work you are doing on behalf of the men and women of DOD and the warfighting effort. We are working hard together on these issues. Look forward to future and further conversation and engagements.

And with that, I believe that there are no further questions from members. If that is correct, I will stop here. And as of now, the hearing stands adjourned.

[Whereupon, at 11:02 a.m., the subcommittee was adjourned.]

A P P E N D I X

MAY 18, 2022

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

MAY 18, 2022

Chairman James R. Langevin
Cyber, Innovative Technologies, and Information Systems Subcommittee

Department of Defense Information Technology, Digital Developments, and Artificial Intelligence for Fiscal Year 2023

May 18th, 2022

The subcommittee will come to order. Welcome to today's hearing, "Department of Defense Information Technology, Digital Developments, and Artificial Intelligence for Fiscal Year 2023".

We have convened this as a hybrid hearing. Members who are joining remotely must be visible onscreen for the purposes of identity verification, establishing and maintaining a quorum, participating in the proceeding, and voting. Those Members must continue to use the software platform's video function while in attendance, unless they experience connectivity issues or other technical problems that render them unable to participate on camera. If a Member experiences technical difficulties, they should contact the committee's staff for assistance.

Video of Members' participation will be broadcast in the room and via the television/internet feeds. Members participating remotely must seek recognition verbally, and they are asked to mute their microphones when they are not speaking.

Members who are participating remotely are reminded to keep the software platform's video function on the entire time they attend the proceeding. Members may leave and rejoin the proceeding. If Members depart for a short while, for reasons other than joining a different proceeding, they should leave the video function on. If Members will be absent for a significant period, or depart to join a different proceeding, they should exit the software platform entirely and then re-join it if they return. Members may use the software platform's chat feature to communicate with staff regarding technical or logistical support issues only.

I have designated a committee staff member to, if necessary, mute unrecognized Members' microphones to cancel any inadvertent background noise that may disrupt the proceeding.

Today, we are joined by Mr. John Sherman, the DoD Chief Information Officer, serving concurrently as the interim Chief Digital & Artificial Intelligence Officer. He is joined by Ms. Margaret Palmieri, the Deputy Chief Digital & Artificial Intelligence Officer, and Dr. Kelly Fletcher, the Principal Deputy Chief Information Officer.

The position of the Chief Digital & Artificial Intelligence Officer is a new one at the Department of Defense, effective as of February. The ***CDAO*** "will serve as the Department's senior official responsible for strengthening and integrating data, artificial intelligence, and digital solutions", and at its outset, assumed responsibility for the three preexisting entities that our members will be familiar with – the Joint Artificial Intelligence Center, the Office of the Chief Data Officer, and the Defense Digital Service. While Mr. Sherman has appeared before us

previously, he did so in his CIO capacity, and today marks the inaugural appearance of the CDAO in front of Congress.

For as long as I have served on this committee, there has been a bicameral and bipartisan push to elevate the role technology plays in the Department, and to disassemble the artificial stovepipes that exist within the sprawling bureaucracy. In bringing the CIO and CDAO together today, the committee is making clear precisely how important of a role technology plays in warfare, and that no single leader can manage it all. From data, to operationalizing artificial intelligence, to building resilience in our networks – these topics are just too vital to be foisted onto a single official's already full plate. I applaud the Department's leadership for taking this first step in creating the CDAO.

Next comes that vital pivot when the Department moves from concept to execution, and as the saying goes, "the devil is in the details". The lion's share of the CDAO's duties were previously held by the Chief Information Officer, and future success will depend, in part, on the clear delineation of responsibilities between the CIO and CDAO. These are positions whose responsibilities will persistently sit adjacent to one another. It is critical that these "lanes of the road" are clear not only to one another, but to the Department, the rest of the Executive Branch, Congressional oversight committees, and our international partners and allies.

In addition to this delineation, I am eager to hear how the CDAO will organize its efforts. In inheriting three separate entities in the JAIC, Defense Digital Service, and the Chief Data Officer, the CDAO is poised to develop exciting new constructs, and build expertise across teams that have previously been siloed. For instance, we have seen how critical good data principles are to building useful Artificial Intelligence models. Hence, it only stands to reason that the CDAO would be thinking about new ways to align the teams that had previously worked these problems in separate silos.

Finally, I hope to hear how both the CIO and CDAO will be working with the Services. While we finally have empowered CIOs within each of the military departments, there are not natural parallels for the CDAO. Will the CDAO's engagement with the services be directed at their CIOs, or are there other, more suitable positions for the CDAO to work with? There are many historical comparisons to show that all of the best efforts within the Office of the Secretary of Defense can be quickly stymied without commensurate efforts by the Services.

Again, I am excited to hear about all of these matters and more, but before proceeding, I want to remark briefly about Mr. Sherman and his CIO team. When he was with us last year, I put a spotlight on the frustrations that this subcommittee was dealing with, specifically in transparency on the budget request and information technology matters with his office. In the year since – under John's leadership – we have seen a remarkable transformation when it comes to transparency, increased responsiveness to congressional inquiries, and the timely delivery of products required by law. Too often, it falls to Congress to point out the shortfalls or failings of the Department of Defense, but when deserved, we should

also acknowledge its successes, and I commend John and his team for its track record over this last year.

With that, I want to thank our witnesses for appearing before us today. I'll now turn to Ranking Member Banks for his remarks.

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 AI-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.

John Sherman
Department of Defense Chief Information Officer

Mr. John Sherman was sworn in as the Department of Defense Chief Information Officer (DoD CIO) on December 17, 2021. In this role he is the principal advisor to the Secretary of Defense for Information Management / Information Technology (IT) and Information Assurance, as well as non-intelligence space systems; critical satellite communications, navigation, and timing programs; spectrum; and telecommunications matters.

Prior to assuming his duties, he served as the Acting DoD CIO and Principal Deputy, DoD CIO from June 2020 to September 2021.

Before joining the Department, Mr. Sherman served as the Intelligence Community (IC) CIO from 2017-2020. In this position driving and coordinating IT modernization among 17 agencies, he led major advancements to the IC's cloud computing, cybersecurity, and interoperability capabilities. He built long-term commitment to these priorities among stakeholders, both in government and industry, and ensured that the IC would remain a leader in each of these areas.

Prior to his tour as the IC CIO, Mr. Sherman served from 2014-2017 as the Deputy Director of the Central Intelligence Agency's (CIA's) Open Source Enterprise (OSE), where he helped transform Open Source Intelligence, leveraging new technologies and interagency partnerships to enhance the growing OSE mission. He previously served for seven years in several senior executive positions at the National Geospatial-Intelligence Agency (NGA), where he led organizations involved in analysis, collection, homeland security, organizational strategy, and international affairs. Earlier, he served as the Principal Deputy National Intelligence Officer for Military Issues on the National Intelligence Council, and as a White House Situation Room duty officer. Mr. Sherman began his IC career in 1997 as an imagery analyst.

Mr. Sherman is a 1992 Distinguished Military Graduate of Texas A&M University where he commanded the Corps of Cadets and received a Bachelor of Arts degree in History. He also earned a Master's degree in Public Administration from the University of Houston. Following graduation from Texas A&M, he served as an Air Defense Officer in the 24th Infantry Division. He is graduate of the DoD CAPSTONE course, the "Leading the IC" course, and the CIA Director's Seminar.

His awards include the Distinguished and Meritorious Presidential Rank, the DIA Director's Award, the CIA Intelligence Medal of Merit, the Secretary of Defense Medal for Meritorious Civilian Service, the NGA Meritorious Civilian Service Medal, and the Canadian Chief of Defence Intelligence Medallion.

Mr. Sherman is married to Liz, who also works in national security. They have two grown children, both of whom are serving their nation and communities.

Dr. Kelly Fletcher
Principal Deputy Chief Information Officer
Department of Defense

Dr. Kelly Fletcher is a career member of the Senior Executive Service and is the is the Principal Deputy CIO. In this capacity, she supports the DoD CIO in serving as the primary advisor to the Secretary of Defense for information technology, cybersecurity, communications, spectrum, and position, navigation and timing. She has served in DoD CIO since February 2020 in a variety of roles including Performing the Duties of the DoD CIO and as the Principal Director for Resources & Analysis.

Dr. Fletcher's federal government career has included leadership roles in both the technology and strategic resourcing domains and she has led a number of significant reorganizations. Prior to joining DoD CIO, Dr. Fletcher served as the Deputy Director for Program Analysis & Evaluation at the Department of Homeland Security (DHS) where she supervised and coordinated the development of the DHS-wide budget (~$50B appropriated). She also led the realignment of the Federal Protective Services (more than 10,000 employees, ~$1B annual spend) from the Cybersecurity & Infrastructure Security Agency (CISA) to the Management directorate.

Dr. Fletcher served in the Department of the Navy from December 2016 to September 2018 in roles including Acting Department of the Navy CIO and Business Modernization Lead. As the CIO, she provided strategic leadership for all Department of the Navy information technology policy and budget decisions and led a Department-wide reorganization of information technology governance and oversight.

Dr. Fletcher spent six years with the Office of the Secretary of Defense (OSD) Cost Assessment and Program Evaluation (CAPE) where she served as the Special Assistant to the Deputy Director and as an operations research analyst. Prior to her government service, she worked in the private sector as an engineer.

Dr. Fletcher earned her Ph.D. in engineering from Georgia Institute of Technology and her B.S. from Washington University in St. Louis.

Margie Palmieri
Deputy Chief Digital and Artificial Intelligence Officer,
Department of Defense

Margie Palmieri is currently the Pentagon's Deputy Chief Digital and Artificial Intelligence Officer. Prior to this she was Director, Integrated Fires for the Deputy Chief of Naval Operations for Information Dominance (OPNAV N2/N6), where she managed investments, training and policy for U.S. Navy integrated fires capabilities, including electronic warfare, cyber, and targeting. She also served as Director, Chairman's Action Group, Office of the Chairman of the Joint Chiefs of Staff, and as Deputy Director, Decision Superiority (OPNAV N2/N6F4), where she managed a diverse portfolio of strategic, operational, and tactical command, control, intelligence, surveillance, and reconnaissance (C2ISR) concepts and capabilities. Margie entered the Navy as a Presidential Management Fellow Graduated from Rutgers University with a Master's degree in public policy and a Bachelor's degree in political science.

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

MAY 18, 2022

QUESTION SUBMITTED BY MR. FALLON

Mr. FALLON. How are the offices of the CIO and CDAO working to expand access to 5G on military installations? What can be done to speed up these efforts?

Mr. SHERMAN, Dr. FLETCHER, and Ms. PALMIERI. The office of the CIO is currently working with OUSD R&E in their lead role for 5G to transition the responsibility of implementation oversight to the Office of the CIO by 1 October 2023, in accordance with FY21 NDAA Section 224. The Office of the CIO is engaged in the DOD 5G Cross Functional Team (CFT) as the principal organization responsible for 5G Policy and Enterprise Infrastructure Programs to deploy secure and interoperable 5G Wireless Networking across all DOD departments and agencies. The coordinated and concurrent actions that would have the greatest impact to reduce the timeline to establish 5G communications on military installations would be to consider increased funding to the Services for transition and implementation.