

[H.A.S.C. No. 118-66]

**THE TECHNOLOGY AND AI FIGHT FOR
21ST-CENTURY OPERATIONS IN
THE DEPARTMENT OF DEFENSE**

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBER, INFORMATION
TECHNOLOGIES, AND INNOVATION

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

HEARING HELD
MARCH 22, 2024



U.S. GOVERNMENT PUBLISHING OFFICE

56-900

WASHINGTON : 2025

SUBCOMMITTEE ON CYBER, INFORMATION TECHNOLOGIES,
AND INNOVATION

MIKE GALLAGHER, Wisconsin, *Chairman*

MATT GAETZ, Florida	RO KHANNA, California
LISA C. McCLAIN, Michigan	SETH MOULTON, Massachusetts
PAT FALLON, Texas	WILLIAM R. KEATING, Massachusetts
DALE W. STRONG, Alabama	ANDY KIM, New Jersey
MORGAN LUTTRELL, Texas	ELISSA SLOTKIN, Michigan
JENNIFER A. KIGGANS, Virginia	JARED F. GOLDEN, Maine
NICK LaLOTA, New York	PATRICK RYAN, New York
RICHARD McCORMICK, Georgia	CHRISTOPHER R. DELUZIO, Pennsylvania

JOSHUA STIEFEL, *Professional Staff Member*
MICHAEL HERMANN, *Professional Staff Member*
BROOKE ALRED, *Research Assistant*

CONTENTS

	Page
STATEMENTS PRESENTED BY MEMBERS OF CONGRESS	
Gallagher, Hon. Mike, a Representative from Wisconsin, Chairman, Subcommittee on Cyber, Information Technologies, and Innovation	1
Khanna, Hon. Ro, a Representative from California, Ranking Member, Subcommittee on Cyber, Information Technologies, and Innovation	2
WITNESSES	
Martell, Dr. Craig, Chief Digital and Artificial Intelligence Officer, Department of Defense	4
Sherman, John, Chief Information Officer, Department of Defense	3
Skinner, Lt Gen Robert, Director, Defense Information Systems Agency	6
APPENDIX	
PREPARED STATEMENTS:	
Martell, Dr. Craig	42
Sherman, John; and Skinner, Lt Gen Robert	27
DOCUMENTS SUBMITTED FOR THE RECORD:	
[There were no Documents submitted.]	
WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING:	
Mr. Moulton	55
Mr. Luttrell	55
QUESTIONS SUBMITTED BY MEMBERS POST HEARING:	
Mr. Moulton	59
Mr. Strong	59
Dr. McCormick	62

**THE TECHNOLOGY AND AI FIGHT FOR 21ST-CENTURY
OPERATIONS IN THE DEPARTMENT OF DEFENSE**

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON CYBER, INFORMATION
TECHNOLOGIES, AND INNOVATION,
Washington, DC, Friday, March 22, 2024.

The subcommittee met, pursuant to call, at 9:01 a.m., in room 2118, Rayburn House Office Building, Hon. Mike Gallagher (chairman of the subcommittee) presiding.

OPENING STATEMENT OF HON. MIKE GALLAGHER, A REPRESENTATIVE FROM WISCONSIN, CHAIRMAN, SUBCOMMITTEE ON CYBER, INFORMATION TECHNOLOGIES, AND INNOVATION

Mr. GALLAGHER. Good morning, everyone. Welcome to today's hearing, "The Technology and AI [artificial intelligence] Fight for 21st-Century Operations in the Department of Defense."

Since the start of this Congress, the Armed Services Committee has held nine hearings dedicated to driving change in DOD [U.S. Department of Defense] through adoption of new technology and pivoting to an innovation-first posture.

No one, obviously, expects the Pentagon, the largest bureaucracy in the world, to turn on a dime. It is an aircraft carrier, not, you know, a little Corvette. But I don't think any member believes the Department is moving with the speed, force, or unity of action necessary to get our warfighters what they need.

We have established that national security in this century is contingent on rapidly embracing new technology, experimenting, iterating, and pivoting from a platform-centric combat to network-centric warfare. And yet there doesn't appear to be any adversary as formidable as the change-resistant culture in DOD.

My hope for this hearing is not only to hear about your plans for the coming fiscal year but more so to understand the precise obstacles and barriers to reform that you have seen, that you have encountered on a day-to-day basis.

And as I have said before in this room, you know, for those of us who attend the Reagan National Security Forum every year, that you can almost, like, copy-and-paste the speech that the Secretary of Defense gives there. It is all about, you know, we are going to kill the Valley of Death. And we talk about it, and the same people have the same conferences, and then it doesn't actually get any better.

So, put differently, why it seems to this committee that, a year later, the implementation of policies we have passed and the direc-

tives on AI, zero trust, and software integration from your bosses seem to have made little progress. And I assume we all agree that speed is essential, and I hope that this hearing fosters an honest conversation about what is holding you back, what you are doing to go faster.

We are very pleased to have before us John Sherman, the Department of Defense's Chief Information Officer; Dr. Craig Martell, the inaugural Chief Digital and Artificial Intelligence Officer; and Lieutenant General Bob Skinner, the Director of the Defense Information Systems Agency and the Commander of Joint Forces Headquarters-Department of Defense Information Network.

General, you get the award for longest title after your name.

And I will note that this is Dr. Martell's final appearance before the committee, having announced last week that he is set to depart his position on April 15th.

And before hearing from the witnesses, I yield to the ranking member for any comments he may have.

STATEMENT OF HON. RO KHANNA, A REPRESENTATIVE FROM CALIFORNIA, RANKING MEMBER, SUBCOMMITTEE ON CYBER, INFORMATION TECHNOLOGIES, AND INNOVATION

Mr. KHANNA. Thank you, Mr. Chairman. And thank you for your bipartisan focus on how we make the Department more innovative, agile, and capable of adopting the latest technology and software and working with the private sector to remain the most innovative military in the world.

I hope at today's hearing we can explore not just what the Department is doing but what more flexibility is needed and how we can have greater agility. The reality is, we have a challenge of harmonizing this ecosystem, to bring it up to the speed of modern innovation, while operating in our era of great-power competition.

In particular, efforts such as securing the defense industrial base, implementing zero-trust architectures, accelerating the cloud transition and roll-out of a robust identity, credentialing, and access management capability are fundamental.

Two weeks ago, this subcommittee had a very interesting hearing on software development and software acquisition. And, a month ago, the committee held a hearing on accelerating the pace of innovation across the Department.

As we approach the end of this term, I guess what would be helpful to me is a few, two or three, very concrete recommendations, particularly of what the committee can do or needs to do legislatively to help with making the Department more innovative.

Is it, at this point, that Congress has done everything it needs to do and it is more a matter of implementation? Or do you see a role for the committee to continue to do more legislatively? And, if so, what would those recommendations be?

Thank you, Mr. Chairman, and I yield back.

Mr. GALLAGHER. Mr. Sherman, you are recognized for 5 minutes.

**STATEMENT OF JOHN SHERMAN, CHIEF INFORMATION
OFFICER, DEPARTMENT OF DEFENSE**

Mr. SHERMAN. Good morning, Chairman Gallagher, Ranking Member Khanna, and distinguished members of the subcommittee. Thank you for the opportunity to testify before you today.

I am glad to be here with Dr. Martell, as well as General Skinner, as you noted, Director of DISA [Defense Information Systems Agency] and Commander of Joint Force Headquarters-DODIN [Department of Defense information networks].

Together, Lieutenant General Skinner and I lead a team that provides direction, oversight, and technical expertise to secure and modernize the Department's information technology; enhance warfighting command, control, and communications, or C3; manage the DOD's use of electromagnetic spectrum; and cultivate a digital workforce.

We look forward to sharing the progress on the Department's digital transformation efforts and discussing our key priorities for fiscal year 2025.

As we have seen in Asia and Europe, the cyber threats we face today are evolving, and we must keep pace to both support the Nation's warfighters and protect key national-security capabilities.

Protection of our networks and the networks of the defense industrial base is critical. We are laser-focused on zero-trust implementation. And, earlier this year, we expanded eligibility for the Defense Industrial Base Cybersecurity Program that will significantly enhance the cybersecurity posture for these companies.

Cloud computing and software modernization remain central to our IT [information technology] modernization efforts. When I testified last year, the Department was just beginning the enterprise cloud journey, and I am happy to report significant and successful progress.

Through the Joint Warfighting Cloud Capability, or JWCC, DISA has successfully awarded more than 47 task orders over the last year, and over 50 more are in the pipeline right now. We also publish DOD guidance to streamline cloud contracting and reduce contract sprawl across the Department.

In today's environment, and as you all focused in on your hearing last Wednesday, it is critical, more than ever, that we provide DOD personnel with secure and resilient software when and where they need it. We recognize the urgency of this issue and are working hard to ensure we are successful.

Our software modernization strategy and ecosystem of more than 55 software factories are transforming the way DOD develops and delivers this force multiplier. This requires changes to our processes, policies, workforce, and technology. Accelerating the authority to operate, or ATO, and strengthening reciprocity are absolutely key to this effort.

Just as important as the software is ability to operate in any environment. Our adversaries have spent decades investing in capabilities to make the best use of electromagnetic spectrum, and that is critical to defend the Nation. However, we also understand the increasing commercial demand for spectrum and are working with the White House, Department of Commerce, and other interagency partners to explore ways to address increasing Federal and com-

mercial demand for spectrum access without compromising national security.

5G is also critical to both DOD and civilian industry. Last fall, my office became responsible for this mission, and we are accelerating the deployment of 5G on military installations, advancing enterprise capabilities, and addressing resource requirements.

Each of these missions and others are critical to our warfighters and would be impossible without the right people. This past year, we laid the foundations to enable DOD to grow a dynamic and innovative workforce needed to succeed in the 21st century. Our implementation of the DOD Cyber Workforce Strategy is ongoing to ensure we work with industry to recruit and retain the right people with the right skills for the right jobs.

As people are our greatest resource, I understand their interaction with the Department's IT infrastructure, weapons systems, and business systems directly affect the mission and morale of each warfighter, civilian, and contractor. To enhance user experience, we established a Customer Experience Office to harness resources and data to tackle this multifaceted challenge.

Thank you for your consistent and dedicated support and for the opportunity to testify this morning, and I look forward to answering your questions.

[The prepared statement of Mr. Sherman and General Skinner can be found in the Appendix on page 27.]

Mr. GALLAGHER. Thank you.

Dr. Martell.

STATEMENT OF CRAIG MARTELL, CHIEF DIGITAL AND ARTIFICIAL INTELLIGENCE OFFICER, DEPARTMENT OF DEFENSE

Dr. MARTELL. Thank you. Chairman Gallagher, Ranking Member Khanna, and distinguished members of the subcommittee, I thank you for allowing me to testify here today and to share the work the CDAO [Chief Digital and Artificial Intelligence Office] has been doing.

I will read through this, but I want to start by answering the direct question, which is, what have we been doing and how can we make it faster?

We have spent the last year building what I could call a virtuous cycle. That virtuous cycle is delivering value, creating new demand, and then iterating.

And so I will talk through the tools that we have been using to do that. But I think, to answer the direct question at the beginning, we have to continue that virtuous cycle, and I think that is what is going to increase the acceleration and delivering value to the warfighter.

The CDAO is accelerating Defense-wide adoption of data analytics and AI so that the DOD can make better decisions faster, from the boardroom to the battlefield.

We create sustainable change at scale through two functions: leading and overseeing—and this is our Principal Staff Assistant function, mostly through policy guidance and oversight—but also actively delivering capabilities across the full range of the hierarchy of needs. So the hierarchy of needs is how we analyze what needs to get done when.

This enables change at both speed and scale—speed, by delivering apps and products directly to the end user quickly—think both warfighters and running the business of the DOD—and scale, by delivering platforms and services to allow builders at the edge, the owners of the problem, to best solve their problem.

So think about it this way: We are a centralized organization. If our job is to build all of the AI of the Department, that does not scale. We will build onesie-twosie solutions. And we are tackling very large individual solutions—JADC2 [Joint All Domain Command and Control], for example. We can talk about Harbinger and other things that we have been working on. And that is really important for the centralized org with the expertise to drive those issues.

But it is also really important to create the tools, policies, processes and best practices so that the folks at the edge can actually deliver value when they need that value, so they can deliver AI when they need that AI. They are the ones who understand the problem; they are the ones who are going to understand the solution. It shouldn't be only centralized. It has to be distributed as well.

So we have been tackling both of these fronts simultaneously. The first allows for winning the fight tonight. The second allows for sustainability of those wins.

And we do this, as I said, through the hierarchy of needs. The hierarchy of needs for us is that you have to get the data right. So the lowest layer, the foundational layer is: Do we have the right data? Is the data accessible? Is the data understandable? And can people use that data to build apps that provide solutions? So think about a separation between data and apps.

The next level above that is simply analytics and metrics. We spent a great deal of time this year getting people to move from effort-based metrics to outcome-based metrics. And that has allowed for the running of the Department in a way that we haven't seen before. So every monthly meeting with the Deputy, there is a dashboard with the metrics for that Principal Staff Assistant and how well they are doing. And gathering the data for that has been significant.

And on the top of that is AI, because without metrics to know how well you are doing—because, remember, AI is statistics at scale. You measure the past to predict the future. You have to know how well you are predicting the future. To do that, you need the metrics to measure yourself against it, and you need the quality data.

So this hierarchy of needs combined with our agile approach is how we are going to drive the sustainable change through our virtuous cycle.

And that is a bunch of buzzwords, but what do I mean by an agile approach? We have had major success on CJADC2 [Combined Joint All Domain Command and Control] this year, in particular by having data owners and industrial software engineers sitting right next to warfighters, literally in the room, and as those warfighters need something new, the data owners go find that data, and the software engineers change the software, and it is delivered within

days. This sort of iteration, this sort of agile iteration, is what is going to continue to drive that virtuous cycle.

So we deliver by learning by doing, shipping fast and iterating quickly, with warfighters, as I said, developers sitting side-by-side. This is done on real networks with real data to learn and deliver for real warfighters fast.

And we couldn't have done it without working closely with our industry partners. And we have used a lot of the tools that you have given us to be able to build contracts fast and to procure their services very quickly.

So CDAO looks forward to working closely with the subcommittee on these issues and others as we scale DOD's current and future use of data analytics and AI for national security.

Thank you.

[The prepared statement of Dr. Martell can be found in the Appendix on page 42.]

Mr. GALLAGHER. Thank you.

General Skinner.

**STATEMENT OF LIEUTENANT GENERAL ROBERT SKINNER,
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY**

General SKINNER. Good morning, Chairman Gallagher, Ranking Member Khanna, and distinguished members of the subcommittee.

I am honored to be here today and represent the approximately 19,000 personnel who support the missions of the Defense Information Systems Agency and Joint Force Headquarters-Department of Defense Information Networks.

I am also honored to sit alongside Dr. Craig Martell and one of my two bosses, the Honorable John Sherman, a key ally and partner in the campaign to innovate, modernize, secure, and defend the Department's networks, systems, and data to achieve and maintain information superiority.

Each day, we are energized and focused on ensuring the Joint Force is in a position of advantage against any Nation or group that desires to harm us or our allies as we set the globe in the cyber domain.

Along with our key partners within the Federal Government—alleges, industry, research, and academia—we continue to leverage lessons learned from the ongoing conflicts in Ukraine and Gaza; the nefarious activities of our pacing threat, the People's Republic of China; and global cyber events to strengthen our digital technologies and forces.

Through the support of this committee, we have made significant progress over the last year and look forward to highlighting our future plans.

Resiliency, agility, survivability, and velocity are key tenets in describing our initiatives, starting with our Department's flagship Joint Warfighting Cloud Capability contract, which was awarded in December of 2022 and provides access to multiple global cloud fabrics that ensure our warfighters can conduct operations anywhere in the world.

Along with the 47 task orders Honorable Sherman mentioned, we have also successfully deployed an initial overseas cloud capability in support of INDOPACOM [U.S. Indo-Pacific Command] missions.

Recently, we also kicked off a pilot, the Joint Operational Edge, that will deploy hybrid cloud capabilities to remote locations across the globe.

As discussed in the hearing you held earlier this month, it is critical that we ensure that DOD personnel have secure and resilient software regardless of where they are located. We continue to develop agile and modern software development methodologies with templates, tools, and automation in our software factory integration platform which is available to the Department.

Equally important to operational software availability is our perimeter defenses. We have two key pilots ongoing with commercial companies that are increasing our ability to see and counter adversary activity, which are increasing each and every day.

Along with these activities, we are lockstep with the Department's zero-trust strategy through our Thunderdome initiative. In 2023, we deployed Thunderdome to 15 sites on classified and unclassified cyber terrain and will accelerate deployment to more than 60 sites this year.

Thunderdome, which is part of our next-generation network and data environment, will provide defense agencies and combatant commands with improved user experiences while also increasing cybersecurity by knowing who is accessing the network and data, limiting individuals to only that data they are authorized to access, enhanced data analytics through artificial intelligence, and increased segmentation, like fire breaks in houses that prevent fires from spreading.

While we continue to make significant advances, our work is not done. Leaning forward, I believe our new strategic plan outlining the Agency's fiscal year 2024 to 2029 goals sets the North Star to enable best value capabilities to our Department and our warfighters.

A final area to highlight is our commitment to no-fail missions, such as the National Leadership Command Capability. Within our strategy, DISA will deploy an integrated, multiple-level, secure voice and video communications and conferencing capability to provide direct support to senior leaders, including the President, the Secretary of Defense, the Chairman, and the nuclear command and control community.

None of these initiatives are possible without our bold, innovative, and critically thinking workforce. In line with DOD's Cyber Workforce Strategy, DISA has released our Workforce 2025 strategy that outlines key objectives to recruit, retain, and professionally develop our team to ensure the right personnel with the right skill sets are in the right positions.

Our overall readiness, strength and resilience, and warfighter success relies on the strong support that this subcommittee has provided for many years. I am grateful for your support and the opportunity to testify this morning. I look forward to your questions.

Thank you.

[The prepared statement of Mr. Sherman and General Skinner can be found in the Appendix on page 27.]

Mr. GALLAGHER. Thank you.

We will now move to questions.

Dr. Martell, INDOPACOM has pieced together the Joint Fires Network in the absence of a JADC2 solution or operational capability.

Elaborate on how your organization—what you have done to contribute to the JFN [Joint Fires Network]—

Dr. MARTELL. Absolutely.

Mr. GALLAGHER.—and, by extension, INDOPACOM command and control. I guess, put differently, how do you see the joint operating system and CDAO's JADC2 efforts fitting into the JFN?

Dr. MARTELL. Yeah. Thank you for the question, Chairman Gallagher.

We work hand-in-hand with INDOPACOM—with R&E [research and engineering] and INDOPACOM—with research and experimentation and INDOPACOM on JFN. The underlying data layer, which drives the right data to JFN to be able to make the decisions, to be able to close chains, comes from the CDAO. Some of it was theirs already, but they needed a whole bunch more.

We have a team that sits with them, and when they need more data, we help find that data, we help deliver that data, and we help make sure that data is there at speed and scale so that they can use it on a regular basis.

So they were a key part of our last guide experimentation, and it was in INDOPACOM. And the success and some failures in that experimentation was due to that partnership. I am happy to go into deeper about exactly what worked and what didn't work in the closed session, but we are tightly aligned.

Mr. GALLAGHER. Can you elaborate, taking a step back, just elaborate for us laypeople on the difference between the joint operating system and the data integration layer?

Dr. MARTELL. I would say, the joint operating system is part of the data integration layer.

So think about the data integration layer as two major components: a catalog to help you find where data is; and APIs [Application Programming Interface] that allow that data to be served. That is really what—and that data has to, obviously, sit on a cloud somewhere, so the work with CIO [Chief Information Office] is really important there.

So the data is in the right cloud place. The data has an API that allows an application builder to access that data when needed. And it is discoverable. And not only is it discoverable, when it is discovered, it is understood. So there is metadata that describes what that data means, how that data is used, and how that might be ingested into an application that is being built.

JOS [Joint Operation System] does specific things that we had originally contracted them for, and they are now part of that data integration layer. They have data that they are providing, Anduril has data that they are providing, that is part of—that has an API layer and is discoverable through that centralized catalog.

So you want to think about the data integration layer as a multi-vendor, heterogeneous entity that really is the data that is needed, is discoverable and accessible. And so that is what we are driving forward.

Mr. GALLAGHER. And, then, in PB25 [President's Budget 2025], it says that the JOS is moving to production.

I like the idea of CDAO using all sorts of acquisitions authority to move rapidly, taking commercial technology like the JOS through prototyping and into production. But could you elaborate more on how you see the JOS in production?

Dr. MARTELL. I may have to take that for the record or for the closed session, because I don't actually know specifically what we can talk about about what it delivers. But they deliver—and my team can tell me if I am allowed to now.

But they deliver specific information that was necessary for the Joint Fires Network. It is their hardware that is distributed—it is Anduril's hardware that is distributed across the INDOPACOM theater that allows that data to flow easily. And it is discoverable through our catalog and through our sets of APIs.

I think I didn't answer the question more specifically than I did before. Sorry about that.

Mr. GALLAGHER. And you are leaving soon. As you look back, what are the metrics that you would judge your tenure on?

Dr. MARTELL. Massive increase in demand for getting it right. We just did a presentation across the whole Department about the current state of JADC2 and the successes that we had. A year ago, there were a lot of "I don't know what this means," "I don't know what you mean by 'getting the data right,'" "I don't know what you mean by 'having the data accessible to the warfighter at the right time and the right place.'" That is now well understood.

CJADC2—I was very pleasantly surprised, there is no longer an ambiguity, at least within our org, about what CJADC2 is. It isn't a thing. It isn't a system. It isn't even a destination. It is a set of behavioral patterns and the underlying dataflows to support those behavioral patterns.

I mean, CJADC2 is command and control for the 21st century. You do command and control in the 21st century by the right flow of data. The demand for that data flowing correctly has not quite exponentially but geometrically increased, I would say, over the last year and a half. And if there is a win that I am strongly willing to claim, it is that.

Mr. GALLAGHER. And in the 7 seconds I have left, how would you respond just to the articles about the poor command climate surveys?

Dr. MARTELL. Yeah, I think that is great and—that is a great question and a really important one.

We did a very hard task. We took four organizations; we merged them to get four—with very distinct cultures. And we had to break a lot of expectations in doing that. There were lots of people who wanted to do particular things, and we said, "Yeah, no, we are going to look for economies of scale, and we are going to do these things instead." That is a monumental task for any merger and acquisition, and it is going to upset some people.

We have worked really hard over the last year to work with some industrial partners on getting our culture right, on making sure that our teams are being heard, that communication flows better. We did sort of biased execution, maybe, to the expense of communication with our people in the beginning, and I own that. I am looking forward to next month when the new pulse surveys are released, because I feel confident that they will say good things.

Mr. GALLAGHER. Thank you.

Mr. Khanna is recognized for 5 minutes.

Mr. KHANNA. Thank you, Mr. Chair.

Dr. Martell, I see that you worked at Dropbox and Lyft before your service to our country.

Can you describe some of the collaboration with the Silicon Valley technology companies that you have and how that can improve?

Dr. MARTELL. We couldn't have done the job without tight partnership with key companies. Palantir is one. Anduril is another. Databricks is another.

Most of the things—almost everything we do—and then all of the cloud providers, so Google, Amazon—

Mr. SHERMAN. Oracle and Microsoft.

Dr. MARTELL. Oracle and Microsoft. Thank you, John.

Mr. KHANNA. Please keep listing companies in my district. No, I'm just joking.

Dr. MARTELL. I think every Silicon Valley company is in your district, right?

So we couldn't have done it without them. We spent a great deal of time talking to the leaders of those companies to get buy-in for the story that I am telling you now.

Like, what I tried to do was take best practices from Silicon Valley, which is, really, the data is more important than the—the data has to precede the app that is on top of it. It is not more important, but it has to precede—quality data has to precede the app, sit on top of it. Quality data has to precede AI. It is just logically inconsistent otherwise.

And so I vetted this view with all of my colleagues in Silicon Valley. I had many conversations, not just with the big companies but also with lots of startups, to make sure that they were onboard and that they would be willing to engage as we built out this multi-vendor, heterogeneous data-integration layer that would allow for separation of data from apps.

Mr. KHANNA. Thank you. Are there things we can do to improve the collaboration, or do you think it is in a pretty good place?

Dr. MARTELL. Well, I think we still have some work to tackle. I think DIU, the Defense Innovation Unit, is doing a really good job at tackling those. Doug Beck is a really strong hire, and so I am really glad he is onboard.

You know, I have seen an increase in the way we have been interacting with small businesses, for example. Because of the marketplace we have built through Tradewinds, we are now up to 65 nontraditional company contracts, we are up to 75 small business contracts. And many of these are done in 30 to 60 days. And that is because of the authorities that you all have given us.

So we are seeing some growth, we are seeing some inertia increase, but we need that to continue. I mean, I think the biggest takeaway—and, actually, if I am candid, the thing that I feel best about is, at the end of my tenure, people are demanding more of what we are trying to do, and faster.

I 100-percent agree, faster has to happen. 100-percent agree. But I think it is now clear what has to happen faster, which is: getting the data right, having the data flow correctly, being able to inte-

grate with companies as quickly as possible. And it shouldn't be something that we build; it has to be multi-vendor, heterogeneous.

Mr. KHANNA. Dr. Martell, I also see that you have a computer science Ph.D. degree from the University of Pennsylvania.

Now, many people rightfully have been concerned about anti-Semitism, and there is no place for that on college campuses, but some of the rhetoric in this building has gotten pretty excessive. One Member of Congress said, I want to start defunding these universities, and the "rot" in higher education.

Could you talk about what it would mean for our national security and our ability to have a lead in AI if we just started defunding MIT [Massachusetts Institute of Technology], University of Pennsylvania, Harvard, and many of these universities?

Dr. MARTELL. Thank you for that land-mine question, Ranking Member Khanna.

I think it is a tough call. The environment of a university, in order to be effective, has to allow for everyone to be able to think freely.

But I do agree that if we don't continue to fund STEM [science, technology, engineering, and mathematics] the way we need to fund STEM and continue to fund the technology in the way that we need to fund the technology at not just the top universities but at all universities, then that is going to put us behind.

So continuing to fund has to be the case.

Mr. KHANNA. I yield back, Mr. Chairman.

Mr. GALLAGHER. Mr. Gaetz?

Mr. GAETZ. General Skinner, are you a gamer?

General SKINNER. No, sir, I am not.

Mr. GAETZ. No "Madden"? No, like, EA—

General SKINNER. My son is —

Mr. GAETZ. —Sports, "Call of Duty"?

General SKINNER. My son is, but I am not.

Mr. GAETZ. I am not either. But it seems as though a lot of our servicemembers are. I mean, I have seen, a lot of these USOs [United Service Organization], they are building all these great gaming complexes.

And I took interest in a report that we were feeding some of the "StarCraft II" game models into an integration with ChatGPT, and this piece, "AI Surpasses Humans—U.S. Military ChatGPT Outperforms in War Scenario Planning."

And I guess what they did in this case was, they told ChatGPT to function as an assistant to a military commander in this engagement. So I imagine, like, an AI Dwight Schrute, assistant to the regional manager. But it turns out, in changing conflict dynamics, the military assistant turned out to be quite capable.

So, Dr. Martell, you seem to have some familiarity with this circumstance. What can we learn from the integration of gaming models, AI, and military strategy?

Dr. MARTELL. So I will talk less about gaming, because I am not a gamer, but about how we might effectively use tools, generative AI like ChatGPT.

We have been working really hard to figure out where and when generative AI is going to be useful and where and when it is going to be dangerous.

The danger is, it is extremely difficult—it takes a very high cognitive load to validate the output of this model. And so there is a very large demand signal for AI to replace experts and allow novices to replace experts. That is where I think it is dangerous.

Where I think it is going to be most effective is helping experts be better experts or helping someone who knows their job well be better at the job that they know well.

Mr. GAETZ. I don't know, Dr. Martell. We are all on the front end of this wave, but I find a lot of novices showing capability as experts when they are able to access these large language models—

Dr. MARTELL. So, if I can, sir, I think the reason is, it is extremely difficult to validate the output, right?

So, as long as there is a way—I am totally onboard as long as there is a way to easily check the output of the model. Because hallucination hasn't gone away yet. There is lots of hope that hallucination will go away. There is some research that says it won't ever go away. That is an empirical open question that I think we need to really continue to pay attention to.

But, most importantly, if it is a difficult-to-validate output, then it is going to be—then I am very uncomfortable with it.

Mr. GAETZ. Yeah. I mean, I have even used, just in my modest way, like, Claude to audit the hallucinations of ChatGPT and vice versa.

And I can see the young people behind you nodding in the affirmative. So sometimes that can be a check.

And I think you are right on the outputs, I think you are dead there. But I think it is—dead-right—I think it is interesting, though, to think about this in terms of—

Dr. MARTELL. Absolutely.

Mr. GAETZ. —an assistant. And then you think about that in the air domain, in the space domain.

But I want to get to the inputs as well. Because you made a really good point in your testimony about the quality of the data dictating, kind of, the ceiling on this enterprise.

Dr. MARTELL. Right.

Mr. GAETZ. And I envision a circumstance where we are in this room marking up the NDAA [National Defense Authorization Act] and there is a big fight among all the lobbyists for the defense contractors about who owns the data. Right? Just as we see in the large language models, The New York Times and these entities saying, “Well, you trained on our data and our stuff, and so we have some ownership interest in the work product that comes out.”

As you depart government service, on to something else, what advice can you give the subcommittee about how to have as much of that data open-source and acceptable so we don't have a circumstance where, like, Lockheed Martin is saying, “Well, we have to protect our source code—

Dr. MARTELL. That is right.

Mr. GAETZ. —on the F-35” and back to that sort of stuff?

Dr. MARTELL. So I think the right tactic there is to separate stovepipe solutions—which really are data all the way up to the end user—into two layers, a data layer and an app layer, an application layer, and then create two separate marketplaces.

So the app marketplace makes perfect sense. You guys get it. Who is going to open my Word doc? Is it going to be Google or is it going to be Microsoft or some third party? That is the app layer. But then the actual word-processing doc is the data layer.

But you can also build a marketplace in the data layer. If Lockheed Martin had invested a great deal of IP [internet protocol] and work to building out that data layer, well, maybe we pay them for access to that data and figure out interesting contracting ways where they can actually make money selling that data not just to themselves but to other app builders, but require that data be accessible.

So I really think——

Mr. GAETZ. That is a really important point. You know, I hope we are able to get back to it at some point. Because what I worry about is, they will create the cost of that data as so cost-prohibitive so as to vertically integrate all the features of the contract.

And Mr. Sherman, who testified about contract sprawl earlier, I think, is acknowledging that we are going to have to confront that. And I think——

General SKINNER. Yes, sir.

Mr. GAETZ. —it is a sticky wicket.

General SKINNER. I think that is right.

Mr. GAETZ. Thank you, Mr. Chairman. I yield back.

Mr. GALLAGHER. Mr. Moulton.

Mr. MOULTON. Thank you, Mr. Chairman.

Mr. Sherman, I co-led the legislation to establish 988, the new National Mental Health Hotline. And in the first year and a half, calls are up over 50 percent, texts are up over a thousand percent, literally saving thousands of lives.

The Commandant called me last year to share what he has heard from Marines about what a difference it has made in their lives and their units.

I know the leadership of the Department is working on reducing our shocking number of suicides, and one straightforward way to help is to simply make sure that 988 is dialable from all DOD phones. It is a legal requirement that you can dial 911, but not yet 988.

So what can we do to make sure we get there?

Mr. SHERMAN. Congressman, first, thank you for sponsoring that legislation. As Secretary Austin has said, mental health is health, and this is imperative.

So, within the Department of Defense, we have validated its use in the Pentagon, Fort Myer. We even called it from my office to make sure, because, I am going to be honest, the first few times we were doing this, to make sure you don't have to put a 9 in front of it or something like that, to make sure it could work.

So, working with General Skinner, with his DISA hat on, and also Personnel and Readiness, making sure that that guidance is out there.

We are going to continue to validate. And I want to make sure I am clear on this. This is going to be an ongoing process for whether it is at Fort Cavazos or Camp Pendleton or Edwards Air Force Base, wherever a servicemember or civilian is that needs to

be able to get to that number, that we are going to have to continually validate this.

So this is something we have been talking about just recently here, that this is going to be an ongoing process to make sure that 988 is reachable without having to put 1-1 in front of it or 9 or things that I would have had to do at Fort Stewart in calling from the day room down at 15-ADA (ph).

So, sir, this is something that has got our attention for large and small installations alike to make sure we can validate that.

Mr. MOULTON. Once the troops know this number by heart—and we have done a lot to make sure it is publicized on bases—it is going to be important to have it accessible from places like Okinawa and Landstuhl as well. So I hope you will keep your horizons far.

Mr. SHERMAN. Yes, sir.

Mr. MOULTON. Dr. Martell, thank you very much for your time with the Department.

We all clearly agree that we need to invest in AI capabilities for the future. And we also understand, as you have said, that AI is dependent on data.

It is kind of insane to me that American taxpayers have spent more money on the J-35 than any defense system in history, and yet we download its data from many missions and literally throw it out because we don't have a place to store it.

When is this going to stop?

Dr. MARTELL. I am getting all the great questions, aren't I?

That is a great question, and I appreciate it. We call that data "exhaust," where valuable data is being blown out the tailpipe, and there is an example of it.

I don't feel that I have the expertise to answer that question, when it is going to stop. But I can say that we have to continue the demand for quality data to deliver solutions. And I believe that virtuous cycle is going to then start creating the demand to understand how that data can be most effective.

Mr. MOULTON. Well, I would just point out that, if my laptop or my phone told me that I was out of space, I could solve that problem in a couple hours. So I don't expect DOD to move that fast, but the fact that this has taken literally years and you still can't give us an answer I think is a real problem.

Dr. MARTELL. I will have to take the rest of that as a question for the record and get back to you. I am not sufficiently familiar with—

Mr. MOULTON. Okay. Well, it would be very helpful to have a timeline.

[The information referred to can be found in the Appendix on page 55.]

Dr. MARTELL. Okay.

Mr. MOULTON. And then, of course, once we simply retain that data—you have addressed this in some of the other questions members have asked—how are we going to make it safely available not just to, you know, the primes, right —

Dr. MARTELL. That is right.

Mr. MOULTON. —but to some of the leading private-sector companies in AI innovation?

Dr. MARTELL. So I think there are two parts to that: the safely and the available.

From the available perspective, the technology is there. It is the right APIs that have the right limitations of accessibility on them. But it is more about the contracting, to make sure that the folks who have produced the data—I mean, the data is fundamentally the government's data, but then a lot of work goes into massaging that data to make it accessible. And that is IP that should be paid for, in my opinion. But we have to make the contracts clear about what that payment looks like and how it must maintain its accessibility. That is a really big set of work that we have to do.

On the safely accessible part, I defer to my colleagues on how we can use zero trust to make sure that only the right people are accessing that.

Mr. MOULTON. Well, look, I would just point out that, because of civil-military fusion in China, China is doing this today, right? I mean, they have their top AI companies working on their military problems. So this is another thing where we have to have the urgency to get this done.

A quick question on workforce recruitment, Mr. Sherman: How are we going to find someone to replace Dr. Martell who brings the level of academic expertise and private-sector experience to the job?

Mr. SHERMAN. Well, we are certainly going to miss Dr. Martell. He has been a huge combat multiplier.

I think Dr. Radha Plumb, his designated replacement, is pretty darn amazing too. And I think she is going to pick up the baton where he is leaving it there, sir.

Mr. MOULTON. All right.

Thank you, Mr. Chairman.

Mr. GALLAGHER. Mr. Luttrell.

Mr. LUTTRELL. I am glad that you are nodding your head “yes,” Dr. Martell. That puts me kind of in my comfort zone, that somebody is coming in behind you with some expertise to keep widening the road that you have paved.

I picked up on the cross—I call it cross-functional teams, where you have your engineers sitting with your operators, and that dynamic back and forth just lends itself to forward-leaning success. So I am sure the expansiveness of that is growing, yeah?

You lead the data integration layer for CJADC2, correct?

Dr. MARTELL. Correct.

Mr. LUTTRELL. This is likely, in my opinion, the most critical position in that Department. Given it is centrality in moving and exchanging data between and within each services, this likely requires not just coordination but direction to the various stakeholders.

Can you explain what directive authority you have been afforded in building the data integration layer?

Dr. MARTELL. That is a great question, in terms of the authorities. I can tell you what we have been doing, and then I can take as a question for the record what authorities we have been doing them under.

Mr. LUTTRELL. Okay.

Dr. MARTELL. But, right now, we have been building out the prototype of what it would mean for the hardware to support the flow

of data across combatant commands, for example, so combatant commands can have a unified picture of what is going on in the world.

We are doing that as the key learning exercise—and we do it every 90 days through these guide exercises—as the key learning exercise to understand what combatant—and through war-gaming—what combatant commanders would need to see and what all of the components under the combatant commanders would need to see, would need to exchange, and how data would need to flow in order for it to go from swivel-chair and PowerPoint and email to digital dataflows as that information goes across the combatant commands and within the combatant commands.

So the next step, which we should be doing within the next 3 to 6 months, is building out a set of requirements so that industry can help—I mean, we have been doing this with key industrial partners, mostly Palantir and Anduril, but it needs to be—it needs—and the technology that we have built we are leaving behind. It is there; it is available. That is why we call it a minimum viable capability. It is viable. We then need to build out clear requirements that allow other industrial partners to join in and to expand that data integration layer and then also to expand those capabilities.

Mr. LUTTRELL. That sounds like something this—we might need to tweak this a little bit as you are starting to transition something that you wish you would have had, that the incoming can have. That is something you need to address with this committee, I would say.

Dr. MARTELL. Absolutely. And I would prefer to take this as a question for the record—

Mr. LUTTRELL. Yes, sir. Absolutely. I understand.

Dr. MARTELL. —and get you an absolutely clean—

Mr. LUTTRELL. I understand.

Dr. MARTELL. —clean definition of what we need.

[The information referred to can be found in the Appendix on page 55.]

Mr. LUTTRELL. Mr. Chairman, are we doing two rounds or just one?

Mr. GALLAGHER. I was planning on one, but—

Mr. LUTTRELL. Okay.

Mr. GALLAGHER. —do you need two?

Mr. LUTTRELL. I could use about four or five. All right.

Dr. Martell, can you explain what would be the consequences of affording your position with some sort of directive authority over the services and their development of CJADC2 solutions?

Dr. MARTELL. I am not a fan of that. And I am not a fan of a hard authority there. And I may be saying the wrong words because I haven't quite got up, in the 2 years I have been here, in all the bureaucratic lingo I should.

I think the services understand—in general, let me just say, in general, the center should provide oversight and policy and best practices. The edge knows their problems best.

So solving the problems from the center and imposing it upon the edge I think is dangerous. It is going to create one-size-fits-all solutions that don't—

Mr. LUTTRELL. You should write that down and put it on a plaque so we can hang it in every room in this building.

Dr. MARTELL. I will take that as an activity for the record, sir.

Mr. LUTTRELL. Okay.

Dr. MARTELL. That was a joke. We are not really going to do that, guys.

And the services understand what they need better than OSD [Office of the Secretary of Defense] is going to understand what they need. But there does have to be authority about the interface. So data is going to have to go down into the services, and the right kind of data is going to have to flow up out of the services.

So where we have been spending our energy with the services—say, project convergence or with overmatch—is figuring out how would that data flow. We still have the policy questions or the workflow questions about what data should flow.

So I actually see—what we have been doing, to be clear, is putting the tech before the policy. The tech to allow the data to flow is going to force the right questions: What data should flow? Right?

Like, we can't answer Title 10 and Title 50 combinations a priori. We can't just start with that. We have to watch the data flow, and then there is going to be an increased demand for data to flow, and the right data to flow. And then we can say, "Well, now, that is a policy issue that we can tackle," or, "That is a small version of the policy issue for just that one piece of data."

That is the way that the change is going to happen. The change is not going—my very strong opinion—the change is not going to happen by some large, a priori view, philosophical view, of the way the world should be and then trying to implement that.

Mr. LUTTRELL. Okay. Thank you, sir.

Mr. GALLAGHER. Dr. McCormick.

Dr. MCCORMICK. Thank you, Mr. Chair.

I find it fascinating, we just had our first AI task force meeting just two floors away from us, literally right in line with us. And there is so much focus on this technology right now, it is just unbelievable, from every aspect of, whether it be cybersecurity, defense, mechanical applications, labor force, education, law and what do we consider legal and how do you verify facts, and then of course our security.

This is such a comprehensive issue right now that everybody is focused on right now. I am just going to kind of dive in on a more broad scope so you can give me some more insight into how you are approaching it.

Dr. Martell, much like the computer power and data storage capacity, artificial intelligence advances at an increased rate right now—obviously, exponential rate.

What challenges does this rate of acceleration—in other words, as we are trying to keep up legislatively and regulatory-wise, what does this acceleration create for integrating data, artificial intelligence, and digital solutions for the DOD and how it applies, like, just trying to keep up with this pace?

Dr. MARTELL. So it is remarkable. And I will say, in my 30-year career, this is the most exciting time to be an AI expert. The science has been really remarkable even just the last 5 years, but if you go back 15 years, it has been amazing as well.

I don't know if the science supports the marketing, though. So I think one is to be—"skeptical" is the wrong word. I am very bullish on this technology. But I think it is important to be skeptical about—or to verify—"trust, but verify," if I can quote someone, the claims of the marketing. So that is one.

Number two, I think it is extremely important to not see this as a monolithic technology, which is how it is sold: Get this thing; if we have it, we win, and if they have it, we lose. And I think that is fundamentally flawed. It is neither a panacea, nor is it a Pandora's box.

So if we have it, it doesn't mean every problem we want solved will be solved. And if they have it, it doesn't mean every fear that we have will come to pass. We always have to think about it on a use-case-by-use-case basis, as we always have with any technology.

So the reassurance is, it is just a technology. It will work in some use cases; it won't work in other use cases. We have to have quality data and evaluation metrics to be able to say it is working now or it is not working now.

So I get extremely frustrated with my colleagues in industry who pitch it as magic. I actually think that is the case often. But then when you ask them about the use cases, they have a clear set of small use cases that they know how to measure and are effective: information retrieval via RAG, or first-draft generation, or a number of things which we all feel fairly confident are working well.

But the, sort of, pitch that it is going to reason for us, it is going to solve our problems, we are going to be able to do away with brains and use this instead, that is just way-overhyped.

Now, last year, I think that hype was greater. I think we have all learned in the last year where that hype is starting to come down, and that is making me very happy.

Dr. MCCORMICK. So you mentioned a couple things, claims of marketing and also maybe—I would dispute one thing that you said, because we talk about them having it, us not having it. When a country literally talks about taking over an island that produces basically 100 percent of our AI chips and we don't have a backup, that is kind of a denial of one from the other. And it is different than what you were discussing, I understand—

Dr. MARTELL. No, and I am 100 percent—look, the underlying hardware—for example, the CHIPS [Creating Helpful Incentives to Produce Semiconductors] Act is the right direction to go, because we need to be—that, I think, is a national-security issue, the ability to generate the underlying infrastructure and the underlying data that is going to allow this to be successful. I just meant the models themselves, we have a gap between the science and the marketing.

And one of the things our organization has been doing in Task Force Lima is trying to rationalize that gap. We are building what we are calling a maturity model, very similar to the autonomous driving maturity model, so, you know, Level 1 through Level 5 autonomous driving. That is a really useful model, because people have claimed Level 5 but, objectively speaking, were really at Level 3, with a couple folks doing some Level 4 stuff.

Dr. MCCORMICK. As an ER [emergency room] doc, I am all for kids not driving in cars, figuring out how to do it safely. But I will

say, from a military aspect and my military experience, I am very concerned about the kill chain and what it could mean to us when we have disruptive Chinese technologies that are literally competing with us at this cybersecurity level. That really worries me the most.

I don't know if—

Dr. MARTELL. Sir, I would like to—if I could respond?

Dr. McCORMICK. Sure.

Dr. MARTELL. I am 100 percent in agreement. So I am not saying we don't have to worry about specific use cases. We do have to worry about specific use cases. We just shouldn't worry that it is monolithic.

So, in particular use cases, we should do what we always do: evaluate what our adversaries can do, evaluate what we can do, invest in ways that we can do it better, and invest in ways in which we can maybe contribute to our adversaries not doing it so well.

My only caution was, don't think about it as a scary monolithic technology. Think about particular use cases, and then do the right evaluation of where they are and where we are and invest accordingly.

Mr. GALLAGHER. Mr. Fallon.

Mr. FALLON. Thank you, Mr. Chairman.

I knew it was going to be a good day when I walked in and I saw so many Air Force folks here, being a former Air Force member.

Dr. Martell, what concerns me about a conflict with a near peer—and, obviously, talking about China, Taiwan—and a concern really of everyone on the committee and everybody and all the witnesses is the tremendous potential for loss of life.

Another thing that really bothers me is, when you are looking at war games, where there are some scenarios where we lose in just a very short timeframe a thousand fighter aircraft. That is devastating. And to avoid that kind of a catastrophic loss, I think we need to employ more unmanned aircraft, most notably, of course, autonomous platforms—

Dr. MARTELL. Agreed.

Mr. FALLON. —for not only strike purposes, for sustainment as well.

Dr. MARTELL. Uh-huh.

Mr. FALLON. To do this, the DOD needs to not only invest in hardware but, of course, software—probably even more importantly, the software. So that exists in the commercial space, but companies like Amazon don't have the requirement to operate in GPS-denied environments like the military.

So the question I want to ask you is, what do you think the significance of autonomous unmanned air platforms will have on helping us win a future near-peer fight? And are we doing enough to get where we need to be?

Dr. MARTELL. I completely agree with you; I think they are going to be extremely important. And I think we have to continue to drive that forward.

One of the things the CDAO is doing is supporting the Replicator initiative by creating a sandbox, if you will, where companies can come, using our data, to evaluate the success of their unmanned

aircraft software with respect to the scenarios that we think are going to be effective.

So we are strongly supporting this. Part of what we call “AI scaffolding” that we are building out, part of this way in which we are trying to help scale the Department by giving tools to folks closer to the edge is this Replicator, this Replicator sandbox.

And so we will provide data to that, we will provide scenarios. I am pretty sure—I will double-check—that we are going to provide some software for that. And then the folks who are part of the Replicator initiative will come and try out their software, their prediction, their detection on our data.

So we think it is really important, and we are strongly supporting it.

Mr. FALLON. Could you talk a little bit more about that—you mentioned the AI scaffolding?

Dr. MARTELL. So, you know, as I mentioned in my opening remarks, we really see our job as twofold. One is immediate help to the warfighter; and building out tools, processes, policies, best practices that will allow other folks, the ones closer to the problem, to easily build the solution to the problem. Because a centralized team, it cannot build everything, right? As we talked about before, that creates a one-size-fits-all solution.

Part of our support to be able to scale is what we are calling “AI scaffolding.” So AI scaffolding includes things like the ability to do data labeling as a service. Because knowing what you want to detect means humans have to label that data. That is very difficult. Most teams closer to the edge won’t know how to do that, so we want to provide contracting and expertise to allow them to do that.

Data transformation is a service. The data that has to come into your problem is going to be in a thousand different formats. The amount of work to transform a PDF, a Word doc, et cetera, et cetera, et cetera, into structured data that you need is pretty massive, and that will take up, for the folks on the edge, all of their time. We want to be able to provide services like that.

The building of the model, we strongly believe that should be—because our IP is the data. The government’s IP is the data. We strongly believe the building of the model should be contracted to industry. But on the other side—and we will provide those tools, those contacts, those ability to build, you know, initial models yourself. That is part of our AI scaffolding. The final model should probably be built by absolute experts in this field.

And, then, on the right side of the model building, we think very hard about model monitoring. So one of, I think, the biggest issues that industry just started tackling I would say 5 years ago, 5 to 10 years ago, and government is behind on is, after we ship a model, does it continue to bring value?

Well, remember, AI is statistics at scale. We gather data from the past to predict the future. In a warfighting scenario, the future changes; it doesn’t look like the past. So a model trained on a pre-warfighting scenario is going to start to degrade as the world changes in a fight. How do we measure that degradation? How do we retrain to get that model back up to where we need it to be?

So that is the model monitoring piece. And I wish we had gotten further on that in the 2 years I have been here, but that is going

to be my biggest charge for Dr. Plumb, is really focus on how do we model and measure the value of models over time.

Right now—and it was this way in industry 5 years ago—they are shipped and we forget. They are shipped and we continue to believe. We don't forget. We just continue to believe.

So our contracting, for example, should include model monitoring. The way we deliver the model should include the ability to monitor it.

And so we have done a lot of thinking about this. We need to move out faster on actually executing on it.

Mr. FALLON. Okay.

Thank you, Mr. Chairman. I yield back.

Mr. GALLAGHER. Great.

We will now go into the classified session, which will be upstairs in 2337 Rayburn. I know there were a variety of questions that were not answered because of classification, so we look forward to getting into those. And we will see you up there in a few minutes.

With that, the unclassified portion is adjourned.

[Whereupon, at 9:57 a.m., the subcommittee proceeded in closed session.]

A P P E N D I X

MARCH 22, 2024

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

MARCH 22, 2024

STATEMENT BY

JOHN B. SHERMAN

DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER

LT GEN ROBERT J. SKINNER

DIRECTOR, DISA

**COMMANDER, JOINT FORCE HEADQUARTERS-DEPARTMENT OF DEFENSE
INFORMATION NETWORK**

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

**SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES, AND
INFORMATION SYSTEMS**

ON

**DEFENSE IN A DIGITAL ERA: ARTIFICIAL INTELLIGENCE,
INFORMATION TECHNOLOGY, AND SECURING THE DEPARTMENT OF
DEFENSE**

MARCH 22, 2024

Introduction

Good morning, Chairman Gallagher, Ranking Member Khanna, and distinguished Members of the subcommittee. Thank you for the opportunity to testify before you today. Alongside me is Lt Gen Robert Skinner, Director of the Defense Information Systems Agency (DISA) and Commander of Joint Force Headquarters-Department of Defense Information Network. We look forward to sharing the current progress on the Department's digital transformation efforts.

Chairman Gallagher, I look forward to working with you and this committee to achieve bold action and strengthen our position in key digital transformation areas. The leadership from this committee, through multiple National Defense Authorization Acts (NDAA), has empowered the Department of Defense (DoD) Chief Information Officer (CIO) to manage the Department's information technology (IT) portfolio, including oversight of each of the Military Departments (MLDEPs) and Defense Agency's IT and cybersecurity's budgets.

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

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

Enabling Secure Warfighting IT Capabilities

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

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

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

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

Cryptographic Modernization is another enduring effort essential to our intelligence, information, and warfighting platforms. The potential development of a viable quantum computing capability increases the risk of our adversaries acquiring this technology to disrupt and compromise our National Security Systems (NSS). The Department must develop modern, quantum-resistant encryption solutions to outpace the threats from our adversaries. The DOD's current Cryptographic Modernization 2 initiative is designed to address a large portion of these concerns.

Securing the Defense Industrial Base

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

The CMMC Program will provide a mechanism for the Department to validate DIB compliance with the implementation of previously established cybersecurity requirements on their unclassified information systems that process, store, or transmit federal contract information (FCI) or controlled unclassified information (CUI). The CMMC Program assessments will be conducted against a scaled set of cybersecurity requirements that are based on the criticality and sensitivity of unclassified information needing protection.

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

Modernize DoD Information Networks

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

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

Improving User Experience

The Department must take an enterprise-wide approach to improve user experience and enable the faster delivery of IT capabilities. We are committed to modernizing the digital backbone that supports the warfighter by accelerating the DoD enterprise cloud environment, modernizing business systems, optimizing networks, and buying down technical debt. These efforts will improve user experience by making critical IT infrastructure investments to reduce latency and improve cybersecurity while leveraging cloud for speed, agility, and scalability in support of emerging capabilities and mission readiness.

Accelerate the DoD Enterprise Cloud Environment

Cloud computing remains a fundamental component of the Department's global IT infrastructure and modernization strategy. With battlefield success increasingly relying on digital capabilities, cloud computing provides the IT platform needed to satisfy the warfighter's requirements for rapid access to data, innovative capabilities, and assured support.

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

JWCC provides enterprise-level delivery of commercial cloud services and technology from the strategic to the tactical level, to include austere and Outside the Continental United States (OCONUS) environments. Working with Cloud Service Providers (CSPs), the Department now has access to multiple, global fabrics that ensure our warfighters can conduct operations anywhere in the world. Additionally, DISA has expanded Stratus Private Cloud to OCONUS to enable hybrid cloud deployments overseas.

The current crisis in Ukraine and CJADC2 experiments demonstrate the need for rapid extension of enhanced edge computing capabilities globally to reduce network latency, enable advanced data processing such as AI, and improve operational resilience. The DoD CIO, CDAO, and Under Secretary of Defense for Intelligence and Security are engaged with the Combatant Commands (CCMD), the MILDEPs, and forward deployed partners to deliver the latest cloud computing and communications technologies to meet these requirements.

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

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

Through strong partnership with DoD Components our Cloud and Data Center Optimization initiative enables the Department to achieve a more agile and resilient defense posture. We continue to facilitate the modernization of DoD application/systems, close legacy data centers, and prepare to support emerging capabilities. This initiative focuses on the migration of applications/systems from thirteen organizations to more optimal hosting environments and optimizing or closing vulnerable legacy data centers.

DoD Software Modernization

The Department's Software Modernization Strategy highlights our ability to adapt increasingly relies on software and the ability to deliver secure and resilient software at speed of mission, while ensuring software supply chain control. Transforming software delivery times from years to minutes requires significant changes to our processes, policies, workforce, and technology. The Department released the Software Modernization Implementation Plan in March 2023, identifying key activities, milestones, and responsibilities for driving process improvements and new capabilities to achieve the Software Modernization Strategy goals.

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

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

delivery of software capability while monitoring for any changes in security and enables us to integrate the cybersecurity and cloud-native technologies into the DoD computing platforms used to integrate software development and system operations for accelerated capability delivery. Our workforce and process transformation are aiming to change the DoD approach to offer flexibilities for the recruitment, retention, and development of software professionals across the Department and give them an ecosystem like what they would find in industry to deliver the capabilities we need in DoD. The Department is more than halfway through the FY23-24 Software Modernization Implementation Plan and is beginning development of the follow-on plan for FY25-26.

Defense Business Systems Modernization

DoD must deploy an enterprise approach to deliver modern business capabilities throughout the Department in an increasingly digital landscape. Business systems, which offer common functions across organizations like health, logistics, human resourcing, and training, offer an opportunity to ensure that modern and integrated business processes are in place to support the mission. We are actively working to identify opportunities to consolidate or streamline business functions and data at the enterprise level by improving our processes, enabling data integration, and reducing complex system interfaces. These enhancements will lead to a faster response to mission and provide business data for holistic decision-making. Our enterprise, data-driven Defense Business Systems (DBS) portfolio management approach will identify modernization and drive rationalization across the portfolio to transform the way the Department does business.

The Department is committed to managing DBS as a strategic asset and will use the annual certification process to ensure our DBS portfolio aligns to the strategic priorities and direction of the Department. We are driving to fundamentally transform Department processes to enable a highly efficient business environment that effectively supports our national defense priorities.

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

Budget certification authorities and the Capability Programming Guidance

In accordance with 10 United States Code (U.S.C.) §142, the DoD CIO annually executes its budget and certification authority. An annual Capability Programming Guidance (CPG) is provided to components, ensuring a clear, manageable, and repeatable process to review the proposed components' budgets for those capability areas under my statutory authority. This guidance identifies investment focus areas for the DoD CIO's assessment and is consistent with the National Defense Strategy and Defense Planning Guidance. The document continues to improve by focusing on outcome-based metrics & critical capabilities. In conjunction with the Department's broader budget guidance, the components build their budgets, which are then

assessed against the priorities identified in our CPG.

The DoD CIO successfully completed six fiscal year (FY) budget assessments and determinations, beginning with the FY 20 President's Budget. The certification review process identifies capability areas at risk. We then work with the MILDEPs, and other components, to address these risks areas in future budgets.

Warfighting Command Control and Communications

The essence of military effectiveness, particularly in planning, coordination, and control across the spectrum of the Department's missions, is fundamentally rooted in Command, Control, and Communications (C3) systems. These systems serve as the backbone, delivering the critical information necessary for the seamless execution of operations. We are at the forefront of charting the path for the future development, implementation, fielding, and sustainment of strategic and tactical C3 capabilities. This leadership is exemplified through initiatives such as the Global Command and Control System, ensuring unfettered access to the Electromagnetic Spectrum, pioneering advanced Electromagnetic Battle Management strategies, and spearheading the integration of 5G technologies directly to the warfighter. These initiatives are not just components of our strategy; they represent critical capabilities that are prioritized within the enterprise, underscoring our commitment to maintaining and enhancing the operational effectiveness and technological superiority of our forces.

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

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

Electromagnetic Spectrum

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

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

Spectrum provides the critical connective tissue to that enable all-domain operations and represents a natural seam and critical vulnerability across Joint Force operations. China and

Russia have taken significant steps to challenge U.S. control of the spectrum and seek to exploit U.S. vulnerabilities in the spectrum. Ensuring the U.S. military can train and operate in the spectrum—both at home and abroad—is a strategic imperative.

Spectrum Sharing

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

As the Department’s senior official responsible for coordinating across the Electromagnetic Spectrum (EMS) Enterprise, we are employing and refining our governance processes to ensure synchronization and harmonization of all developments and activities necessary for the successful implementation of the 2020 Electromagnetic Superiority Spectrum Strategy (EMS3). The C3 Leadership Board and the EMS Senior Steering Group has broad participation from stakeholders across the Department, and work to drive towards the EMS3 vision of achieving freedom of action within the EMS at the time, place, and parameters of our choosing while denying the enemy the same.

The DoD supports efforts to ensure U.S. dominance in 5G and next-G development. Previous DoD success in making spectrum available for shared commercial use, including the groundbreaking Citizens Broadband Radio Service, are testaments to this enduring commitment. DoD maintains numerous operational equities throughout the spectrum which must be preserved to enable DoD the ability to protect the homeland, test equipment, train for overseas contingencies and operate in all domains.

The Department acknowledges it cannot achieve spectrum superiority without a whole-of-government, whole-of-industry, and whole-of-nation commitment. Accordingly, we also continue robust engagement with our partners in the interagency, industry, and academia to deliver the best spectrum outcomes for the Department and the Nation.

Electromagnetic Battle Management (EMBM)

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

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

5G

The DoD CIO assumed leadership of the 5G mission and the 5G Cross-Functional Team (5G CFT) on October 1, 2023, in accordance with the FY 2021 NDAA. In this role, CIO is focused on guidance, fielding and implementation of mature 5G capabilities to the warfighter. CIO leads 5G efforts through contributions to international standards development organizations and by identifying and providing implementation guidance for both dual-use commercial and military focused 5G technology applications that provide the optimum return on investment to the Department. CIO also continues to coordinate with the Under Secretary of Defense for Research and Engineering (USD(R&E))'s FutureG office on 5G prototypes / research and development. CIO's current focus is on transitioning the R&E pilots/prototypes to the Services, creating process improvements to accelerate the deployment of commercial 5G on all military installations in accordance with the FY23 NDAA, advancing enterprise capabilities and associated security policy and infrastructure, and addressing resourcing requirements to support the MILDEPs in their implementation of 5G information and communications technology on installations and in tactical and expeditionary use cases.

Positioning, Navigation, and Timing

The DoD CIO is fully engaged in leading the implementation of the Department's positioning, navigation, and timing (PNT) strategy to provide robust and resilient PNT for the Joint Force. This is critical to enabling advanced weapon systems to function in today's highly contested navigation warfare environment. Current efforts are focused on modernization of the Global Positioning System (GPS), including acquisition, and fielding of GPS M-code equipment, modernized GPS satellites, and the next generation operational control segment. To ensure that PNT is accessible to support international U.S. and coalition operations, resilience efforts also concentrate on alternative and complementary capabilities to GPS to provide multi- source PNT in a modular open system approach (MOSA).

To date, the Services' accomplishments include the fielding of GPS M-code ground receivers in key systems that include the Army's Mounted Assured PNT System, or MAPS, which is in the Patriot System, currently in South Korea. The Navy has started fielding the GPS-Based Positioning, Navigation and Timing Service, known as GPNTS, and Non-GPS Aided PNT for Surface Ships or NoGAPSS into the surface fleet. The Air Force is developing the MOSA compliant Resilient Embedded Global Positioning System Inertial Navigation System (REGI) for use in critical DoD aviation platforms. The Navy and DISA are engaged in a joint effort to achieve global timing resiliency through the Critical Time Dissemination initiative and Defense Regional Clocks. DISA is continuing to deploy advanced clock suites and refresh initial configurations to achieve a distributed timing holdover capability.

Enterprise Satellite Communications Modernization

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

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

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

The US Space Force working with DISA has begun the implementation of the Enterprise Satellite Communications Management and Control (ESC-MC) Reference Architecture; they are coordinating closely on the implementation and on hosting the resulting services within the JWCC to optimize security as well as enabling authorized access. Their focus will result in an initial roll-out of capability during FY 2025. The implementation requires changing decades-old analogue business and operational processes used to allocate SATCOM and creating the necessary rules- based processes to deliver machine-to-machine information flows allowing SATCOM resource allocation in minutes and seconds.

National Leadership Command Capability

I want to emphasize a capability at the forefront of the Department's highest priority missions. This three-part capability is the National Leadership Command Capability (NLCC), comprised of Presidential and Senior Leader Comms (P/SLC), Continuity of Operations/Continuity of Government Comms (COOP/COG Comms), and Nuclear C3. Our NLCC customers, to include Congress and the President, utilize C3 systems that provide common capabilities used across operational environments. These communications are critical to ensure our government and operations continue through any adversity.

DISA is committed to deploying an integrated Multiple Level Secure Voice and Video communications and conferencing capability to provide direct support to the NC3 community. This system will utilize existing IT infrastructure at all security classification levels in alignment with Department efforts to prioritize command and control thru modernization and consolidation.

I am fully committed to deliver an improved, modernized National Leadership C3 System, to meet the needs of all NLCC customers. The substantial efforts DoD CIO, DISA, the Services, and the other DoD components are conducting to secure and modernize our NLCC infrastructure.

Cultivate a Digital Workforce

The pivotal achievements and initiatives undertaken by the Department, ranging from user experience enhancements to software and defense business systems modernization, hinge fundamentally on the presence of a skilled and motivated workforce. Recognizing this critical dependency, we have embarked on a strategic mission to cultivate such a workforce through the implementation of the DoD Cyber Workforce Strategy that is designed to identify and bridge workforce gaps, ensuring that we are prepared to meet the challenges of today and tomorrow. Further amplifying our efforts to secure top talent, the introduction of the Cyber Excepted Service has significantly increased our flexibility in attracting and retaining the

specialized skills necessary for our mission's success. Complementing these measures, a comprehensive outreach program has been developed, aimed at drawing in the diverse abilities needed to fulfill our objectives. Together, these initiatives underscore our commitment to fostering a thriving workforce that can propel the Department towards its goals.

Cyber Workforce Strategy

The DoD Cyber Workforce Strategy, released in March 2023, and its implementation plan released in August 2023, remains a top priority for this office. Our goal is to address workforce gaps by recruiting top-tier cyber professionals, expanding our cyber workforce, and enhancing the skills of our existing talent. This initiative is crucial for safeguarding our digital and critical infrastructures, ensuring they are operated securely to defend against cyber threats and protect our data from adversaries.

Implementing a comprehensive approach involves consistent capability assessment and analysis processes to anticipate force requirements effectively, alongside instituting an enterprise-wide talent management program aimed at aligning force capabilities more closely with present and future needs. This effort also entails cultivating a cultural transformation throughout the department to enhance personnel management practices on a broader scale and promoting collaboration and partnerships to enrich capability development, operational efficiency, and career advancement opportunities across the organization.

To provide guidance we released the third publication in the DoD Cyber Workforce policy series to set the foundation for managing, identifying, qualifying, and upskilling our workforce according to the DoD Cyber Workforce Framework (DCWF). The manual plays a crucial role in our workforce by setting forth the qualification standards for every DCWF work role, ensuring that personnel assigned to cyber positions possess the capability to meet mission demands effectively.

Cyber Excepted Service

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

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

Outreach / Development / Retention

Professional development, through education and training, plays a vital role in supporting and enhancing our cyber workforce capabilities. We have several ongoing partnerships and rotation programs to provide professional development opportunities to our workforce.

The Department is working to determine the resource requirements to establish a central program office for cyber academic outreach. This office will oversee cyber-focused engagement programs, enhancing coherence, coordination, and management across the enterprise. Serving as the consolidated focal point for engagements between the Department of Defense and academic institutions regarding cyber-related matters, its objective is to streamline processes and establish a clear pathway for academic institutions seeking engagement with the DoD.

In accordance with the DISA Workforce 2025 Implementation Plan, DISA is conducting outreach and shaping curricula in partnership with our academic and private industry partners, to strengthen the talent pool with training and education necessary to meet DISA and the DoD's cyber and IT mission. The agency, in collaboration with academia and industry, continues to address gaps in the areas of IT, cybersecurity, engineering, and cloud computing. In doing so, this collaboration fosters knowledge transfer to future workforce candidates of the DISA and DOD mission and opportunities available to them, as well as an advanced understanding of key skill areas necessary to be successful in achieving the DISA and DOD mission.

CIO also administers the DoD Cyber Service Academy, formerly known as the DoD Cyber Scholarship Program (DoD CySP), which grants scholarships to students pursuing cyber-related degrees at designated institutions. Recipients of these scholarships are afforded opportunities for hands-on experience through a DoD internship, providing invaluable exposure to DoD cultures and agencies. This approach not only enhances the qualifications and capabilities of our workforce members but also initiates the clearance process for interns, ensuring that applicants are pre-cleared before commencing full-time employment.

We administer the Office of Personnel Management's Federal Rotational Cyber Workforce Program (FRCWP) for the DoD cyber workforce as well. The FRCWP enables cyber-coded government civilians to hone or develop cyber knowledge and skills through applying for, and serving in, rotational details outside their home agencies across the federal government. Rotations promote intra-agency and interagency knowledge sharing, integration and coordination of cyber practices, functions, and personnel management.

Finally, in furtherance of the federal government's Tech to Fed initiative, DISA is partnering with private firms to modify the course curriculum to meet DISA and JFHQ-DODIN requirements for cyber professionals. DISA and JFHQ-DODIN are providing technical and practical ways for veteran candidates to enroll in cyber related programs to graduate more highly qualified potential future employees for cyber related positions, with an understanding of the critical importance specific skill areas have in bolstering our national security posture.

Conclusion

It would not be possible to continue all this work without the consistent and dedicated support of this subcommittee and partnership with Congress. I am committed and I know Dr. Martell and Lt Gen Skinner dedicated in our combined mission of ensuring that our nation continues to be a leader in the digital landscape and combat any challenges to our national security. I look forward

to continuing to work with you all. Thank you for the opportunity to testify this morning, I look forward to your questions.

Mr. John Sherman
Chief Information Officer,
Department of Defense



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.



Lieutenant General Robert Skinner
 Director, Defense Information Systems Agency

Lt. Gen. Robert J. Skinner is the Director of the Defense Information Systems Agency and the Commander of the Joint Force Headquarters-Department of Defense Information Network.

As Director of the Defense Information Systems Agency, Lt. Gen. Skinner manages a global network and leads nearly 19,000 service members, civilians and contractors who plan, develop, deliver and operate joint, interoperable command and control capabilities and defend an enterprise infrastructure in more than 42 countries. This mission directly supports the President, Secretary of Defense, Joint Chiefs of Staff, combatant commanders, U.S. Department of Defense components, and other mission partners across the spectrum of, competition, combat and combat support operations.

As Commander of Joint Force Headquarters-Department of Defense Information Network, he is charged with leading unified action across DoD to secure, operate and defend the DoDIN. He leads the establishment of DoDIN priorities and directs threat-informed actions through formal planning and future operational initiatives, as well as the command and control of daily unified network operations, cyber security actions and defensive operations on the DoDIN.

He was commissioned through Officer Training School (second honor graduate) in 1989. He has served in various tactical and fixed communications assignments, plans, policy and resource staff work. He has commanded at the squadron, group, wing and Numbered Air Force (NAF) levels and served on the staffs at a NAF, major command headquarters, Headquarters Air Force and the Joint Staff. Prior to assuming his current position, he was the director of Command, Control, Communications and Cyber at U.S. Indo-Pacific Command on Camp H.M. Smith, Hawaii.

He earned a bachelor's degree in computer science (summa cum laude) from Park College in Parkville, Missouri, and a master's degree in computer science with honors from Oklahoma City University in Oklahoma City, Oklahoma.

His awards and decorations include the Defense Superior Service Medal with oak leaf cluster, Legion of Merit with oak leaf cluster, Bronze Star Medal, Defense Meritorious Service Medal, Meritorious Service Medal with four oak leaf clusters, Navy Commendation Medal and Air Force Achievement Medal with oak leaf cluster.

CHIEF DIGITAL AND ARTIFICIAL INTELLIGENCE OFFICER
Dr. Craig Martell
Statement for the Record
House Armed Services Committee
Subcommittee on Cyber, Information Technology, and Innovation
March 22, 2024

Chairman Gallagher, Ranking Member Khanna, and distinguished Members of the Subcommittee, thank you for the opportunity to testify before you today. This is my second appearance before the Cyber, Information Technology, and Innovation subcommittee, and I look forward to sharing the ongoing efforts of the Chief Digital and Artificial Intelligence Office (CDAO) and the broader collaborative teaming within the Department of Defense (DoD).

The Deputy Secretary of Defense (DSD) established the CDAO in February 2022, bringing together the authorities and resources of previously separate organizations, including the DoD Chief Data Officer (CDO), Joint Artificial Intelligence Center (JAIC), Defense Digital Service (DDS), and Advancing Analytics (ADVANA) Office.

The DSD charged the CDAO with the mission of accelerating DoD adoption of data, analytics, and AI from the boardroom to the battlefield. This includes the following as outlined in the *DoD Data, Analytics and Artificial Intelligence Adoption Strategy*:

- Lead and oversee DoD's strategy development and policy formulation for data, analytics, and AI.
- Work to break down barriers to data and AI adoption within appropriate DoD institutional processes.
- Create digital infrastructure and services that support and enable Components to develop and deploy digitally enabled data, analytics, and AI solutions.
- Selectively scale proven digital and AI-enabled solutions for enterprise and Joint use cases.
- Surge digital services for rapid response to crises and emergent challenges.

I am proud of the solutions CDAO continues to build for DoD in support of this mission, and the impact the team has made since we last testified before this subcommittee. While CDAO is a Principal Staff Assistant (PSA) to the Secretary of Defense (SD), our organization, authorities, functions, and tools are unique. Unlike a more traditional PSA focused almost exclusively on policy and governance, the CDAO has been asked not only to lead and oversee, but to do and deliver. Getting data- and AI-driven solutions into the hands of warfighters and making sure there is the correct policy in place to do so has never been more essential than it is now. I am excited about the progress we have made on policy, governance, as well as the solutions we have already delivered.

Uniquely, as a PSA driving the delivery of capability to the warfighter, CDAO balances investments to deliver at speed and scale. We deliver solutions for decision-makers and mission users at *speed*, demonstrating the value of data-enabled capabilities, and ‘fielding to learn’ so that we can promulgate best practices. We also support DoD developers and program offices to *scale* the adoption of data, analytics, and AI, enabling Components to build sustainable capability in a responsible manner. Our delivery of solutions for these two customer segments balances the inherent tension between the concurrent priorities of preparing to ‘fight tonight’ and ‘get it done right.’ It is imperative that our national security posture require that we deliver tailored solutions to pressing challenges quickly, while establishing enterprise capability to improve interoperability and efficiency. Importantly, these capabilities, delivered at speed and scale, include not only data, analytics, and AI, but also the key enablers of acquisition, talent management, and experimentation and prototyping.

CHANGES

Over the past year, CDAO has worked to become increasingly agile to deliver value to DoD. We have applied lessons learned during our first year of operation to improve our organization for our customers, the warfighter. Things move fast in the world of data and emerging technology, and it is essential that we are positioned to move faster. The creation of a team focused on Combined Joint All Domain Command and Control (CJADC2) is a prime example of this rapid adaptation. CDAO’s CJADC2 team works across the Office of the Secretary of Defense, the Joint Staff, Combatant Commands (CCMDs), and the Services to improve data accessibility, data interoperability, and decision support tools for Commanders and decision makers. The team is leading delivery of solutions for global integration to include development of the joint Data Integration Layer (DIL), and decision support applications for key customers. We have also entered the second year of running technical experimentation, such as the Global Information Dominance Experiment (GIDE) series, to evolve concepts and technology together in an iterative, metrics-based environment.

Now, the solutions and platforms we deliver are only as good as they are secure. Our newly created Cyber Assurance Office (CAO) is geared towards creating “decision advantage with agile, operationally oriented cyber risk management”. Established to address foundational scaffolding that supports our strategic initiatives, the CAO has provided eleven Authorizations to Operate (ATO) for CDAO capabilities over a 4-month period (increasing cyber security posture of CDAO and reducing execution costs). These ATOs are in support of CJADC2/GIDE, ADVANA, DIL, and SUNet, all key programs CDAO is delivering to DoD and done so with the necessary protections thanks to the efforts of this new office.

CULTURE

CDAO continues to deliver on our promise to deliberately develop a workplace culture that both supports the people of CDAO and delivers strongly against our mission. We have implemented cultural leadership coaching sessions to expose our senior leaders to various methodologies, leadership strategies, models, tools, and tactics for improving culture. Our

quarterly in-person town halls are half-day events where all military and civilian CDAO staff come together and focus exclusively on collaborative team building, shaping CDAO culture, and delivering an experience that strengthens the sense of belonging our people have to one another and to the mission. We continue to expand communications between senior leaders and the CDAO workforce through dedicated time for listening sessions which serve as a forum for staff to directly share candid and honest feedback, concerns, and needs with executive leadership. Our monthly virtual all hands calls were crafted so the entire community has a frequent cadence for alignment, information sharing, clarity around roles and responsibilities of the CDAO subcomponents, socialization of our organizational structure, and informal interactions between employees and leadership. Our popular lunch and learn series feature different programs each week which allow staff to learn about other subcomponents of CDAO. We are also creating opportunities for professional and personal development, training, and growth for employees at all levels to increase their effectiveness and impact on DoD and beyond.

SUCSESSES AND ACCOMPLISHMENTS

Delivering to the Warfighter

As a part of our “do and deliver” obligation to DoD, we have been delivering solutions that use quality data to advance decision-making. We have made great progress since our organization was stood up in 2022 to get data-enabled solutions into the hands of warfighters. These activities take a wide range of forms, from joint experiments to interactive dashboards, CDAO is working to fill every niche we can. The GIDE events and the progress those have enabled on CJADC2 are two of the most exciting initiatives we have advanced this year.

In 2023, the CDAO hosted four GIDE events focused on defining and delivering a joint DIL that will enable INDOPACOM, CENTCOM, NORTHCOM, their components as well as international partners, to access, share, and integrate data to address key operational problems in the Joint Warfighting Concept. CDAO successfully executed these events with key global partners, focusing on global integration and joint maritime kill chains. This series of experimentation is designed to stress-test current systems and processes, introduce new technologies and approaches, and learn in an experimentation environment that replicates real-world operations and exposes areas which require improvement.

In an historic achievement, during GIDE 8 – the last iteration of 2023 – DoD declared the achievement of a Minimum Viable Capability (MVC) for Joint Staff and CCMDs to perform global integration in a CJADC2 context. This allows warfighters across the globe to provide increased decision advantage for DoD. Throughout the 2023 GIDE series, CDAO led mission partners in using live data and operational networks to iteratively experiment with prototype and commercial software applications, data integrations, and new operational concepts. This capability is available to the warfighter today. Looking ahead, using the GIDE 2024 series as a venue, CDAO will continue to work with a rapidly expanding industrial base to diversify the portfolio of solutions available to the Joint Staff and CCMDs for global integration.

Another successfully tested solution for the Warfighter is the Smart Sensor, which matures AI-enabled software onboard an autonomous MQ-9 Reaper to detect objects in the battlespace. Using AI-based technologies reduces required bandwidth necessary for passing full-motion video by identifying objects of interest and pushing that information into the sensor platform. It allows operators to maintain target awareness even in a degraded communications environment.

In FY23, the Smart Sensor team conducted research and development work, including development flight tests and a limited operational assessment, during an INDOPACOM deployment. The objectives of the deployment were to operate an AI and autonomy software package in an operational environment, rapidly retrain the Smart Sensor system from land-based mission orientation to deploy in a maritime environment, collect sensor data, and improve the ability to disseminate data from the airborne drone. While there are objectives which need to be further addressed, it proved to be an extremely useful deployment providing the project with many lessons learned as well as demonstrating the capability is on track for US Marine Corps Initial Operating Capability (IOC) requirements. Development efforts continue in FY24 in order to meet the US Marine Corps' planned IOC timeline of 1QFY26.

Delivering Infrastructure

AI/Autonomy Scaffolding

The Smart Sensor program highlighted above is an example of the scalability of the tools CDAO builds. We cannot scale our impact without enabling others to also scale their use of data, and deliver solutions themselves. We have established scaffolding that enables self-service and analytics, accelerating change at scale. Our approach to this enormous task covers everything from our investments in scaffolding to ensuring Large Language Models (LLMs) are used responsibly.

ALPHA-I is a portfolio of investments in tools, processes, and infrastructure that enable the holistic development of machine learning, AI, and autonomy, in DoD. CDAO is managing the procurement and availability of these investments in this portfolio across DoD. This set of investments is useful across CDAO activities, specifically for the Replicator Initiative announced by DSD at the end of last year. CDAO was directed to establish a data and AI Hub in support of the Replicator Initiative, and ALPHA-I is prepared to set-up the scaffolding and infrastructure of components of this AI Hub. Indeed, CDAO is partnering directly with the Defense Innovation Unit (DIU) to leverage commercial AI scaffolding tools, and has entered a Memorandum of Agreement in January 2024 with the express purpose of expanding this collaboration to make this infrastructure available to users across the Department.

ALPHA-I in support of DoD Autonomy programs enables AI/autonomy performers to iterate on their software in protected development and test environments, with government-owned datasets and classified design reference missions, over the course of potentially years of sustainment. The end state is mission-performant, multi-domain enterprise autonomy testing

and development that is only possible with shared tools, acquisition vehicles, datasets, and a culture of sharing lessons learned.

Delivering Business Wins

The use of capability enabled by quality data metrics extends past the battlefield into the fiscal and operational domain of DoD. CDAO is not only delivering solutions to aid business functions of DoD, but also providing a strategy and framework for DoD-wide use. Our approach to the “boardroom” side of data, analytics, and AI needs is holistic, and creates both solutions and guidance for accelerating adoption.

The CDAO developed and released the Responsible Artificial Intelligence (RAI) Toolkit, a resource that provides a voluntary process to identify, track, and improve alignment of AI projects to RAI best practices and DoD AI Ethical Principles, while capitalizing on opportunities for innovation. CDAO collaborated with DIU and, in particular, built on DIU’s 2021 Responsible AI Guidelines to develop the Toolkit. RAI work at DoD maintains the ultimate goal of end-user trust in AI technology, called justified confidence, due to measurable and explainable criteria showing that a model works within the parameters necessary to assist the user in accomplishing the mission. Use of the Toolkit will help assure end-users that AI capabilities work in alignment with DoD’s ethical obligations and that issues have been identified and addressed. By furthering warfighter trust in AI capabilities, the Toolkit helps unlock more capability for the warfighter and brings more support for commander intent to the battlefield.

Another big win for the CDAO and DoD this year was the development and deployment of Pulse. CDAO’s Pulse centralized data model and business analytic tools leverage technology on ADVANA to monitor and track performance metrics. The Pulse Analytics Dashboards refer to the application suite for reporting on performance management across DoD and integrating data across the National Defense Strategy Implementation (NDS-I), DoD Strategic Priority Metrics (SPM), Business Health (BHM), and any additional applications aligned to communicating progress towards executing Secretary of Defense priority areas. The Pulse suite of applications is DoD’s enduring initiative to institutionalize a culture of data-centric thinking, relying on data to drive improved performance and global competitive advantage. In 2023, Pulse provided decision advantage via an integrated executive dashboard for the SD and DSD to track progress on DoD priority areas using a centralized database of key metrics to enable data-driven performance management.

Underpinning multiple efforts to better integrate AI and innovative technologies to DoD is our ability to work with industry and other DoD innovation organizations. Beyond traditional cost-type development contracts, the CDAO Acquisition Ecosystem allows for multiple ways to buy products and services such as commercial solutions openings, other transaction agreements, basic ordering agreements, and blanket purchase agreements. In addition, we also offer expedited contracting processes; and AI driven tools to streamline federal procurements. These contracting pathways can also provide a flexible acquisitions onramp for technologies prototyped and validated within other DoD organizations that lack long-term scaling abilities.

For example, in 2023 we debuted our Tradewinds Solutions Marketplace, a new business model that expedites market research and competition through matchmaking non-traditional defense contractors and government buyers based on plain language requirements and videos documenting potential solutions. The Marketplace allowed for 13 awards based on 119 “awardable” solutions from 419 submissions.

Delivering Data for Strategic Priority Metrics

In July 2023, DSD directed the offices of primary responsibility (OPRs) to update the current value and targets of all Strategic Priority Metrics (SPMs) before the end of the fiscal year and ensure there was a plan to connect all current and future performance metrics to authoritative data sources. CDAO PSA analytic product teams targeted data engineering and analytics support to OPRs where needed. By end of September, 105 of 119 FY23 metrics used data to calculate a current value in the SPM Dashboard. An example of this transition is the integration of data logic for Washington Headquarters Service’s (WHS) outcome-based PSA metrics into the Pulse framework. CDAO worked directly with each WHS directorate to successfully identify data sources, confirm business logic, and build a dashboard prototype for 30 of 34 metrics, equating more than 300 unique current value calculations at the PSA-level.

Additionally, CDAO aims to enable users with self-service options for input and connection to its databases. As a testament to the self-service-driven model underlying Pulse applications, the Air Force recently integrated their set of 60 SPMs into the Pulse common data model for the first time, with minimal CDAO guidance or support.

TASK FORCE LIMA

The evolution of AI and emerging technologies remains highly dynamic with major advancements happening overnight. The mainstream explosion of LLMs is an example which required a good deal of agility from the CDAO. The DSD established Task Force Lima to harness the opportunities and mitigate the risks associated with applying generative AI to DoD mission sets. Since its establishment, Task Force Lima has engaged DoD components from across the Services, Combatant Commands, defense agencies, and field activities, as well as the Intelligence Community. Underpinning this effort is work CDAO is leading the development of a LLM maturity model that helps DoD ensure responsible application of LLMs considering specific use cases. During a LLM workshop at the CDAO’s Advantage DoD 2024 Data and AI Symposium last month, CDAO requested input from industry with a focus on reviewing maturity models.

DIGITAL TALENT

A necessary part of creating a lasting infrastructure for adopting AI across DoD, are the people that are going to build and maintain this technology. A memo for the record was delivered to Office of the Under Secretary for Personnel and Readiness to establish CDAO as the Digital Workforce Functional Community Manager. We are partnered with the Office of the Under Secretary for Research & Engineering, the functional community manager for software work roles, to build the Defense Digital Workforce. We have begun by coding existing DoD

talent and positions that execute roles in data, analytics, AI, and software. We are also investing in capabilities that will allow the digital workforce to be globally identifiable, accessible, and available for DoD use. CDAO has built a robust team to systematically analyze DoD's digital workforce and promote education and management as a unified cohort. In an additional effort to train and educate our own people, we are offering training to senior leaders across DoD through the Naval Postgraduate School, MIT, and online portals to improve understanding of data, analytics, and AI among current DoD personnel to facilitate and accelerate adoption.

Outside of DoD, CDAO is identifying and curating prospective digital talent and stimulating interest in working for DoD. CDAO has led direct engagement with 15,000+ students across all 50 states through DoD's Civilian Talent Pipeline Programs.

GOALS

The *2023 DoD Data, Analytics, and AI Adoption Strategy* differs from the first two data and AI strategies because it focuses on **how** DoD will accelerate adoption of data, analytics and AI in a manner that fits with all DoD Components. It unifies previous DoD-level strategic guidance, with more of a focus on alignment and synchronization to scale capabilities across the department. When effectively implemented, this strategy will allow leaders and warfighters to make rapid, well-informed decisions by leveraging high-quality data, advanced analytics, and AI. Built into this new strategy are a set of goals and guidelines that CDAO is helping the department action and work toward:

- **Driving a culture of experimentation and campaigns of learning:** Through our leadership on initiatives like the GIDE, the CDAO is rapidly integrating capabilities in support of CJADC2 and testing systems using cross-domain, operational data.
- **Integrating data, analytics, and AI leadership and investment:** Analytics and AI are applications of data. Through efforts such as the AI and Data Accelerator (ADA) initiative, the CDAO unifies the Department's approach to these technologies rather than treating them separately.
- **Breaking down barriers to systemic reform:** The CDAO understands that unlocking the full value of data, analytics, and AI is not just a technology-development problem. CDAO's work on building the Department's digital talent, for example, focuses just as much on shifting culture, process, and human behavior.
- **Developing enabling digital infrastructure:** CDAO's impact cannot scale without enabling others to do & deliver for themselves. With resources like the Joint AI Test Infrastructure Capability (JATIC) and platforms like Alpha-I, the CDAO is fielding infrastructure and structural scaffolding that enables self-service analytics and AI, accelerating change at scale.

This strategy provides DoD with guidance to adapt to new technologies as they come along, and proactively positions the adoption of whatever new data- and AI-enabled technology has disrupted the industry. The CDAO's integrated, agile approach to enabling self-service will

better allow us to leverage the strengths that are the sources of our advantage: our diverse society, our culture of ingenuity, our innovation base, and our network of Allies and partners.

INVESTMENTS

Going into FY25 and beyond, CDAO continues to make a great deal of investments in scaffolding, technologies, platforms, and people that are essential to our mission. During our first 25 months of operation, we have built multiple applications on Advana and identified ways to scale data and AI development that are essential tools for DoD. CDAO also continues to devote resources to efforts like CJADC2 and the Non-Geo INT projects from Project Maven as they grow in maturity and importance.

The Advana platform is the single enterprise authoritative data management and analytics platform that serves over 100,000 users across DoD. They are a key CDAO investment and expected to reach 150,000+ users in FY24. The platform is a foundational enterprise data management, data integration, analytics, and AI capability specifically designed to support large-scale, data driven decision making processes within DoD. Advana supports several CDAO efforts, such as CJADC2, GIDE, Pulse, and Alpha-I.

Alpha-I is CDAO's portion of investments in tools and platforms that enable the holistic development and scaffolding of AI and related technologies. One of the missions of CDAO is to appropriately scale the use of AI across DoD, which will require technologies to scaffold and help scale. These investments include:

- **Enterprise Data Labeling Service:** Piloting a common data labeling contract and tool deployment on multiple networks to support the data annotation needs of multiple AI projects initially focused on computer vision.
- **AI-Data Platform (AI-DP):** A demonstration of multiple (5) leading industry AI project development, orchestration, and data management capabilities on SUNet and SIPR to facilitate and coordinate development, management, collaboration, and sharing between multiple DoD AI stakeholders.
- **Enterprise Physics-based Platform Autonomy Simulation Tools (Sensor-level):** This is a commercial software platform that enables platform-level autonomous system development and test.
- **Enterprise Physics-based Mission Autonomy Simulation Tools:** This is a commercial software platform that enables "fleet level" autonomous mission behavior development and test.
- **Enterprise perception AI and autonomous system T&E Tools:** This is a set of select commercial and government-owned T&E tools for the test of both perception AI as well as the test of full autonomous systems performance, both a single vehicle and in collaborative missions.

CDAO's major efforts delivered to the warfighter are underpinned by campaigns of experimentation and learning. Our CJADC2 team is leading several key initiatives including:

- **Data Integration Layer:** Integration of data sources across DoD and intelligence community and prototype data mesh services that will inform additional requirements for enterprise capability to be developed starting in FY25.
- **GIDE:** Ongoing execution of quarterly experimentation events with the Joint Staff, Combatant Commands and FVEY partners.
- **Mission Command Applications:** Enterprise decision support tools initially for INDOPACOM, EUCOM, NORAD/NORTHCOM, CENTCOM and TRANSCOM, including but not limited to commercial licenses for Maven Smart System (MSS)
- **Joint Operating System (JOS):** A prototype commercial capability to validate enable low-latency data integrations for use cases like time-sensitive targeting.

CONCLUSION

The CDAO continues to drive massive value and an integrated approach to scaling data, analytics, and AI for the entire DoD. We are providing the necessary guidance to implement a holistic, agile AI strategy, as well as delivering platforms and solutions in the hands of warfighters. I look forward to working closely with the Subcommittee on these issues and others, as we push the boundaries of technology within DoD and enact long-lasting changes that keep us ahead of our adversaries.



Dr. Craig Martell

Department of Defense Chief Digital and Artificial Intelligence Officer

Dr. Craig Martell is the Department of Defense Chief Digital and Artificial Intelligence Officer, reporting to the Deputy Secretary of Defense in the Office of the Secretary of Defense. His appointment as the CDAO brings extensive industry experience and artificial intelligence (AI) and machine learning (ML) expertise to the Department.

As Chair of the CDAO Council, Dr. Martell leads Principal Staff Assistant policy officials and stakeholders in advising Departmental leadership; driving systemic DoD-wide strategy and policy; and advocating for programmatic, institutional culture, and budgetary changes relative to DoD data, analytics, and AI. Dr. Martell is championing the Departments' efforts to increase data sharing in the areas of health records and law-enforcement records, ensuring appropriate consistency with privacy and confidentiality regulations. As CDAO, Dr. Martell has extensive interactions with Departmental, and general awareness of Federal, entities engaged in statistical activities related to data, analytics and AI.

Prior to joining the DoD, Dr. Martell was Head of Machine Learning for Lyft where he built a state-of-the-art Machine Learning (ML) Platform, allowing Lyft engineering to quickly build and ship ML models using large-scale, new and ongoing statistical programs. From 2018 – 2020, Dr. Martell was Head of Machine Intelligence at Dropbox, responsible for all machine learning, including overall vision-setting, drawing from analytics as applied to ML, and clear, concise communication across the organization.

Dr. Martell's proficiency in statistical principles and methodologies has been demonstrated in his several patents including a Hybrid Classification System in 2021 and System and Method for Encrypting Data in Pictorial Data in 2008. He has published several papers anchored in mathematics and statistics including MAJIC: A Java Application for Controlling Multiple Heterogenous Robotic Agents and is also the co-author of the book Great Principles of Computing, published by MIT Press in 2015.

Dr. Martell has been a Senior Advisor, Relevance Science & Engineering at the National Laboratory for Education Transformation since 2016. And from 2003 – 2014, he served as Associate Chairman of Computer Science at the Naval Postgraduate School.

Dr. Martell earned a Ph.D. in Computer and Information Sciences from the University of Pennsylvania in 2005.

**WITNESS RESPONSES TO QUESTIONS ASKED DURING
THE HEARING**

MARCH 22, 2024

RESPONSES TO QUESTIONS SUBMITTED BY MR. MOULTON

Dr. MARTELL. I defer to the CDO of the F-35 program, USAF. [See page 14.]

RESPONSES TO QUESTIONS SUBMITTED BY MR. LUTTRELL

Dr. MARTELL. The authority to build the Data Integration Layer derives from the Deputy Secretary of Defense memo titled “Initial Operating Capability of the Chief Digital and Artificial Intelligence Officer”, dated February 1, 2022. The memo directs the CDAO to “create enabling digital infrastructure and services that support Components’ development and deployment of data, analytics, AI, and digital-enabled solutions”, among other functions. [See page 16.]

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

MARCH 22, 2024

QUESTIONS SUBMITTED BY MR. MOULTON

Mr. MOULTON. A significant portion of data on F-35s collected/generated during missions is discarded because there is no place to store it. When and how will DOD stop this data exhaust from F-35s?

Dr. MARTELL. I defer to the CDO of the F-35 program, USAF.

QUESTIONS SUBMITTED BY MR. STRONG

Mr. STRONG. Understandably, the cost of designing, training, and deploying AI is top-of-mind for any organization. Has the Department considered how it can leverage its existing technological capabilities—including on-premise, private cloud, public cloud, and hybrid cloud computing capabilities to design, train, and deploy AI in a manner that ensures compatibility with existing investments?

Mr. SHERMAN. Thank you, Mr. Strong, my team, and I appreciate the offer to speak with your staff to connect to Huntsville-area technology developers. To answer on the efforts, the Department has long recognized the current and future AI demand for computing power and capacity. There are plans to develop Capability Planning Guidance—in concert with CDAO input—about the necessary funding for AI designing, training, and deploying. The adoption of cloud and our various architectural models for cloud have and continue to remain fundamental in modernizing our IT infrastructure for an AI future.

We are relying on our commercial cloud service providers to deliver the needed capability, innovation, and scale to enable an AI-powered warfighter. Improving our visibility of cloud use and cost through our JWCC contract and contract rationalization efforts will help us understand critical trends and areas of mission impact for more informed investment decisions across the technology stack (both commercial and government). Given our fiscal constraints, we must be measured in our investment decisions in conjunction with CDAO, understanding that AI initiatives today are still primarily narrow but one day, will shift to that next level of intensity. We are preparing to be ready with flexible processes that allow us to securely, economically, and timely meet that need.

Mr. STRONG. Mr. Sherman, one of your deputies, David McKeown (Deputy Chief Information Officer for Cybersecurity) spoke at AFCEA's TechNet Emergence conference held earlier this month and said that no one in industry has come to him with a cyber protection program using AI . . . McKeown told the contractor-heavy audience at AFCEA, "if you happen to know of any products out there that are leveraging AI to do cybersecurity things, I'd love to talk to you. This is a key part of our zero-trust strategy."

The Armed Services Committee has done considerable work in recent NDAA's to push for cyber technologies using AI, and I know of several technology companies in my hometown of Huntsville that

are in fact developing cyber defense technologies using AI. For instance, to address the Space and Missile Defense Command (SMDC)'s Space & Ground Systems operational cyber threat detection and prevention requirements and support the zero-trust strategy, technology is being developed to auto-configure, self-optimize, and self-train defensive models to detect and mitigate cyber threats against critical ground systems and space assets. This technology leverages advanced Artificial Intelligence (AI), Machine Learning (ML), and Reinforcement Learning (RL) technologies to provide a holistic approach to space and ground systems cyber protection by covering the entire threat domain.

Any comments on the future of technologies like this from you would be appreciated. Further, my staff would like to discuss this with your office further to help connect the technology developers with the DOD end user.

Mr. SHERMAN. Our Team members routinely meet with technology companies to identify areas in which they may bring new or amplify existing capabilities to the Department. We welcome the opportunity to learn more about how these companies are leveraging AI, ML and RL in their approaches. Note that the team is leveraging AI capabilities to support department's Cyber Supply Chain and Software Supply Chain Assurance activities. As you can imagine, the big data analytics required to conduct supply chain risk analysis of our weapons and information systems is significant. The Department has engaged leading supply chain illumination companies, such as Exiger, Ion Channel, and Interos, to promote and deliver supporting AI technologies to the Department, down to program level, as well as to our industry partners. In a recent example, one of these illumination companies, Exiger, is leveraging Karambit.ai to help evaluate the source code of—and at the request of—a market-leading U.S. company that provides critical software to the Department. This company has developed code in a country of concern for more than a decade; therefore, it has high risk profile.

Examples of employing automated supply chain illumination tools and AI provide transparency into the information and communications technology supply chain. These tools can also help industry regain assurance of their technology, ensuring provenance and integrity of their code, in accordance with Executive Order 14028, Executive Order on Improving the Nation's Cybersecurity. Another area of interest is the utilization of AI and ML capabilities is the area of continuous monitoring and orchestration. AI/ML capabilities are well suited for the DoD's continuous monitoring and orchestration needs due to their abilities to comb through petabytes of data at tremendous speed to inform risk-based decision-making with accurate, real-time, threat-based intelligence. We welcome industry's partnership in leveraging AI for cybersecurity. We're hoping industry will step forward to demonstrate capabilities that the Department can learn from and adopt.

Mr. STRONG. Understandably, the cost of designing, training, and deploying AI is top-of-mind for any organization. Has the Department considered how it can leverage its existing technological capabilities—including on-premise, private cloud, public cloud, and hy-

brid cloud computing capabilities to design, train, and deploy AI in a manner that ensures compatibility with existing investments?

Dr. MARTELL. I defer to Mr. Sherman and Lt Gen Skinner to best respond to this question.

Mr. STRONG. Understandably, the cost of designing, training, and deploying AI is top-of-mind for any organization. Has the Department considered how it can leverage its existing technological capabilities –including on-premise, private cloud, public cloud, and hybrid cloud computing capabilities to design, train, and deploy AI in a manner that ensures compatibility with existing investments?

General SKINNER. Yes, this is something that DoD is always considering. It is a complex challenge involving technology adoption and a need for compute capabilities available across a spectrum of use cases, as there is not one-size-fits-all.

Current DoD policy and guidance encourage the use of agile software development via numerous mechanisms, including DoD Instruction (DoDI) 5000.87, “Operation of the Software Acquisition Pathway;” the 2022 DoD Software Modernization Strategy; the 2021 DoD Enterprise DevSecOps Strategy Guide; as well as other issuances from both the Office of the Secretary of Defense and the individual Services.

DoD should consider that any program with software capabilities be developed via a Modular Open Systems Approach (MOSA), which a few programs have already adopted. This approach allows defining a broad set of end goals that allow flexibility for industry partners to develop the most creative and advanced capabilities to meet those goals rather than develop capabilities that must meet predetermined DoD-mandated technical specifications that may be outdated by the time the capability is fielded. At a minimum, requirements documents should ensure that data from systems being developed will be collected, stored, and shared in a manner consistent with Department data strategies, policies, and guidance. This would enable greater interoperability and more iterative and agile development practices.

With respect to compute in general, the DoD is considering how it can best optimize the compute currently available to the maximum extent practicable across the mix of use cases that allow for the mix of on-premise, private cloud, public cloud, and hybrid cloud computing capabilities. The generative AI use case in particular is driving the need for increased compute availability. The compute available today is insufficient to satiate demand, nor agile enough with scale to respond to what’s easily knowable and foreseeable on the horizon. The rubric being addressed is to define what the compute needs look like in 5 years, and how the investments should be structured to achieve the ability to meet demand in the changing and evolving landscape.

In summary, your question is the right one, and we are working thru thinking about this exact problem as this is a foundational aspect of AI adoption that must be frequently revisited to ensure a good match between capability and infrastructure.

QUESTIONS SUBMITTED BY DR. MCCORMICK

Dr. MCCORMICK. Mr. Sherman, the Department of Defense (DOD) uses websites to communicate information and effectively engage the public. It operates more than a thousand public websites for the Military Departments, Joint Staff, Combatant Commands, Department of Defense Agencies and DOD Field Activities. In June 2020, the DOD tasked the Defense Media Activity (DMA) with consolidating all DOD public-facing websites, but little progress has been made toward that goal. Congress has supported DMA through several budget cycles, most recently including a \$5 million increase for DMA in the FY23 Appropriations Act. However, in the recently released FY25 budget request, the DOD has, again, not requested funding for this program, despite it being highlighted in the DMA's strategic priorities list and Congress' continued support.

Is Defense Media Activity's (DMA) public web program still a strategic priority for the Department of Defense (DOD)? If yes, why has DOD not requested funds for the program in its budget requests and should we expect future year's requests to include the proper resourcing for this critical initiative?

Mr. SHERMAN. Yes, consistent with the Annual Report on the Progress to Implement the 21st Century Integrated Digital Experience Act (IDEA), consolidating all DoD public facing websites is still a priority. This report underlines the DoD's process in achieving these goals. However, specific questions on funding requests would be better directed to the director of DMA consistent with DoD Directive 5105.74. <https://dodcio.defense.gov/Portals/0/Documents/21stCenturyIDEAREport-2023.pdf>

Dr. MCCORMICK. Mr. Sherman, what is Defense Media Activity's (DMA) status of consolidating all Department of Defense public-facing websites, meeting security requirements, and complying with the 21st Century IDEA Act?

Mr. SHERMAN. Per DoD CIO's Annual Report on the Progress to Implement the 21st Century Integrated Digital Experience Act, DMA is consolidating DoD public facing websites using the Web Enterprise Business hosting solution. This system meets all DoD standards for information security and continues to make progress in implementing the 21st Century IDEA. For more information, please refer to the more comprehensive Annual Report on the Progress to Implement the 21st Century Integrated Digital Experience Act. <https://dodcio.defense.gov/Portals/0/Documents/21stCenturyIDEAREport-2023.pdf>