[H.A.S.C. No. 118–11]

HEARING

ON

NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2024

AND

OVERSIGHT OF PREVIOUSLY AUTHORIZED PROGRAMS

BEFORE THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES
ONE HUNDRED EIGHTEENTH CONGRESS
FIRST SESSION

SUBCOMMITTEE ON CYBER, INFORMATION TECHNOLOGIES, AND INNOVATION

ON

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

HEARING HELD
MARCH 9, 2023

U.S. GOVERNMENT PUBLISHING OFFICE
52–381 WASHINGTON : 2024

SUBCOMMITTEE ON CYBER, INFORMATION TECHNOLOGIES, AND INNOVATION

MIKE GALLAGHER, Wisconsin, *Chairman*

MATT GAETZ, Florida
LISA C. McCLAIN, Michigan
PAT FALLON, Texas
DALE W. STRONG, Alabama
MORGAN LUTTRELL, Texas
JENNIFER A. KIGGANS, Virginia
NICK LaLOTA, New York
RICHARD McCORMICK, Georgia

RO KHANNA, California
SETH MOULTON, Massachusetts
WILLIAM R. KEATING, Massachusetts
ANDY KIM, New Jersey
ELISSA SLOTKIN, Michigan
JARED F. GOLDEN, Maine
PATRICK RYAN, New York
CHRISTOPHER R. DELUZIO, Pennsylvania

Josh Stiefel, *Professional Staff Member*
Wendell White, *Professional Staff Member*
Payson Ruhl, *Research Assistant*

CONTENTS

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

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON CYBER, INFORMATION
TECHNOLOGIES, AND INNOVATION,
Washington, DC, Thursday, March 9, 2023.

The subcommittee met, pursuant to call, at 9:30 a.m., in room 2212, 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

The CHAIRMAN. Good morning, and welcome to our CITI [Cyber, Information Technologies, and Innovation] hearing on "Defense in a Digital Era: Artificial Intelligence, Information Technology, and Securing the Department of Defense."

Just a reminder of our three holy commandments on the CITI Subcommittee. One is that we shall start on time. Check.

Two, 5 minutes—we will enforce the 5 minutes. I understand that you may not have the shot clock there. So we'll give you a little bit of grace and we'll try and—you got phones so you can time yourself.

And please try not to use obscure acronyms and jargon. We want to communicate in simple and direct language that normal human beings in America can understand.

We are pleased to be joined today by the Department's [Department of Defense] Chief Information Officer [CIO], Mr. John Sherman, and the inaugural Chief Digital and Artificial Intelligence Officer, Dr. Craig Martell.

I welcome both of you and especially, Dr. Martell, in your first appearance with the House Armed Services Committee. You both have very important jobs and our job is to ensure that you do your jobs well.

To underscore the stakes of your job and our job, I would like to quote a recent report from our friends at the Australian Strategic Policy Institute—ASPI—quote, "Research reveals that China has built the foundations to position itself as the world's leading science and technology superpower by establishing a sometimes stunning lead in high-impact research across the majority of critical and emerging technology domains including artificial intelligence and key quantum technology areas.

In the long term, China's leading research position means that it has set itself up to excel not just in current technological development in almost all sectors but in future technologies that don't yet exist.

Unchecked, this could shift not just technological development and control but global power and influence to an authoritarian state where the development, testing, and application of emerging critical and military technologies isn't open and transparent and where it can't be scrutinized by independent civil society and media.

In the more immediate term that lead could allow China to gain a stranglehold on the global supply of certain critical technologies. Such risks are exacerbated because of the willingness of the CCP [Chinese Communist Party] to use coercive techniques outside of the global rules-based order to punish governments and businesses, including withholding the supply of critical technologies," unquote.

Gentlemen, I am concerned that we are losing in key areas of the strategic competition with the CCP. I would prefer that we win. As we say in Green Bay, winning isn't everything. It's the only thing.

So today, I look forward to hearing from you how we can fight smarter and win this competition.

And with that, I recognize the Ranking Member, Mr. Khanna.

[The prepared statement of Chairman Gallagher can be found in the Appendix on page 35.]

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

Mr. KHANNA. Thank you, Chairman Gallagher, and I appreciate your leadership on this committee and your bipartisan spirit in which you have conducted the hearings.

I would also like to welcome Mr. John Sherman, the DOD [Department of Defense] Chief Information Officer, and Dr. Craig Martell, the Chief Digital and Artificial Intelligence Officer. Thank you for your service and thank you for appearing before the subcommittee.

On the heels of the 1 year anniversary of the war in Ukraine one constant theme that we have seen is ways that the war has been transformed and different from the past.

From the ubiquitous presence of tactical unarmed—unmanned aerial vehicles to the use of digital platforms it's obvious that the continued integration of advanced technologies in combat is an essential component of modern warfare and that is why the DOD's CIO and Chief Digital Intelligence and Artificial Intelligence Officers' appearance is so important.

One of the things we need to focus on in the second year of the creation of the Chief Digital and Artificial AI [Artificial Intelligence]—Artificial Intelligence officer is the challenges that you have encountered and ways that we can offer assistance. Deconflicting some of the duties is important. One of the other pretty important issues is the recruitment of talent and the retention of talent, and how we do a good job in recruiting the top talent.

I know we have an advantage of doing that in the private sector in Silicon Valley. But we need our best and brightest in technology coming into government and I want to get your thoughts on additional steps that we can do for recruitment.

Furthermore, the growing importance of the electromagnetic spectrum and the highly visible role of the Department's spectrum usage is something that I hope this committee can discuss.

Finally, I want—would like to hear your work about securing our networks and that of the Defense Industrial Base. That is absolutely critical in any modern warfare.

Thank you again for both of your appearance before this committee.

The CHAIRMAN. Thank you.

Mr. Sherman is 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 here today.

Now, last summer I also held the position of Acting Chief Digital and Artificial Intelligence Officer. But as you note, sir, sitting next to me is Dr. Craig Martell, who is now the permanent CDAO [Chief Digital and Artificial Intelligence Officer]. We are privileged to have him on the DOD team and we work together on many key priorities that we are going to discuss today.

All of our modernization initiatives are focused on ensuring the joint force is prepared to win against peer and near-peer competitors. This means identifying and leveraging effective technologies and approaches to stay ahead of our pacing challenge of the People's Republic of China as well as any other nation or group that might seek to do us or our allies harm.

Succeeding in this space is why my team and I come to work every single day and it is our overriding mission imperative. We also continue to take in lessons on how the digital landscape is constantly evolving from the battlefields of Ukraine and elsewhere, and we endeavor constantly to strengthen our interoperability with allies and partners around the globe.

Driven by these priorities, we have made key strides in digital modernization since I last testified before this subcommittee last year.

In December, we announced the award of our new Joint Warfighting Cloud Capability, or JWCC, which will provide us with enterprise cloud computing from four world-class companies at all three security classification levels from the continental United States out to what we call the tactical edge, meaning an island in the Western Pacific, key terrain in Eastern Europe, or even a ship at sea.

JWCC, which supersedes the single vendor single award JEDI [Joint Enterprise Defense Infrastructure] cloud procurement that we cancelled in 2021, will enable the Department to develop and deploy software in an agile, secure, and scalable manner while providing for data and compute and storage that will undergird efforts led by my CDAO colleague and others.

Additionally, we continue to strengthen the Department's cybersecurity posture underscored by our Zero Trust strategy and implementation plan. The concept of Zero Trust involves protecting critical data and assumes that an enemy is already on our network, and that we must verify the credentials of everyone and everything and that there be no unrestricted lateral movement across our enterprise.

We plan to implement Zero Trust all across the Department by 2027 and are working with the DOD components on their plans, ongoing actions, and investments to achieve this goal.

Meanwhile, we are pursuing multiple lines of efforts to strengthen the cybersecurity of the Defense Industrial Base companies through outreach, provision of services, alignment of DOD activities, and preparation of the Cybersecurity Maturity Model Certification program, which will provide us with a mechanism to verify that companies are handling sensitive DOD data and are instituting required cybersecurity measures.

We are also working with stakeholders and DOD to remediate the, quote, "technical debt," unquote, that has accrued on many of our key weapon systems. While we didn't necessarily have to worry about terrorists and insurgents hacking into our jets, ships, or tanks over the last 20 years, we know that nation states will certainly try to do so.

Ensuring our service members operate in cyber-survivable equipment is a top priority for the Department. In the same vein, we continue to strengthen our command, control, and communications capabilities.

These include electromagnetic spectrum operations for which we and CIO have taken over Department level oversight since this last year.

Representing the nexus of electronic warfare and spectrum operations, our forces' ability to dominate in this domain is critical to fighting and winning on any modern battlefield.

All the while, we never forget our success comes down to people. We are releasing a new cyber workforce strategy and a related policy manual that will help us better identify, recruit, develop, and retain top-notch talent.

Also, for the military and civilian members in DOD who have had to struggle for far too long with IT [information technology] systems that are simply difficult or slow to use, we are doubling down on our efforts to improve user experience all across our enterprise.

Using my office's budget certification authority, my team and I are driving strategies and will hold organizations accountable for continued progress.

All of these activities rely on the strong support that this subcommittee has provided to DOD for many years.

Thank you for this backing and for the chance to testify here today. I look forward to answering your questions.

[The prepared statement of Mr. Sherman can be found in the Appendix on page 36.]

The CHAIRMAN. Thank you.

Dr. Martell is recognized for 5 minutes.

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

Dr. MARTELL. Chairman Gallagher, Ranking Member Khanna, and distinguished members of the subcommittee, thank you for the opportunity to testify before you today.

This is my first appearance before Congress and I look forward to sharing the ongoing efforts of the Chief Digital and Artificial Intelligence Office.

It's an honor for me to serve our nation as the first DOD CDAO. The importance of this role, the mission of the CDAO, and our service to the warfighter are not lost on me.

From my experience as a professor of machine learning at the Naval Postgraduate School to my time leading machine learning teams at some of the most innovative technology companies in the U.S., I am proud to bring best practices and lessons learned to accelerate and scale data analytics and AI in support of the national security mission.

The Deputy Secretary of Defense established the CDAO in February of last year, bringing together the authorities and resources of previously separate organizations, which included the DOD Chief Data Officer, the Joint Artificial Intelligence Center, the Defense Digital Service, and Advana, the Advancing Analytics Office.

We recognize that data analytics and AI are core capabilities in supporting the Secretary of Defense's priorities to defend the nation, take care of our people, and succeed through teamwork.

When I arrived in June, my team and I assessed the data analytics and AI capabilities and gaps at all levels of the Department. We reviewed the recommendations from the National Security Commission on Artificial Intelligence.

We assessed existing digital technologies within the Department, partner organizations, and the commercial sector. From these efforts we have identified four key strategic elements.

One, improving data quality. I am going to say that over and over again today. Two, enabling advanced analytics and metrics; three, providing the appropriate AI scaffolding; and finally, cultivating the key enablers for all of us. We refer to this as our hierarchy of needs.

At the base of this hierarchy are the enablers—talent, culture, and leadership. These are the foundations of the work we do in CDAO.

This includes fostering an educated workforce, leveraging the strengths of the commercial and academic centers—sectors, and effectively integrating both our data and activities with our allies and partners.

In addition, as a close partner to Honorable Sherman in the office of the CIO, they're delivering the storage, security, and computing infrastructure that this hierarchy depends upon. We work very tightly on this.

Above these enablers the next level is quality data. As our number-one priority, quality data will enable decision advantage by powering both the analytics and the AI layers of this hierarchy.

For example, data paired with powerful analytics dashboards will allow us to see what we own and where it is. Sounds simple. Remarkably important.

Similarly, complex AI models will bring enhanced capabilities both to warfighting and to running the business. These are not doable without quality data.

Addressing these challenges via this hierarchy of needs will drive the Department to being data-centric, to being the data-centric organization it needs to be.

Now, note this hierarchy is a logical hierarchy. It doesn't mean we are not going to move forward on AI and getting things to the warfighter until data is perfect. We are going to be doing all of these things simultaneously.

So, based on this strategy we are pursuing the following initiatives in 2023. One, creating the JADC2 [Joint All-Domain Command and Control] data integration layer, which will enable combatant commands as well as partner nations to access, share, and integrate data at all levels; two, providing the enterprise with the appropriate AI scaffolding, which includes the services and infrastructure most needed to accelerate AI development and adoption across the DOD; three, conducting a talent management pilot for establishing a defense digital corps, a cadre of digital experts aligned to digital positions across the DOD and managed as a unified cohort; and finally, supporting our business performance metrics to ensure progress on the goals laid out in the DOD Strategic Management Plan and the National Defense Strategy implementation plan.

I look forward to working closely with this subcommittee on these issues and others as we enable DOD's current and future use of data analytics and AI for national security.

Thank you.

[The prepared statement of Mr. Martell can be found in the Appendix on page 50.]

The CHAIRMAN. Thank you.

We'll now proceed to question and answer. I will recognize myself for 5 minutes.

Dr. Martell, you sort of talked about the, I think, or hinted at the tension in your job, which is—was all these things we need to do over the long term. We need to improve—turn DOD into a data-centric organization.

But in the short term, our warfighters, our joint warfighters, our combatant commands have needs. They have rising threats they have to confront.

At present, Joint All-Domain Command and Control, or JADC2—textbook example of jargon—is increasingly siloed into individual service plans, which extends the timelines even more.

As I understand it, the Deputy Secretary created your position primarily to help meet this urgent need, that is, to rapidly deliver operational data-centric and truly joint warfighting capabilities to the COCOMs [combatant commands], especially Indo-Pacific Command.

If this is your mission, and that's a mission I would support strongly, can you just tell us clearly what CDAO is doing to deliver on it? You mentioned four things. Maybe—is that what you would say and that is—what do you mean by scaffolding?

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

[Technical interference.]

The CHAIRMAN. You're not in trouble.

Dr. MARTELL. Okay. Did I do something wrong?

I think fundamental to the problem of the JADC2 issue is that we think about it as a product or a destination or a particular capability. I don't think that's right at all. That's not how we look at it.

JADC2 is simply a new way to do business. It's being able to get the right data at the right time to the right place so we can jointly exercise command and control across all domains from sensor to shooter.

So you mentioned that the services are stovepiped. But I don't necessarily see that as a stovepipe. They build systems that work for their particular needs and that's fine. We shouldn't want to stop that. We shouldn't want to dive deep into what they know how to do.

But what we need to do is get the data from those systems to a command level so that—and have it flow easily to a command level so command decisions—strategic command decisions can be made and tasked down to shooters.

So we see our job as developing this data integration layer. We can dive deeper into the geeky aspects of it. But this data integration layer, which allows all of those systems to talk to it as a—so that it can be shared where it needs to be when it needs to be.

The CHAIRMAN. So your office now has substantial staff and resources. What will be the fairest way for us to measure your success?

What are the right metrics so that the next time you come and testify before us we can sort of fairly assess you on how you're doing your job? Is it adoption of capabilities? Speed of delivery?

Is it the number of experiments? Is it the number of meetings? Dollars spent? What would be the right metrics to judge your success?

Dr. MARTELL. I hope it's not the number of meetings or dollars spent, right. I think it's very important to not have effort-based metrics. We need outcome-based metrics.

And so we think about—and to be clear, it's still unclear to me—that's a weird sentence—to be clear it's unclear—but it's still unclear to me how we are going to measure these things all the way down to the levels that we need to.

But what we are driving for is time to usability—if someone needs a new capability and we've provided the underlying scaffolding how quickly can that capability be fielded.

Amount of data-driven decision making, and we think about this sort of a number of ways, but for amount of data-driven decision making per COCOM—per combatant command. Amount of data-driven decision making per three-star forum.

So we can actually measure these fora and we can measure the number of dashboards being used, which is providing data to those four.

And, finally, time to usability. How quickly—so time to delivery is, from a producer's perspective, we are going to get it to you. How quickly can that then be used.

So once it's delivered if it just sits on the shelf that's also not sufficient. It has to actually be used. So what sort of best practices and training do we have to wrap around that so that the warfighter can use it.

The CHAIRMAN. I appreciate that.

Mr. Sherman, I may have to get to you in a second round of questions. Quickly, though, Dr. Martell, can you just explain again and just—for a liberal arts major—what do you mean by the scaffolding that you're talking about?

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

Most people think about AI as a product that's delivered. I think those products being delivered will be delivered best by our commercial sector. But there are things that the DOD needs to do around that product that's being delivered that we are not doing.

For example, what the product should be doing—what a particular model should be doing, say, trying to detect something on the battlefield we are the subject matter experts of that.

We should be saying this is A, this is B, this is A, this is B, and getting that data labelled correctly should be our responsibility. Currently, we give that to industry as a responsibility but I believe we should own that because that's our IP [intellectual property].

Simultaneously, on the other side——

The CHAIRMAN. My time has expired. I have to hold myself to my own rules so we'll have to come back. Otherwise, I will be a total hypocrite.

I just want to emphatically endorse what you said about meetings. To paraphrase Drucker [Peter Drucker], meetings are a concession to a deficient organization. One either meets or one works. One cannot do both. So we should not use that as a metric.

Mr. Khanna is recognized for 5 minutes.

Mr. KHANNA. Thank you. I am reminded of the Oscar Wilde quote that the problem with socialism is too many damn meetings.

I appreciate the——

Dr. MARTELL. I am not sure if I am supposed to respond to that.

[Laughter.]

Mr. KHANNA. I appreciate your testimony. You know, we had Dr. Eric Schmidt at my oversight hearing and one of the points he made in the talent of cyber and tech is that he thought the DOD was doing a good job in recruiting, a good job at the service academies. But the challenge was really the ability for people and technology to rise to meaningful positions.

Obviously, you know, you don't have the multimillion-dollar exits in Silicon Valley. But the other thing that attracts people to these tech companies is their ability not just to be grunt workers, not just to be mid-level folks, but to actually be in leadership and to be central in driving things.

And as jamming and AI in so many of the theaters of modern war may involve technology, what is the pathway to get people up the ladder so they feel empowered?

Both Dr. Martell and then Mr. Sherman.

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

I agree completely that we need to build pathways for tech folks in the Department. But I think one of the benefits we have is that all of our workforce has been getting increasingly technical as our technology is getting increasingly easier to use.

So one of the things we need to depend upon as a nation we have to continue those pushes so that we generate practitioners. Particularly in AI it has been dominated by experts and I would say for the last 15 years it has been dominated by experts.

But there's a movement now where there's enough commoditized tools where skilled practitioners can actually deliver the value that experts used to be able to do. That's the tactic we are taking.

How do we upskill the folks that are in the Department now and, secondarily, how do we attract maybe not those people who already know walking out of school from a select group of schools that they're going to get a Silicon Valley job.

What about those folks who are not sure they're going to get a Silicon Valley job or a high-paying job? That's still untapped talent in the United States.

How do we create a pathway, an extended apprenticeship, so that when they leave working for the DOD or working for the government they're actually significantly better and more attractive to those industrial jobs?

I don't think hire to retire is the right solution. I think transforming them is the right solution.

Mr. KHANNA. And I appreciate that, Dr. Martell.

But for Mr. Sherman I would just say, though, that you shouldn't aim just to have the top folks go to Silicon Valley and get the next layer.

I mean, a lot of the top folks in Silicon Valley—Vint Cerf, who is at Google, came out of DARPA [Defense Advanced Research Projects Agency] and it was really the Department of Defense that led so much of the innovation that came up with the mouse, that came up with drones, that came up with the Internet, that came up with GPS [Global Positioning System].

So, you know, the hope would be that the best and brightest would still want to come to Defense and the inverse as opposed to going to Silicon Valley.

Dr. MARTELL. Thank you for that comment, Representative Khanna.

I think that's right. I think it'd be more attractive if we have a robust workforce in place. So I actually see this as a means to that.

Mr. KHANNA. Mr. Sherman?

Mr. SHERMAN. And, Congressman, I would just add to this a couple of points.

Using every—excuse me, every arrow in our quiver that have been given to us by you all in Congress, things like Cyber Excepted Service and other hiring authorities where we can pay folks a little bit more, get them in the door more quickly, and also think differently about how we manage folks' career and not the traditional 30-year, come in the door, and have the traditional step up the ladder there.

Now, folks are never going to make the same amount of money in DOD. That's not what's going to bring them in here. It's going to be the mission—protecting us against the PRC [People's Republic of China], putting ISIS [Islamic State of Iraq and Syria] back on their heels, those kind of things. I saw this in the intelligence community as well.

But we have to think differently about the credentials that folks need to come in, things like apprenticeships, looking—you know, what are the degree requirements. Maybe a 4 year degree is not required. Apprenticeships can be a way to go on this.

And then, very importantly, recognizing that folks are going to come in and out of the door here and we have to partner with industry and I talk a lot publicly about this. How are we going to do this where someone comes to DOD, then goes to industry in Silicon Valley or Austin or North Carolina or wherever and comes back?

How can we do this without having the security folks' head explode where they have to go through another year and a half or 2 years getting in the door?

We are going to have to figure this out. And to that point, sir, we have a new Cyber Workforce Strategy. It's actually coming out this week.

One of the key pillars is exactly this point about creative approaches on how we get past the old think about how we manage tech careers on this, sir.

Mr. KHANNA. Well, I will look forward to working with you and the chairman on this.

The CHAIRMAN. Mr. Gaetz is recognized for 5 minutes.

Mr. GAETZ. Dr. Martell, it seems that for us to beat China at AI the first thing we have to do is catch up to China in AI, right?

Dr. MARTELL. Thank you for that question, Congressman Gaetz. I don't actually think we are behind China with respect to AI. I think—but I—let me sharpen that.

With respect to technological capabilities we are as far ahead as anyone. With respect to talent, we are as far ahead as anyone although I think there's a danger there.

I think the fundamental difference is they are working—they are doubling down on high-quality data and high-quality compute. So we have high-quality compute but we need to double down on getting the data right.

Mr. GAETZ. I think you need to start my clock, Mr. Chairman. Thanks. Thanks for that extra time.

The CHAIRMAN. Oh, darn it.

Mr. GAETZ. So I rescind everything I just said. We can start again. No. Yeah, this is all off the record.

The CHAIRMAN. It's still on the record.

Mr. GAETZ. Yeah.

The CHAIRMAN. But Mr. Gaetz gets——

Mr. GAETZ. Yeah. No, I got you. I got you, Mr. Chairman.

So most of the analysis I've seen indicates that they're way ahead. So your testimony is interesting because it seems—you do appreciate and understand that it runs cross current, a lot of what we hear about China's current supremacy in AI, right?

Dr. MARTELL. I do, Congressman Gaetz. Thank you.

I think we could have a more interesting conversation in the closed session. I am happy to do that.

Mr. GAETZ. Okay. So you talked about the data sets and I am really interested in the ways that China builds those data sets where they get information. Does China have the capability to collect intelligence from the offshore oil rigs that they operate and own?

Dr. MARTELL. Thank you for that question, Congressman Gaetz. I would rather talk about it in a closed session.

Mr. GAETZ. Well, I don't know. Sometimes I worry that we overclassify these things. Like, shouldn't the American people know if there's oil rigs offshore that are, like, using Chinese data to collect information?

Dr. MARTELL. So I think probably a more correct answer is my expertise doesn't extend to China to that degree. I think we are going to win any fight by providing quality data, create the right scaffolding to establish their talent.

Mr. GAETZ. Well, yeah. Let me ask another place—let me ask another place where they may collect data.

So does China collect data from the cranes that they sell to U.S. ports?

Dr. MARTELL. Thank you for that question. I am not an expert on China's——

Mr. GAETZ. Yeah, but I am kind of concerned that an assessment of their AI capabilities is going to lash pretty closely to where they're getting these exquisite data sets, right.

And so if they're able to utilize AI to aggregate this massive amount of data that they get from the cranes that they sell our ports, from the DJI [Da Jiang Innvoations] drones that our law enforcement fly around, from the oil rigs that our U.S. oil companies sell to them, that really is an important plug into AI, don't you think?

Dr. MARTELL. Congressman Gaetz, I actually do and I think it's a very important point and I am not trying to dismiss it.

When I said I don't think they're further ahead with respect to AI, I don't think they're further ahead with respect to the algorithm capabilities or the talent capabilities.

In fact, most algorithms are commoditized and anybody has access to them at this point. If, in fact, they are gathering data from more places that will, in fact, produce robust AI and if we need to—we can have a really robust conversation about what data we should be gathering.

I am very open to that. But I am in agreement with you that getting the data right and getting the right data is what drives robust AI.

Mr. GAETZ. I've spent all my time with you talking about how China gets their data because I don't view our AI scenario as in a bubble. I think we are in direct competition with China. We win or they win.

Dr. MARTELL. I agree.

Mr. GAETZ. And if we don't know who's ahead, I do worry about getting to those deliverables in a way that we can measure them and fund them and advance them.

So, hopefully, we'll be able to have more fruitful discussion about how they collect data, how we can integrate that into our broader cyber strategy and our AI strategy.

Dr. MARTELL. I look forward to that. Thank you.

The CHAIRMAN. Thank you, Mr. Gaetz.

Before I recognize Mr. Ryan, I want to recognize the Stump family from Green Bay, Wisconsin. They've travelled all the way from America's district, the Eighth District of Wisconsin, to listen to our witnesses and engage in this discussion about AI and technology. So it's very important. Thank you.

Mr. Ryan is recognized for 5 minutes.

Mr. RYAN. Thank you, Mr. Chair, and welcome to our guests from Wisconsin, and thank you to you, both gentlemen, for being here today, for your service, especially Dr. Martell.

Stepping into a new role and position in any organization is always a challenge and in the biggest bureaucracy in the world. I am sure ——

Dr. MARTELL. It's been a joy.

Mr. RYAN. ——it's been not boring. So thank you for stepping up and both of your public service.

I wanted to actually build on what Chairman Gallagher was getting towards with you, Dr. Martell. You were starting to talk about kind of the roles and—not authorities but the roles and responsibilities when it comes to within JADC2 specifically kind of who builds what.

You were talking about scaffolding and you were beginning to say what you thought the role of commercial partners is.

Could you expand on that and——

Dr. MARTELL. Absolutely.

Mr. RYAN. ——to be specific and sort of where my—what I would like to hear from you is how do we—not a new problem but how do we work better with and enable particularly smaller and less known but, I think, often most talented companies to plug in to the scaffolding that we are building?

Dr. MARTELL. Thank you for that question, Congressman Ryan.

One of the things that's surprising—was surprising to me when I got here is how acquisitions work. You set out a bunch of requirements and then 5 years later a product is delivered and the world has changed drastically in those 5 years.

That's the sort of thing we are trying to tackle. We are trying to be able to be efficient, flexible, iterative, and experimental.

So our goal is to get a data layer which allows for data to flow from any point to any other point and then apps can sit on top of that data layer.

So a particular combatant command or a particular commander might want an app from one vendor and another combatant commander might want an app from another vendor, and we need to see that data layer as the underpinning of the marketplace that allows any vendor to show up and say, I have a solution for this particular problem.

I think that's a much more iterative way and experimental way to get at—to get out this as opposed to saying, every commander, you get the same thing, when the commander out on the ground might need something very different than something in the maritime domain.

And we need to allow for that marketplace both for the big players who produce real value, and particularly in the AI space. Three guys in a garage might actually change the game and we need to allow that to be available to them as well.

Mr. RYAN. I agree. My concern is time and urgency. I mean, we've heard many different timelines for potential major conflict, particularly China, and building a data integration layer against a bureaucracy that's not used to doing that.

I mean, how do—how quickly do you think we can build that? What can we do as, you know, in our role as Members of Congress to enable that to accelerate that, or what authorities do you need? What resources do you need?

Dr. MARTELL. Thank you for that—for that offer, Congressman Ryan.

I will take it as a question for the record for probably the end of the year to get back with you with more specifics. Right now we are undergoing the GIDE experimentation series, which is Global Information Dominance, where we are actually testing these things.

[The information referred to can be found in the Appendix on page 61.]

We just did—we just finished one. We are doing another one next month, I believe, with a key partner being INDOPACOM [U.S. Indo-Pacific Command], and understanding how what we've learned, for example, at EUCOM—at European Command—might be applicable in a maritime domain like in INDOPACOM.

So we'll have—the point of that experimentation is to come up with a capabilities gap analysis so we can actually answer those sorts of questions for you.

Mr. RYAN. Great. Thank you. I am running short on time.

Mr. Sherman, on cyber talent management could you just continue to expand on that? Are there additional authorities? You talked about the Cyber Excepted Service. Are there additional authorities or tools that would be helpful to advance that mission?

Mr. SHERMAN. Congressman, I think we have the tools at our disposal like Cyber Excepted Service and targeted local management supplement, which is additional funding we can—or pay we can provide to folks in certain areas.

I think we just need to continue to use these authorities and continue, sir, to work with industry, you all in Congress and elsewhere, as we generate ideas about how to think creatively about a 21st century workforce, some of whom may come in for a long career but others very likely are going to come in and out and matter of fact, we are going to want them to do that for career areas like data scientists and others to not stay in government their whole time but go to industry and come back and figure out how we can do this in an agile way to stay ahead of the PRC and others.

Mr. RYAN. I appreciate that. I would encourage you think creatively if there are additional tools and authorities I think you're hearing from us we want to give them. So please come back, and I yield back my 1 second.

The CHAIRMAN. Great use of time.

Next up a son of Notre Dame, Mr. Fallon.

Mr. FALLON. Thank you, Mr. Chairman. You know, when we talk about securing our networks against our adversaries, our enemies, it's absolutely—you know, I think it's critical that we understand exactly what we are up against and where our vulnerabilities may exist.

It doesn't do us much good to invest billions of dollars in security if there are entire swaths of our network that remain open and vulnerable, of course, to hostile actors.

And as we talk to folks in the industry I've come to learn that this was, in fact, our reality in the DOD Information Network in the not so distant past.

Thankfully, we've had—you know, we've taken the steps necessary to remedy the situation and I believe it's essential that we continue to invest in technology and secures our networks by leveraging new advances in technology with our network through the eyes—we have to see our network through the eyes of the enemy and where they would perceive vulnerabilities.

So, Mr. Sherman, how are you leveraging AI-backed technologies to discover and remediate vulnerabilities before adversaries can exploit them?

Mr. SHERMAN. So in terms of AI-backed technologies the main place we are going to apply that is what we call the big data platform where we bring data together to assess what is going on on our networks.

But, sir, if I could say, AI is just part of this. It really is, to your point and your question about what we know the other side is doing, is the partnership I have with General Nakasone at U.S. Cyber Command and the National Security Agency to get threat-informed intelligence about what the other side—China, Russia, et cetera—are doing against our networks.

And also, again, AI undergirds some of this but it really is that Zero Trust approach I noted in my opening statement where we assume an enemy is already on our network. The burglar is already in the house, and how do you prevent them from moving laterally throughout the house and using what's called Identity, Credential, and Access Management where it has to be verified—someone's identity—along the way to make sure that they can't move to get to your most critical data.

Sir, it's a new way of thinking about cybersecurity, not just at the perimeter or not even a defense in depth but a whole new way of thinking about you don't trust anything or anyone and that's what we are really doing to lock down our networks, sir.

Mr. FALLON. Kind of assuming that maybe the submarine is below the destroyer already, right, and you can't see him but he might be there.

Mr. SHERMAN. Right.

Mr. FALLON. Dr. Martell, how do you see AI developing as a component of the DOD's cyber mission? And also, how can we remove barriers to entry for companies developing and deploying AI?

Dr. MARTELL. Thank you for those questions, Congressman Fallon.

I echo what Mr.—Honorable Sherman said that it's mostly about data and it's mostly about Zero Trust, and let me—let me say that

Zero Trust underlies it—it's a—it's a binary relationship that goes both ways, right.

So we can't build what we build without the Zero Trust underpinnings that Mr. Sherman provides. But I also think AI can provide some help to security, particularly in anomaly detection.

So once we know the flows and we can track the flows of people through the zero trust architecture, we can build systems that will help us detect whether it's an anomalous flow, something we might want to look at. We might want to just sort of dive a little deeper there.

Mr. FALLON. And, Mr. Sherman, as far as recruiting talent, you know, we have people come into our office, and it doesn't matter what industry they're in. They have a labor shortage. They have a labor need, and now we are not even meeting our recruiting goals.

I was listening on the Armed Services—I am sorry, we learned that last year in Armed Services that the Navy, the Air Force, the Army, weren't hitting their recruiting goals. So where are you all with labor? And you just mentioned about attracting that so how do you attract the talent and—because it is competitive and they can make so much more on the outside?

Mr. SHERMAN. Sir, that is exactly what we've been getting after as well with this new Cyber Workforce Strategy. We have something called a Defense Cyber Workforce Framework.

It sounds bureaucratic, but it's where we've taken all of the 70-plus work roles in cyber and digital and with a fine toothed comb much more granularity than you would see from the Office of Personnel and Management on exactly the sort of work roles where we are going low or we are right where we need to be and we might need to apply some new incentives, kind of with the rear stat of adjusting where we are getting low on maybe cyber defenders or software coders or whatever, and this has been a key tool we've implemented.

We've added AI in data work roles and this has been enlightening for me as a CIO about the levels of specificity we have to have to make sure when you start to see a kind of a warning light, hey, we are getting low on this type of work role, we need to apply some Cyber Excepted Service or other types of market supplement we can put against this.

It's been a lot of pick and shovel work, sir. But now we have a foundation to really look across the dashboard to see where we are particularly with our civilian but also working with our military workforce.

So I would say we are making a good start on this. We've got the tools we need and applying the authorities you all have given us to address shortfalls.

Mr. FALLON. Thank you both.

The CHAIRMAN. Thank you.

Mr. Golden, a great Marine, is recognized.

Mr. GOLDEN. Semper Fi, man.

[Laughter.]

Mr. GOLDEN. Sounds like a bad thing.

Dr. Martell, in your prepared remarks you talked about the Cyber Workforce Framework and you referred to a pilot for a defense digital corps program.

I want to—obviously, the goal is to foster digital talent and everyone's—we've had several rounds of questioning there. So the National Security Commission on AI previously advised that perhaps there should be a Digital Reserve Corps, which I think would be a nice complement to what you're talking about with having a digital corps.

So is that something that you have thought about? Here in the House, the For Country Caucus has been pushing for that. We are a caucus of all vets. Tony Gonzales has been the lead on that. We've gotten it through the House and previous NDAAs [National Defense Authorization Acts]. It's always kind of suffered in the Senate.

But could either one of you or both of you comment on whether or not that might be a way to have your cake and eat it, too? I mean, we just had a conversation about talent is going to the tech industry and the private sector.

Why not try and get some of those folks to serve while they're also out there in the private sector?

Dr. MARTELL. Thanks for the question, Congressman Golden.

Hallelujah. I think that would be amazing, particularly because the Defense Digital Corps' goal is to see—to figure out what talent is needed across the Department and to be able to bring that talent in and seed it but also manage it as a cohort because they're going to be onesies, twosies, and alone, and no one wants that job, right.

And then—and but if they're a cohort and they can share—and they can share problems, they can share issues, we can much better manage and grow them, right, and give them real careers.

If we can do that seeding by folks coming in for—depending on how this works, we can talk about this afterwards. I would love to.

But even if it's, you know, 2 weeks a year and a weekend a month but then periodically for a year at a time that would—that would lend itself very nicely to the way we are thinking about it.

Mr. SHERMAN. Ditto on all he said and I would add, too, I think we need to push ourselves to think creatively about how we do this.

I mentioned security clearances, but not everyone needs a secret or top secret, and particularly with the explosion of remote work that—how do we tap into talent where they don't have to all come move here to the Beltway. They can stay in Texas or Massachusetts or Washington State or wherever they are and tap into that talent.

I definitely think that's something we ought to look at. And again, on that broader cyber strategy, our third goal on there as—it's worded more finely than this but think creatively and come up with creative solutions.

I think this would definitely fit on that that we would need to explore further.

Mr. GOLDEN. Well, I suspected that you both would think that was a good idea. So, of course, my audience is the committee itself and the Senate committee. So I think that's something that we should push once again and, hopefully, get through in the next NDAA.

With the time remaining I wanted to ask either one of you to field this question, which is pretty simple and I think Pat here was onto something talking about the urgency and how quick can you move.

What are you learning just looking at the battlefield in Ukraine right now about how you can adapt on the fly to start to use data, to start to use apps, and maybe even blend, you know, those emerging technologies with the things that we already have in place right now?

Dr. MARTELL. Thanks for that follow-up, Congressman Golden.

We have lots of technology that we can bring to bear on solutions on problems and we have lots of people willing to tackle those.

The things that I've seen that have worked well is when we get that technology in the hands of a large group of people well trained and they're able to stand up quickly and deliver real value. I am happy to go into it deeper in a closed session.

Mr. SHERMAN. We better be secure, we better be agile, and we better move in a digital environment. They're fighting World War II tactics but on a 21st century battlefield and we better adapt, and we are taking lessons learned on this and particularly how we would look at a China scenario.

But I think those pillars, whether it's satellite communications, cybersecurity, or, as the ranking member noted, electromagnetic spectrum operations, how we fight through spectrum and maneuver and survive there, all these lessons are going to be relevant and speed matters. So that's what I am taking away from this.

Mr. GOLDEN. Thank you. I will yield back.

The CHAIRMAN. Dr. McCormick?

Dr. MCCORMICK. Thank you, Mr. Chairman.

The committee has been closely following the prospective sharing of the 3.1 to 3.4 gigahertz spectrum and, obviously, with the amount of technology and communication that we are doing that's just parabolically expanding we have real concerns about giving that up to the commercial industry, which would just gobble it up instantly, and once you give it away you can't bring it back.

Who ultimately makes the decision on whether that's divested from or not?

Mr. SHERMAN. As it stands right now, per a 2000 NDAA it would be the Secretary of Defense, basically, making that decision.

On proposed legislation that the administration currently backs it would be the President and his or her role as Commander in Chief, but based on direct advice from the Secretary of Defense on that matter.

Dr. MCCORMICK. Would there be any reason for the Secretary of Defense to ever consider giving up any bandwidth?

Mr. SHERMAN. Not giving it up, Congressman, but figuring out how we could share it, sharing in terms of time, in terms of geography, or in terms of radio frequency so we could conduct our military training operations here in the U.S. in homeland defense but also giving our economy an ability to stay ahead of the Chinese in areas like 5G.

Dr. MCCORMICK. With the amount of technology that continues to expand and the amount of people that keep on burdening the gigahertz spectrum, if we start sharing, though, how—I don't understand how we ever grab it back and my concern is once we start sharing it's a bottomless pit.

In other words, they will never be satisfied with what they get and they'll never want to give it back up, and the fact that we—in the military we get more and more advanced needs why would we—once again, why would we go there when there's—there's got to be another way.

Mr. SHERMAN. Well, absolutely, Congressman. We wouldn't want to vacate where we are shoved out and never to return again. Sharing would mean kind of joint ownership of this where if we are conducting military operations near an installation, conducting homeland or border security, that we would have the military radars on and be able to operate and that the telecom providers would potentially have to switch to another area, and we've got some examples we've done in past administrations where we can walk and chew gum.

But the bands you noted, sir, this 3.1 to 3.45, is beachfront property both for long-range radars as well as telecom needs here. And to the chairman's point about competition and dominating against China, I have the CIO equities for DOD.

I want our radars to work, be able to protect this homeland, keep our citizens safe. But I also know economic dominance matters, too.

So I am committed. We have a study we are undertaking right now per the Infrastructure and Investment in Jobs Act that Congress—you all tasked us to do that culminates on 30 September. No decisions would be recommended to be made until we can do our due diligence and figure out if sharing is even possible, sir.

Dr. MCCORMICK. Okay, great. I am from Camp Pendleton so I am used to that, people trying to gobble up prime real estate there.

When it comes to the battlefield and some of the technologies, I am a firm believer that we have the best staff NCOs [noncommissioned officers] in the whole world and that's why we are working better under conditions where we don't have comms [communications].

Obviously, top-heavy organizations like Russia and China don't have that luxury nor do they have the same experiences, which brings to bear that our technologies and disrupting their communications become paramount, as well as securing our own because it's always—as an ANGLICO [Air Naval Gunfire Liaison Company] guy I've always had problems with disruption of frequencies.

The CHAIRMAN. Sorry. I was just excited. That was me.

Dr. MCCORMICK. He loves the ANGLICO. He loves ANGLICO.

[Laughter.]

Dr. MCCORMICK. I guess my question is do you feel like, and this—I am not asking any secret questions—do you feel like we are putting enough investment into that counter-comm and in the comm abilities in the military.

Mr. SHERMAN. So what you're talking about, sir, are electromagnetic spectrum operations. What we've done—we did in Vietnam, we had to do in Desert Storm, Bosnia, and elsewhere, but to different degrees in Afghanistan and Iraq. But as we get ready for China we better be able to fight and dominate in this space.

So, to your point, sir, I think investments from what I've seen are sufficient now but this is something I am going to bird dog very carefully from my office here, particularly as we see the services starting to kind of regenerate electronic warfare and other capabilities both to put the enemy back on their heels and ensure our NCOs and our trigger pullers can stay in touch with one another.

As we've seen on the Ukrainian battlefield, all the dynamics with EMSO [electromagnetic spectrum operations] of how the Russians are trying to use it and the Ukrainians are using it that we cannot be cut off on this to be able to make sure we can conduct combat operations.

Dr. MCCORMICK. So your feeling is right now we are doing adequate but we need a big investment for the future to continue with this?

Mr. SHERMAN. I think we need to keep a close eye on it here and monitor as we regenerate this capability that we had in the Cold War, that we had to kind of maybe somewhat turn away from a bit during the War on Terror.

As we regenerate it I want to assure this committee I am going to keep a close, close sight on this as we move forward.

Dr. MCCORMICK. I yield.

The CHAIRMAN. Well, I apologize for that. I got carried away with the gavel. Like the Ring of Power it ultimately corrupts.

So I recognize Mr. Luttrell.

Mr. LUTTRELL. Keep it handy.

Gentlemen, thank you for being here in front of us today.

You talk about data quality as one of your pillars and I absolutely understand the importance of data quality. But as we move forward here, aggregating the data is, obviously, what's most important because you talk about sensor to shooter.

My question is are we utilizing retrospective data or prospective data only, either one? Because as dirty as data is and we have to filter it, and as Mr. Golden said, we are trying to keep pace with China.

But if we don't have the infrastructure in place how are we going to clean that data to give that information back to the shooter, as you say?

Dr. MARTELL. Thank you for that question, Congressman Luttrell.

That's a can of worms in a number of ways, right.

So do we wait till the data is clean before we act? No. So we are going to have to act on dirty data until we—until we get it right.

One way we'll tackle this is to say no new bad, so we know that we have to deal with the past stuff, the systems and the data that have been built—that have been built in ways that are not up to snuff but we need to make sure that things going forward are doing things right.

So part of the way we think about this is as we built up this infra [infrastructure] new things that we bring on board are doing data right.

But we absolutely do have to go back and recontract as contracts come up as we have to reacquire things. We have to—part of what we are going to deliver are the contracting vehicles that allow folks to specify this is what good data looks like and this is what getting data looks like, getting it right.

And the other thing I just want to add is distributed governance and building CDO [Chief Data Officer] structures down through the components is extremely important to this.

Mr. LUTTRELL. It just seems——

Dr. MARTELL. It has to be aligned with incentives.

Mr. LUTTRELL. It seems like such a slow process considering the silos that we all work in, especially in government.

Dr. MARTELL. It's absolutely a slow process, sir. But so we have to be able to do that slow process and get it right while simultaneously still allowing for new folks to deliver value.

That's a balance that we are going to have to strike. There's not going to be a way to snap our fingers and just have it get it right fast.

Mr. LUTTRELL. Sure. This is going to be a follow-up, but we—you and I are going to have to meet because this is—sitting on a panel with a bunch of shooters right here, who's setting the inclusion criteria for the data that's inbound and do we have that infrastructure?

We are talking about exascale computing here. I mean, forget about petaFLOPS [floating point operations per second]. If we are doing real-time maneuverability it's got to be quick. It has to be that lightning fast, and given just the footprint of the American arsenal itself does DOD have that infrastructure?

I know DOE [Department of Energy], as far as I know, has the fastest computer in the world, Summit, and I don't know if DOD is even anywhere close to that.

Mr. SHERMAN. Well, not for high—yes, we have high-performance computers. But to your point, this is why that Joint Warfighting Cloud Capability we had to stick the landing on this and we got it now with four companies in no particular order—Oracle, Google, Amazon, and Microsoft—all bringing their cloud computing capabilities—and, sir, I know you're familiar with this—out to that tactical edge and that's what we are pressing, whether it's out on an island—inside the First Island Chain or somewhere in Eastern Europe or Sub-Saharan Africa to be able to have our special operators or wherever cloud computing capabilities, OCONUS [Outside the Continental United States] as well. State of the art.

And this is why JWCC and as we move past that JEDI cloud procurement that had all the issues that we have this now, and we are going to have it at all three security classifications up to top secret, which is going to be a game changer on this and that's why this has been so important, sir.

Mr. LUTTRELL. Is there a beta test in process—progress right now or a scalable program that's in place that you can—that we can see, so in real time?

Mr. SHERMAN. Well, we could show you. We have cloud capabilities already underway in the Department and——

Mr. LUTTRELL. I am talking all the way from where I can reach out to—I can reach out to an operator on the ground say this is what I—I am receiving this.

Mr. SHERMAN. I think we could show you that. And the other thing, sir, I will tell you we are building off what the Intelligence Community has pioneered and I know you have likely seen some of this yourself, sir. So we are—we are not reinventing any wheels on this. We are riffing off what my IC [Intelligence Community] counterparts have done.

So, sir, we'll take that for the record and we'd be happy to try to set up a demo or something on that for you, sir.

Mr. LUTTRELL. That'd be great. Thank you. I yield back, Mr. Chairman.

The CHAIRMAN. Mrs. Kiggans.

Mrs. KIGGANS. Thank you, Mr. Chairman. Thank you to our panellists for being here today.

As a liberal arts major also I've done some reading about spectrum and the backbone of our communications network and using abundantly by the public and private sectors alike.

So the latest battleground over spectrum allocation involves the mid-band, which is crucial not only for 5G and cellular data but also for DOD, missile defense, air navigation, space asset tracking, and several other critical uses.

Private spectrum for telecommunications use is vital for economic growth and global connectivity. While the importance of federal spectrum allocated to DOD for national security purposes cannot be overstated.

So given the competing interests between public and private sector spectrum needs, what proposed solutions does your office think are viable for band sharing, going forward? And are there other lower spectrum bands being explored for DOD use?

Mr. SHERMAN. Ma'am, we're—to the study we are conducting here on that 3.1 to 3.45 gigahertz that's beachfront property set for the radars as well as the telecoms [telecommunications companies].

We have a study underway, culminates on 30 September, that we've been leading since last year sharing—not vacating, not where we get kicked out of it, and where DOD has to go find some other spectrum, which will be very difficult, but how do we walk and chew gum and figure out, again, from geography, time and radio frequency use how do we make all this orchestra work together with the telecoms in this highly congested but highly desirable space?

We are examining this right now and we would note that this is one of the most difficult parts of band analysis we've ever done just because it is so desirable both for long-range radars to acquire missiles and so on but also for 5G propagation.

So we are studying this. But what I just talked about, those three principles of time, geography, and radio frequency, are what we are thinking.

If we are going to find a potential solution to this, that's how it's going to be done with the telecoms and that's why I am working so closely with Commerce [Department of Commerce] and NTIA [National Telecommunications and Information Administration] and our interagency partners to make sure we look at the angles on this. But protecting this country is paramount consideration on this.

Mrs. KIGGANS. Thank you. And then I have a couple bases in my district. I represent Virginia's Second District, so Master Jet Base Oceana.

Just listening to users over there, and I don't know if this is the right venue to ask, but I just want to communicate some complaints of those guys.

When—they got a lot going on, right. They're training to fly. They're flying jets over there. But they complain about the computers and when you ask them what frustrates you about your job, what can we do better, it's the computers and it's the time to log on and I don't know—it's the security portals that they have to go through. It's the wifi capabilities. It's the age of the equipment.

So it's—for me, it's the little things. We talk about quality of life and recruitment and retention for our armed forces, and that's what they communicate. I mean, number one, it's—infrastructure is a big one. But, I mean, computers is the second thing that they tell me.

So I am assuming this is your department. I mean, are those things that—those little day-to-day things for those end users that they just show up and they want to go home to their families at night too and they get frustrated?

And I want to do better for them so how can you help me do that?

Mr. SHERMAN. So we are going to lean in and the term we use is called user experience. But, really, it's the fix our computers piece what you're getting at.

And I got to tell you from my—however much longer I am in this job this is a top priority here and we already have some wind in our sails on this as the budget comes out here shortly, some investments we are making.

It's a multifaceted problem. It is, yes, some new hardware. It is, yes, having cybersecurity scans that don't conflict with one another. It's having fiber on base down in Norfolk or where else.

It's not having dated hardware like routers and switches and stuff that have been allowed to atrophy. It's a multifaceted problem.

And just yesterday, ma'am, I was talking to the Air Force's Chief Experience Officer about how we do things like measure and not just go anecdotes, because I hear a lot, too, from the sailors and airmen and guardians and everybody else.

But what can we do to really monitor the network to know when the spinny wheel is happening for the sergeant at Fort Eustis and she's trying to get her maintenance report in.

We are going to get after this because we are not going to fight with one hand tied behind our back, and it is a quality of life issue, ma'am, and I am dedicated to getting after this.

Mrs. KIGGANS. Thank you so much. Please make that a priority, and I yield back. Thank you.

The CHAIRMAN. Mr. Deluzio.

Mr. DELUZIO. Mr. Chairman, good afternoon. Good morning. Lost track of the time of day.

Good morning, Mr. Sherman, Dr. Martell. Thanks for being here. Thanks for your work and your team's work to protect our information technology, cybersecurity, our networks. I think folks often don't understand what goes into that good work. So thank you.

In our full committee hearing yesterday with NORTHCOM [U.S. Northern Command], SOUTHCOM [U.S. Southern Command], Assistant Secretary for Homeland Defense and Hemispheric Affairs, one of the issues we touched on that I asked some questions about was defense of our critical infrastructure, which I think is a place that, obviously, touches defense but, certainly, homeland security and other parts of our vital defenses here.

And we talked about not just malicious actors in China and otherwise but one of the—some of the challenges coming from the fact that much of our critical infrastructure is privately owned. It's not just under public control.

So, Mr. Sherman, I will start with you if you could talk about what those challenges are, what we can do better, what, you know, this subcommittee and our committee should be thinking about.

Mr. SHERMAN. So the biggest thing is just what you said. We are going to take this seriously here. We need to work across the interagency as we work with Homeland Security, CISA [Cybersecurity and Infrastructure Security Agency], my friend, Jen Easterly over there—I've worked with her for years—on how we work across all the industrial sectors.

Now, for us at DOD, the Defense Industrial Base piece, the defense critical infrastructure, is where my line of sight is, but this is going to take a whole of government, whole of industry, and folks taking it seriously, and this is where we could continue to use your assistance here on the subcommittee and the broader HASC [House Armed Services Committee] is making sure COs [commanding officers] and others don't see this as a nice to have—we saw Colonial Pipeline 2 years ago and other places—that this isn't just a blinky lights something that you can invest in if you want to.

This is critical. An adverse actor can take down your entire—whether it's a pipeline, network. We've seen technical debt in things like with air traffic control and things that have happened recently. We've got to take this very seriously.

So at Department of Defense we are focused on the Department of Defense Information Network but also our critical infrastructure.

And one thing I have is budget certification authority where I can hold services' and others' feet to the fire to make sure they're having appropriate investments, and we need to do better on this, on areas like defense critical infrastructure to make sure we are protecting that piece of our enterprise as well, sir.

Mr. DELUZIO. Well, as a follow-up, you know, how would you—and for folks who aren't as dialed into what it is we are discussing—the work that goes into defense of critical infrastructure—how do you compare where our Defense Industrial Base is relative to other components of our critical infrastructure in this country?

Mr. SHERMAN. Sir, I think that would be hard from my seat as the DOD CIO to do a holistic looking across energy, automotive, and everything.

I will know that—say that in the defense side we know that's where the Chinese, Russians, and others are trying to expropriate plans, blueprints, and everything else, and really trying to help work with that industry to lock that down.

I would just add, working with our interagency partners on all the different areas, raising awareness of this—we have a new National Cyber Strategy. There's been other executive orders and so forth. Working with you all here in Congress to raise awareness about this.

And we've had some notable incidents, I think, that have been in the news that are raising companies' awareness. So we have to keep up the press and not stop on that.

Mr. DELUZIO. I will ask maybe just one more follow-up.

Pieces of the way that we ensure cybersecurity in the Defense Industrial Base do you think have application to other components of our critical infrastructure in other sectors?

Mr. SHERMAN. I think it absolutely does as we have standards that I know some may see as onerous and we are working with industry to not make it onerous.

But to make sure there's something we can all hold ourselves to account, and implementing basic cybersecurity. The National Institutes of Standards and Technology, which I know sounds bureaucratic, has standards to be able to apply on basic things, on principles like two-factor authentication, end-to-end encryption, and things that all companies ought to be able to looking at to do.

And I grew up in South Texas in an area where we had a very small family company. I know how it is to have federal regulations land on somebody in Victoria, Texas or elsewhere. But we've got to be thoughtful about, whether it's a small company or a big one, that everybody should take responsibility on this.

Mr. DELUZIO. Okay. Mr. Chairman, thank you.

Mr. Chairman, I yield back, and I think I did use two acronyms, NORTHCOM and SOUTHCOM. I apologize.

The CHAIRMAN. It's going into your social credit score.

Mr. DELUZIO. Fair enough.

The CHAIRMAN. Mr. LaLota.

Mr. LALOTA. Thank you, Mr. Chairman.

Gentlemen, appreciate you being here and your leadership, your dedication, sharing your experiences with us.

I represent a suburban district east of New York City, 750,000 people in Suffolk County. We, Mr. Chairman, are America's district and appreciate the dialogue we have here today.

Last September the government of Suffolk County suffered a cyberattack that shut down many of the government services that my constituents rely upon. Emergency dispatchers had to take down 911 calls by hand. We had no access to the geolocating function that's typically normal there.

Police were forced to use finicky radio transmissions in call incidents and had no access to email reporting from the field. Contractors were paid in paper checks. That created a huge backlog of services in the county.

At the county's traffic agency people were unable to pay pending tickets, which created extra fees and became a huge hassle in Suffolk County.

In addition to the major shutdown of government services, the hackers who claimed responsibility for the attack threatened to slowly leak sensitive information that the government had at hand and, unfortunately, the situations like this aren't unique to Suffolk County.

We are constantly hearing about cyberattacks, data spillage, and ransomware and phishing throughout the country almost on a daily basis. If hackers can have such an effect on my county I fear that there can be a larger government entity, state, or, God forbid, our federal government be subject to a similar attack.

The Office of the CIO, as I understand it, was responsible for the DOD IT enterprise cybersecurity. I, too, am a liberal arts major so I am leaning a little bit into this as well. And I do understand that you have protection over our unclassified and classified networks.

So my question is this to both of you, please, gentlemen. What is your office doing to gather lessons learned from these state and local attacks to ensure that their prevalence, their impact, is reduced prospectively?

Mr. SHERMAN. Sir, we work closely across the interagency—I mentioned DHS and CISA, for example, Department of Homeland Security—to learn about the very unfortunate attack against your district there, sir, and elsewhere, where we hear about attacks against schools, industries, and elsewhere, and what we call the targets or, excuse me, tactics, techniques, and procedures—TTPs is the government acronym on that—on how the adversary is using these mechanisms to employ ransomware or to hack into systems.

I work very closely with the U.S. Cyber Command and the National Security Agency, which is both under General Paul Nakasone, and from them I not only get the cyber aspects but also the threat-based intelligence of what state and nonstate actors are doing and how they're operating and evolving.

This is something I do every week and multiple days a week working with them to understand how we ought to be defending differently. I mentioned earlier about a concept called Zero Trust where we assume an enemy is already on our network.

This is the state of the art on—we've talked about it for a while but we are getting after it at the Department of Defense on not just the old perimeter defend at the castle and moat, and not even what we call defense in depth but really preventing an adversary's ability to move across a network and hold data at risk as what happened in the attack you described, sir.

So we must be a learning organization and stay very up with the threat-based intelligence on how an adversary is going to operate.

Mr. LALOTA. Can you describe what your interactions are or will be with state and local governments to that end? I understand that you properly explained the big picture on what the issue is and how it should be attacked.

But I fear that information, that guidance, isn't getting to the local officials where the rubber meets the road.

Mr. SHERMAN. Sir, my interaction would not be direct. It would be through the Department of Homeland Security who would interact with the state and locals there and also, maybe obliquely, where we have, of course, U.S. military installations and garrisons that are relying on defense critical infrastructure, power, and so on, coming on to those garrisons and bases and so on.

But primarily through DHS is where that interaction and where I am going to be hearing about what's happening in your district and also where if we are seeing something from a national security perspective U.S. Cyber Command working with them could share that from a national security perspective.

Mr. LALOTA. Thank you.

Switching gears for a moment, Congress required the Department of Defense to establish a comprehensive framework for the cybersecurity of the Defense Industrial Base in section 1648 of the 2020 NDAA.

Their support was a full 2 years late and yet didn't seem to address a host of problems that still seem apparent about how the DOD manages the Defense Industrial Base cybersecurity.

Did section 1648 force any lasting change to how the department manages its support to the Defense Industrial Base?

Mr. SHERMAN. It absolutely motivated it and we've got to keep doing better on this front. As we conduct outreach to the Defense Industrial Base, as we organize ourselves internally, there's over a dozen DOD entities, large offices that are touching this sector here to make sure we are organizing properly and not double communicating or sending conflicting messages and also offering services as—to the Defense Industrial Base.

For example, the National Security Agency's Cybersecurity Collaboration Center works—has service——

The CHAIRMAN. Your time has expired. However, I was going to ask that question in the second round. So why don't we plant a flag there and we'll come back to it? Sorry.

Mr. SHERMAN. Roger. I will be right at audible, sir.

The CHAIRMAN. I am a rule follower, a Catholic Marine. So I am sorry.

Mr. Keating is recognized for 5 minutes.

Mr. KEATING. Thank you, Mr. Chairman.

I just had one strain of questioning. Thank you both for being here.

I noticed, Dr. Martell, your background on the private side. I noticed the experience, you know, as head of machine learning for Lyft and head of machine intelligence for Dropbox as well as leading several IE teams' initiatives at LinkedIn, and I also know the challenges we have with workforce and getting trained educated people throughout our workforce.

So I was wondering, given that background that you had, what plans you might have to leverage from those experiences and expand knowledge and skill sets in AI across the Department of Defense as a whole.

Can we do those kind of things internally as well and can we expand what we have?

Dr. MARTELL. Thank you for that question, Congressman Keating.

I was born in Massachusetts, by the way.

Mr. KEATING. Well, we won't hold that against you.

Dr. MARTELL. Thank you. It's a tough year for the Red Sox this year. So I think perhaps but——

Mr. KEATING. Go Bo Sox.

Dr. MARTELL. So I think we have to get at two things here. If you look at what a—what talent used to be needed for AI it was Ph.D. level expertise.

As the tools become commoditized and as just education, even JPME [joint professional military education], for example—professional military education—sorry, sir—professional military education is starting to add more data, more AI, more IT literacy, that the need for that expertise is going down.

So I think there's two ways we can tackle this. One is we need to upskill folks we already have. We've already built out 10 new work roles that are specific to AI—with Honorable Sherman's org [organization] that are specific to AI and data, and my team has—is beginning to do analyses across the Department about which components need which work roles.

Secondarily, I think we can—we need to work with the services and the civilian orgs to be able to give actual careers to folks who want to do those sorts of work roles.

Currently, it's the case that you—if you're in the service you might do a data work role for one tour and then you move on to something else and you're doing something completely different.

And, in addition, your promotion is not based upon being successful in the data aspects. Your promotion is based upon, for example, if you're an unrestricted line officer on your leadership.

So we need to actually think hard about how we can have the careers and the motivations in those careers drive expertise in data, AI, et cetera.

Simultaneously, I think we really need to tackle some untapped aspects of our workforce in the U.S. If you went to a select school you're going to have people pounding down your door to give you a very expensive job offer. I think that's great, and if we can motivate those folks to come into the service, to come into government, that's wonderful.

But there's a number of folks who might be just below that level or just a little bit below that where we can serve as an apprenticeship that transforms their capabilities.

And so we might take a hit on the front side where we are having to do extra work to bring them up to speed. But at the end, we have folks who are highly capable, and my view is we actually want to encourage those highly capable folks to go out to industry because that motivates people to come in the other side of the pipeline.

Now, they might stay forever. That would be awesome. But if we are seen as the ones that take you from not being able to get that amazing job, come work with us, and then you get that amazing job, I am very happy with that.

Mr. KEATING. I am really glad to hear that. It really echoes and what I learned way back in my MBA [Master of Business Administration] days in a Massachusetts college BC [Boston College]. So I really am pleased that you're going in that direction.

Thank you so much, and I yield back.

The CHAIRMAN. Onto a second round, I want to pick up where we left off with Mr. LaLota's question. He mentioned that the Section 1648 report was 2 years late. Additionally, DIB [Defense Industrial Base] cybersecurity is your responsibility, correct?

I am tracking, however, at least six separate offices within OSD [Office of the Secretary of Defense] who have asserted leadership—some sort of leadership role in protecting the Defense—I did an acronym—Defense Industrial Base. Not DIB. Defense Industrial Base. To outside organizations and entities.

So two questions. One is Mr. LaLota's question—did the report force change, and then, two, what are you doing in your role to bring coherence to an effort that, from my vantage point, looks somewhat scattershot at present?

Mr. SHERMAN. So to riff off that earlier question, yes, it has driven change, Congressman. Absolutely it has.

Onto the how are we organizing ourselves for victory here, so when I got this last year, looking—polling around DOD how many organizations are touching a Defense Industrial Base company, whether it's a small or medium or one of the big primes, and it's more. It's 12 to 13, depending upon how we count it.

And I first held a meeting and brought all them in a room—Defense Contract Management Agency, Defense Counterintelligence and Security Agency, DOD Policy [Office of the Secretary of Defense for Policy]. I can go down a list.

But putting myself in the shoes and talking to a lot of companies, how does this feel when you have got different entities either providing helpfully or trying to be helpful providing information or coming to you with a requirement?

So what we've done, my acting deputy, who's also the chief information security officer, has stood up a monthly cadence with these organizations to get ourselves aligned on the DIB Management Council here. I think we call it something a little bit different.

But bringing these organizations, who's sharing what, who's talking to whom. Let's get aligned here and, again, put ourselves in the shoes of the affected companies.

So maybe it could be helpful. It could be threat-based intelligence that maybe national security agencies providing through that collaboration center I mentioned or another entity, and they need to be cross talking so if they hand something to one company and they say also, we got this from another DOD organization.

So that's what we are doing, sir. We are trying to align this and make it a little more sensible and less bureaucratic.

The CHAIRMAN. But you consider yourself the leader of that council?

Mr. SHERMAN. Yes, sir.

The CHAIRMAN. Of the six different offices that——

Mr. SHERMAN. Actually 12. Yes, sir.

The CHAIRMAN. Well, okay.

Mr. SHERMAN. Yes, sir.

The CHAIRMAN. Twelve different offices.

Okay. Mr.—Dr. Martell, excuse me—before JADC2 we had the Joint Information Environment. Before the Joint Information Environment we had the Global Information Grid.

Have you reviewed those past efforts to understand why they failed and what you might do differently so that JADC2 does not suffer the same fate?

Dr. MARTELL. Thank you for that question, Chairman Gallagher.

When I—I have been in the office now eight months and I've tried very hard to ignore history, and the reason I have is as I started going down that rabbit hole I felt myself being inculcated with the old ways of doing things.

So I've asked myself what's the right solution, and we are now just turning to making sure that this right solution maps correctly to our goals.

So, look, I think the right solution is building out a marketplace that allows multiple vendors to bring apps to bear where these older solutions were—and I am going to defer a lot to Honorable Sherman because I believe these were under his purview—but they were older—these older solutions had rigid requirements that were established a long time before delivery and by the time the delivery came the world has changed.

We need to create a marketplace and infrastructure that allows for that dynamic change and that's how we are tackling JADC2.

The CHAIRMAN. Mr. Sherman, in what little time I have left, I am pleased to hear that we are moving out on a multi-cloud expeditiously. However, it seems we just lost the last 2 and a half years.

What lessons should we derive from that?

Mr. SHERMAN. Sir, do you mean in terms of the acquisition or what did we learn in the 2 years?

The CHAIRMAN. Well, both. What did we learn——

Mr. SHERMAN. So this was one area here that—yes, as the U.S. government it shouldn't take us this many years to get enterprise class for the Department of Defense and we mention about the CCP and if Xi on that side said something—he needs something that quickly he'll have it very quickly.

We have to do better as a whole of government here in being able to procure and acquire services for the Department of Defense. This is an area we did get through. There was no protest. It's ready to go.

But this is something that, frankly, sir, we should have been able to do more quickly and without all the bureaucratic and other issues that came up.

Now, on the functional piece the upshot here we have what we've learned on the intelligence side with our multi-cloud multi-vendor approach, and then also within the military services their own cloud efforts.

You hear terms like Cloud One and others. That's the Air Force effort. We have a lot of lessons learned we are integrating into this enterprise cloud effort. So we are not at a standstill. We have a running start from what we did there, sir.

The CHAIRMAN. My time is about to expire.

Does either Mr. Khanna, Mr. Keating, Mr. Luttrell—any more questions?

You guys got off easy today.

Well, with that, I just would emphasize a couple points as we close.

One, I think you saw a lot of interest in sort of general talent management and whether we are adequately using the authorities that Congress has given you, particularly Cyber Excepted Service authorities. I know we talked about that earlier this week, Mr. Sherman.

So I would like to develop some sort of routine process whereby you can come and tell us, here's how these authorities are being used, here's what we are learning, and here's, you know, where we may need—we could expand it or maybe we can't expand it.

So I just would hope you would commit to that, going forward.

And then, Dr. Martell, we had a little bit of a discussion about metrics. I just would encourage you to think through and would welcome a follow-up discussion on what is achievable.

I recognize that, you know, the Pentagon is a massive aircraft carrier. It doesn't turn on a dime. But what is achievable in the next 2 years? What can we really deliver to our warfighters within the next 2 years?

And so I would be eager to work with you on what are fair metrics in both of those areas, going forward.

And with that, the hearing is adjourned.

Oh, we are going to move into a closed session—closed briefing.

And now the hearing is adjourned.

[Whereupon, at 10:48 a.m., the subcommittee was adjourned.]

APPENDIX

MARCH 9, 2023

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

MARCH 9, 2023

Chairman Mike Gallagher
Cyber, Innovative Technologies, and Information Systems Subcommittee
Defense in a Digital Era: Artificial Intelligence, Information Technology, and Securing the Department of Defense
March 9th, 2023

Good morning, and welcome to our CITI hearing on "Defense in a Digital Era: Artificial Intelligence, Information Technology, and Securing the Department of Defense." A reminder of the three CITI commandments: (1) we shall start on time; (2) five minutes shall be five minutes; (3) thou shalt not use acronyms nor jargon. Simple and direct language that normal Americans can understand

We are joined today by the Department's Chief Information Officer, Mr. John Sherman, and the inaugural Chief Digital & Artificial Intelligence Officer, Dr. Craig Martell. I welcome both of you, and especially Dr. Martell in his first appearance with the House Armed Services Committee. You both have very important jobs, and our job is to ensure you do your jobs well.

To underscore the stakes, I'd like to quote a recent report from our friends at the Australian Strategic Policy Institute: "research reveals that China has built the foundations to position itself as the world's leading science and technology superpower, by establishing a sometimes stunning lead in high-impact research across the majority of critical and emerging technology domains…[including] artificial intelligence (AI)…and key quantum technology areas.…In the long term, China's leading research position means that it has set itself up to excel not just in current technological development in almost all sectors, but in future technologies that don't yet exist. Unchecked, this could shift not just technological development and control but global power and influence to an authoritarian state where the development, testing and application of emerging, critical and military technologies isn't open and transparent and where it can't be scrutinized by independent civil society and media. In the more immediate term, that lead…could allow China to gain a stranglehold on the global supply of certain critical technologies. Such risks are exacerbated because of the willingness of the Chinese Communist Party (CCP) to use coercive techniques outside of the global rules-based order to punish governments and businesses, including withholding the supply of critical technologies."

Gentlemen, I'm concerned we're losing in key areas of this strategic competition and I'd prefer to win. As we say in Green Bay: winning isn't everything, it's the only thing. That's especially true when the fate of the Free World is at stake. So I look forward to our witnesses telling us how we fight smarter and win.

STATEMENT BY

JOHN B. SHERMAN

DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER

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 9, 2023

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 Dr. Craig Martell who is the Chief Digital and Artificial Intelligence Officer (CDAO). 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 in the 118th Congress. 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 (MILDEPs) and Defense Agency's IT and cybersecurity's budgets. Dr. Martell, the senior official responsible for strengthening and integrating data, artificial intelligence (AI), and digital solutions in the Department and myself work closely to ensure shared missions are met.

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 five fiscal year budget assessments and determinations, beginning with the Fiscal Year (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.

Cyber Workforce Strategy

We are continuing to develop a workforce capable of operating within the cyber domain, defending against adversaries, and supporting larger, critical CIO initiatives and efforts such as the Joint Warfighter Cloud Capability (JWCC).

A cyber workforce strategy is a priority of this office with a goal of enabling the Department to be able to close workforce gaps while expanding its cyber workforce and developing talent to securely build, operate and maintain its digital and critical infrastructures to protect and defend our data against cyber adversaries.

The recently signed DoD Cyber Workforce Strategy establishes the direction for unified management of the cyber workforce and outlines a roadmap for its advancement.
The strategy outlines four goals: 1) Execute consistent capability assessment and analysis processes to stay ahead of force needs, 2) Establish an enterprise-wide talent management program to better align force capabilities with current and future requirements, 3) Facilitate a cultural shift to optimize Department-wide personnel management activities, and 4) Foster partnerships to enhance capability development, operational effectiveness, and career broadening experiences.

To achieve these goals, we must pursue meaningful actions that reduce the talent pipeline gap, increase the quality and diversity of our cyber workforce, and prioritize professional development.

Our goals align to four key pillars: 1) Identification of needs 2) Recruitment 3) Development, and 4) Retention. First, we need to identify workforce needs and requirements. Second, it is critical we cast a wide net to attract the talent needed to meet these requirements and continually evaluate these efforts. Once the need is identified, and the talent acquired, teams and individuals must be provided the resources to be successful. Finally, incentive programs enable the Department to retain critical talent. We are using these pillars to drive the cultural shift necessary at the Department to ensure our workforce is agile, flexible, and responsive to the changing cyber domain, its threats, and its challenges.

Cyber Workforce Strategy Implementation Plan
We are shaping an agile and innovative implementation plan with clear measures of effectiveness to successfully enhance recruitment and retention of a cyber workforce.

DoD Cyber Workforce Framework Expansion
While the strategy sets the direction for unifying the cyber workforce, the DoD Cyber Workforce Framework (DCWF) provides the foundation for targeted human capital management and establishes a common data model for data-driven decision making. The DCWF has been used across the DoD to advance our understanding of cyber work roles, identify critical needs and gaps, and take action to advance a workforce capable of protecting our nation against ever evolving threats. Given its success the Deputy Secretary of Defense directed the Department to expand the DCWF. Working with the CDAO and Dr. Martell we have included new work roles for artificial intelligence, data and analytics, and software engineering. This expansion shows the utility of the framework methodology. The data driven framework is now used to assess and report on the health of the broader innovation workforce. We will continue expansion efforts to support other critical mission sets.

DoD Manual 8140
DoD Manual 8140 sets the foundation for identifying, qualifying, and upskilling our workforce according to the DCWF. DoD Manual 8140 policy series consists of a directive, instruction, and manual and was published in February of this year.

The manual is critical to our workforce as it establishes the qualification criteria for each DCWF work role to ensure personnel filling cyber positions are capable of meeting mission requirements.

Using the DCWF, the manual enhances interoperability and cyber readiness across the Department by providing a common baseline and understanding of cyber concepts, principles, and applications. The program also provides a continuing professional development mechanism for the Department to ensure the workforce maintains current knowledge and capabilities in the rapidly changing cyber domain.

Through the manual, DoD is expanding the qualification program from a population of less than 90,000 to more than approximately 225,000 military, civilian and contractor positions by establishing foundational and residential qualification criteria for each DCWF work role. Together, the strategy, implementation plan, and 8140 policy series will enable the DoD to develop and deploy an agile, capable, and ready cyber workforce.

Cyber Excepted Service

The DoD Cyber Excepted Service (CES) personnel system was established to ensure that the cyber warfighters are the first positions to be filled by utilizing a wide range of tools and program elements that is unmatched with current competitive service system opportunities. CES works in coordination with the DCWF coding of our workforce.

We are implementing a unique set of tools and programs, such as on-the-spot job offers, pay-setting flexibilities, no time-in-grade requirements, qualified-based promotions, target local market supplements, and advancement and development opportunities to achieve recruitment, retention, and development flexibilities across the Department.

Analytics

Data is key to all our initiatives. We developed an authoritative data analytics platform that provides leadership with enterprise-wide visibility into the cyber workforce using the DCWF work roles. This real-time data aggregation enables DoD leaders to make information-driven decisions to fill gaps through an enhanced way of identifying its workforce mix and conducting a more targeted analysis for fixing recruiting and retention challenges.

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.

We offer the DoD Cyber Scholarship Program (CySP) that provides scholarships to students in pursuit of cyber-related degrees at designated institutions. Each recipient is provided with a DoD internship, giving them hands-on experience and exposure to DoD cultures and agencies. This results in workforce members who are better qualified and better equipped, and it starts the clearance process with interns so that applicants are pre-cleared before beginning full-time work.

In addition, we work with the Centers of Academic Excellence (CAE) program that consists of direct relationships with over 400 universities, colleges, and community colleges with verified curriculum aligned to requirements outlined by the DCWF. CAE students work directly with grant-recipient professors to perform DoD research.

In November 2022, the DoD expanded the cybersecurity workforce by eliminating educational barriers and leveraging registered apprenticeship programs. Removing formal education barriers, combined with the use of apprenticeship programs, provides a faster pipeline to acquire talent, increases talent pool, and enhances diversity by allowing applicants to enter the workforce through nontraditional pathways. Efforts including registered apprenticeship programs enhance our cybersecurity workforce and complement the Administration's focus on diversity, equity, inclusion, and accessibility. Closing the talent gap is critical to strengthen and safeguard our Nation's cybersecurity. Moreover, removing formal education barriers and providing nontraditional skills-based pathways is a step that brings DoD closer to our goal of scaling up a workforce that are critical to mission readiness.

Zero Trust

The DoD has made great strides in establishing a strong foundation for Zero Trust (ZT) adoption and implementation. In January 2022 we established the ZT Portfolio Management Office (ZT PfMO). Last July 2022 we released the ZT Reference Architecture and subsequently, in October 2022, the ZT Strategy and Implementation Roadmap. This document provides strategic guidance, direct alignment of efforts, and prioritize resources for accelerating ZT adoption across the DoD. This includes defining capabilities and activities required to achieve Target Level ZT, which all of DoD must achieve, and Advanced Level ZT, necessary for some systems and data, applications, assets, and services. The DoD ZT PfMO hosted quarterly technical exchange meetings with the MILDEPs, Joint Staff, Unified Combatant Commands (CCMDs), National Security Agency (NSA), and the Office of the Director of National Intelligence, to ensure a clear understanding and alignment of the ZT mission, goals and objectives, and strategy roadmap. The ZT PfMO collaborated and shared updates with the Department of Homeland Security Cybersecurity and Infrastructure Security Agency, NATO, and our international partners to ensure the Federal Government and our allies and partners are moving towards successful adoption and implementation of ZT. DoD is striving to be a leader in the Federal Government on implementing ZT at scale, starting with our most critical networks and systems. With full buy-in from the DoD and its partners, this will be readily achievable.

ZT Pilots and Training Activities

The DoD ZT PfMO will ensure DoD components have the technical options available to implement ZT. The DoD ZT PfMO will initiate a series of ZT pilot scenarios in mid-2023. Additionally, we are working with NSA to develop a Native ZT Cloud which will be a government-owned private cloud designed to achieve more advanced levels of ZT.

The DoD ZT PfMO has been working with the Defense Acquisition University to develop ZT curricula and training courses. Through this collaboration, the DoD ZT PfMO published the DoD ZT Awareness Course on the DoD's Joint Knowledge Online Platform, enabling the DoD's workforce to receive foundational training on ZT. The DoD ZT PfMO is continually developing training curricula, including a Practitioner's Workshop course to upskill the DoD's workforce.

With continued intra-departmental collaboration, the DoD can be a leader in the ZT cultural shift across the Federal Government.

Identity Credential and Access Management

DoD Identity Credential and Access Management (ICAM) efforts provide key foundational support for the implementation of numerous key DoD initiatives to include ZT, Joint All Domain Command and Control (JADC2), and Mission Partner Environment. 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 2022, the DoD CIO, in coordination with the DoD Comptroller, completed several pilots to see how we can leverage ICAM's capabilities to address access control and segregation of duties of financial systems and fielded several new Enterprise ICAM capabilities. DoD CIO will also require components to implement the enterprise capabilities or leverage a DoD CIO approved ICAM offering if the enterprise capability cannot meet the mission requirement. Defense Information Systems Agency (DISA) and NSA will continue to work together to develop an enterprise ICAM approach for dynamic access, which is a key capability to enable attribute-based access control that relies on user and environmental attributes for access.

Cryptographic Modernization

Cryptographic Modernization is another enduring effort essential to our intelligence, information, and warfighting platforms. The emergence 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.

Cybersecurity Maturity Model Certification 2.0

The Department is committed to working with the defense industrial base (DIB) and other stakeholders to achieve our shared objective of protecting national security information. In November 2021, we launched Cybersecurity Maturity Model Certification (CMMC) 2.0 to meet evolving threats and safeguard the information that supports and enables our warfighters, with a simplified approach to compliance. We are currently in the process of codifying the CMMC 2.0 program through the rulemaking process to update the Title 32 of the Code of Federal Regulations (CFR). We will be supporting the Office of the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)), as they lead the effort to update the Defense Federal Acquisition Regulation Supplement (DFARS) through the 48 CFR rulemaking process.

We understand how consequential these changes will be for DIB members whose contracts with the Department that process Controlled Unclassified Information (CUI), and we are especially sensitive to how this program might affect small and medium-size businesses. Our outreach efforts include working with DoD's Office of Small Business Programs, and which is providing resources to small businesses to improve their cyber readiness, others across the Department, to ensure that all potential partners in the DIB and academia understand the

National Institute of Standards and Technology (NIST)-based standards that already contractually apply to those who are handling CUI. We have also had industry roundtables and town halls, where our DoD Deputy CIO for Cybersecurity (DCIO(CS)) discussed how to advance DoD's and industry's shared objectives in cybersecurity risk assessment and management, information sharing, emergency preparedness, incident management, and response coordination. In addition, we continue to expand our programs for assisting industry in understanding and applying the cybersecurity practices necessary to protect themselves and DoD's sensitive information.

Implementing and Integrating Cybersecurity Guidance and Policies

The DoD CIO plays an enterprise oversight and advisory role for cybersecurity across the Department.

Strategic Cybersecurity Program

The USD(A&S) oversees the Strategic Cybersecurity Program (SCP), with an NSA program management office (PMO) performing execution. DoD CIO's role has been supporting USD(A&S) efforts, providing oversight to the NSA SCP PMO, and using CIO budget authorities to ensure components are resourcing for SCP efforts and mitigations and verifying their execution through the cybersecurity budget certification process.

National Security Memorandum-8

DoD is improving the cybersecurity of its NSS following guidance from National Security Memorandum 8, "Improving the Cybersecurity of National Security, DoD, and Intelligence Community Systems," which requires all agencies with NSS to ensure that their systems are upgraded to more rigorous, cybersecurity standards. DoD CIO published Department guidance to incorporate the NSS Checklist into components authoritative inventory tools and categorize each DoD system accordingly.

DoD Risk Management Framework

The updated DoD Instruction 8510.01 "Risk Management Framework (RMF) for DoD Systems," incorporates greater cyberspace accountability for DoD components and information systems by executive program officers, program managers, authorizing officials, and cyberspace and functional operational commanders throughout system lifecycles. It applies an integrated enterprise-wide decision structure for the RMF that includes and integrates DoD mission areas and risk governance process. Finally, it provides guidance on reciprocity of system authorization decisions for the DoD in coordination with other federal agencies to reduce redundant testing, assessing, documenting, and the associated costs in time and resources.

Mitigating Supply Chain Risk for Information and Communication Technology and Services

OMB Memorandum 22-18 Implementation

In implementing EO 14028, the Office of Management and Budget directed in M-22-18 that all Federal agencies seek attestations from software producers about secure software development practices (pending OMB's identification of minimum elements of NIST 800-218) for software in use by agencies that fall within the scope of M-22-18. The DoD CIO is collaborating across the

DoD to meet the various requirements of the memorandum, which will by necessity, require rulemaking for an anticipated Federal Acquisition Regulation, and possible DoD supplement.

Authorities to Exclude and Remove
The DoD CIO is leading the effort to address high-risk information and communication technology vendors by leveraging 10 U.S.C. §3252 and interagency engagement with the Federal Acquisition Security Council.

Implementation of Guidance
To address information and communications technology and services (ICTS) supply chain risk, NIST has updated multiple guides, to include Special Publications 800-53 Rev. 5 "Security and Privacy Controls for Information Systems and Organizations," and 800-161 Rev. 1 "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations." DoD is adopting these updated guides to drive ICTS supply chain considerations into systems designs.

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.

Joint Warfighting Cloud Capability
Last December, the Department awarded the Joint Warfighting Cloud Capability (JWCC) fulfilling our commitment to deliver an enterprise-level multi-vendor, multi-cloud ecosystem to address longstanding requirements and capability gaps in support of the warfighter.

JWCC enables mission owners to contract directly with these Cloud Service Providers (CSP) to create a strategic technological advantage on future battlefields at all three classification levels – Unclassified, Secret, and Top Secret. JWCC provides foundational commercial cloud services and capabilities that enable transformational initiatives such as JADC2 and the Artificial Intelligence and Data Accelerator in coordination with CDAO. JWCC allows for streamlined provisioning of cloud services, fortified security, and commercial pricing parity. Features of JWCC include capabilities and parity of services at all three classification levels, integrated cross domain solutions, global availability inclusive of tactical edge locations, and enhanced

Cybersecurity controls. We will guide and ensure that the Department utilizes JWCC to the maximum extent possible.

Outside the Continental United States Cloud

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 environments. These CSPs give the Department access to multiple, global fabrics that ensure our warfighters can conduct operations anywhere in the world.

The current crisis in Ukraine and JADC2 experiments are demonstrating 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 CCMDs, the MILDEPs, and forward deployed partners to deliver the latest cloud computing and communications technologies to meet these requirements.

Cloud and Data Center Optimization

Through strong partnership with DoD Components our Cloud and Data Center Optimization initiative is enabling the Department to achieve its vision for 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. We have successfully migrated or decommissioned over 760 systems and closed 49 data centers with plans to close 11 additional data centers by FY 2025.

DoD Software Modernization

Last February, we released the Department's Software Modernization Strategy, highlighting the Department's adaptability 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 is preparing to release the Software Modernization Implementation Plan that identifies key FY 2023 and FY 2024 activities, milestones, and responsibilities for driving process improvements and new capabilities to achieve the Software Modernization Strategy goals.

The JWCC award brings us closer to achieving our goal of accelerating the adoption of the Department's enterprise cloud environment, which is a core enabler of our software modernization initiatives, especially the development of Department-wide software factory ecosystem enabling advanced modern software practice such as Development, Security, and Operations (DevSecOps). DevSecOps allows for continuous monitoring of the DoD network 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 expand the DoD

CES approach to offer flexibilities for the recruitment, retention, and development of software professional across the Department.

4th Estate Network Optimization

Today's challenges require that we implement a digital enterprise that maintains pace with commercial innovation and delivers IT efficiently. Through 4th Estate Network Optimization (4ENO), the Department is modernizing DoD IT infrastructure and streamlining the digital enterprise. 4ENO converges the 26 networks that the Defense Agencies and Field Activities (DAFAs) independently own, operate, and manage to a single unclassified network domain and a single classified network domain while eliminating redundant networks, and supporting global access that reduces barriers for joint information sharing, strengthens cybersecurity, and improves end user experience.

To date, four DAFAs completed their migration to the Global Service Desk (GSD) and three DAFAs have migrated 700 users across six sites to the new single service network known as DoDNET. This resulted in the consolidation of six legacy networks and a refresh of network hardware. Between FY 2023 and FY 2026, 4ENO aims to migrate an additional 96,000 users from over 470 sites and transfer nearly 800 more FTEs to the GSD. While 4ENO is a long-term effort, it reflects the Department's commitment to enhance efficiencies, modernize capabilities, and improve operational effectiveness.

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 drive rationalization across the portfolio to buy-down technical debt, and enhance user experience across the Department, ultimately transforming the way the Department does business.

The Department is committed to managing DBS as a strategic asset. We have successfully transitioned business system responsibilities to DoD CIO, including the annual certification, as the result of the repeal of the Chief Management Officer. The Department will use functional and technical criteria to lead a more data-driven annual certification process per 10 U.S.C §2222 authorities and ensure our DBS portfolio aligns to the strategic priorities and direction of the Department. We are driving to fundamentally transform processes to enable a highly efficient business environment that effectively supports our national defense priorities.

Warfighting Command Control and Communications

Command, Control, and Communications C3 systems are fundamental to all military operations to deliver the critical information necessary to plan, coordinate, and control forces and operations across the full range of Department's missions. DoD CIO is leading the way ahead for future development, implementation, fielding, and sustainment of strategic and tactical C3 capabilities. The critical capabilities in this portfolio are a priority for the enterprise.

Electromagnetic Spectrum

Electromagnetic spectrum (EMS) is important to every DoD mission, in every domain. Spectrum not only provides the critical connective tissue that enables all-domain operations but 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.

As the Department's senior official responsible for coordinating across the 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 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.

Spectrum Sharing

The DoD supports efforts to ensure U.S. dominance in 5G and next-G development. Previous DoD success in making spectrum available for commercial use through the Advanced Wireless Services -3, Citizens Broadband Radio Service, and America's Mid-Band Initiatives Teams are testaments to this 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. As I testified during my confirmation hearing before the Senate Armed Services Committee in 2021, "Spectrum sharing must be our watchword going forward" for the U.S. to maintain both its global leadership position and the capabilities of our armed forces.

The Department remains committed to making mid-band spectrum available for industry while meeting our mission requirements. Within the 3100-3450 band, the DoD relies on hundreds of air, sea, and land-based radars for a wide range of missions. It would be untenable for DoD to outright vacate these systems from the parts of the spectrum in which they currently operate. To do so would take decades, cost hundreds of billions of dollars, and cause significant mission impacts to the Joint Force's warfighting readiness and capabilities.

We continue to make strong progress in the spectrum sharing study of the 3100-3450 band, our as required by the Infrastructure Investment and Jobs Act (IIJA). To inform this study, DoD is coordinating closely with the Department of Commerce and leveraging the technical expertise of government, industry, and academia. We will report our findings to the Department of Commerce by September 2023 as required by the IIJA.

Our efforts build on previous sharing initiatives led by the Department. We are committed to helping maximize U.S. 5G and Next G dominance while also ensuring that the Joint Force can both train and conduct operations in and near the continental U.S. where use of terrestrial, airborne, and sea-based radars operating in the mid-band are critical for success.

5G

The DoD CIO continues to work on 5G through contributions to international standards development organizations, and through participation in the Under Secretary of Defense for Research and Engineering (USD(R&E)) led 5G Cross Functional Team (CFT), to identify and provide implementation guidance for both dual-use commercial and military focused 5G technology applications that provide the optimum return on investment to the Department. Our current focus is on the development of required enterprise capabilities, and associated security policy/infrastructure to support the MILDEPs in their implementation of 5G Information and Communications Technology across all military installations in line with the FY 2023 NDAA. Finally, in accordance with the FY 2021 NDAA, the DoD CIO is preparing to assume leadership of the CFT on October 1, 2023, and will continue to work in close coordination with USD(R&E) and USD(A&S).

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. In order 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. In a joint effort by the Navy and DISA, global timing resiliency is being achieved though the Critical Time Dissemination initiative and Defense Regional Clocks.

Enterprise Satellite Communications Modernization

The DoD is rapidly accelerating its satellite communication (SATCOM) services modernization, with particular focus on our international and commercial partnerships. The Department is nearing the conclusion of a ground teleport sharing arrangement with Australia that will offer both participants increased operational capacity and resiliency. As the Department shifts to a Future SATCOM Force Design, diverse commercial and military services will be blended into a single operational enterprise, achieving more agile and scalable communication transport.

Recently, the Department released its Enterprise SATCOM Management and Control Reference Architecture, Implementation Plan, and SATCOM Terminal Reference Architecture for delivering automated SATCOM resource allocation to the warfighter quickly. We are now implementing a solution that establishes cloud-based enterprise services and secure automated resource allocation across military and commercial SATCOM communication service provided networks.

Following commercial SATCOM industry's lead, we are 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.

As the Department integrates commercial SATCOM, we must stay focused on protecting our infrastructure and networks from adversarial threats. The Department worked with industry over the past two years and issued the "Information Assurance – Pre" program where commercial solutions are assessed and graded on the ability to protect the Departments information streams.

SAP IT

The Deputy CIO for Special Access Program (SAP) IT is responsible for policy, oversight, and governance of all need to know SAP IT programs and cybersecurity activities across the Department. The office has made significant progress in establishing, enhancing, and maturing SAP IT policy and governance. Working closely with the team in the DISA, we have implemented repeatable and reliable approaches for managing, coordinating, and protecting SAP IT. These efforts include modernization of the legacy stand-alone "Chinstrap" desktop hardware system. The Compartmentalized Enterprise Desktop (CED) is DoD's new cloud-based virtualized desktop. CED installation and Chinstrap decommissioning is underway and is on track to be completed by the end of the month of March 2023.

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 is 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.

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.

CHIEF DIGITAL AND ARTIFICIAL INTELLIGENCE OFFICER
Statement for the Record
House Armed Services Committee
Subcommittee on Cyber, Information Technology, and Innovation
March 9, 2023

Chairman Gallagher, Ranking Member Khanna, and distinguished Members of the Subcommittee, thank you for the opportunity to testify before you today. Today is my first appearance before Congress, and I look forward to sharing the ongoing efforts of the Chief Digital and Artificial Intelligence Office (CDAO) and the broader Department of Defense (DoD) related to data, analytics, and artificial intelligence and machine learning (AI/ML).

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.

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 functions:

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

It is an honor to serve our Nation as the first DoD CDAO. The importance of this role, the mission of the CDAO, and our service to the warfighter are not lost on me. From my experience as a professor of machine learning at the Naval Postgraduate School, to my time leading machine learning teams at some of the most prominent technology companies in the U.S., I'm proud to bring the best practices and lessons learned from my prior roles to enhance, accelerate, and scale the application of data, analytics, and AI/ML to the national security mission.

The National Defense Strategy identifies four top-level defense priorities the Department will pursue: defending the homeland, paced to the growing multi-domain threat posed by China; deterring strategic attacks against the United States, allies, and partners; deterring aggression while being prepared to prevail in conflict when necessary; and building a resilient joint force and defense ecosystem. Data, analytics, and AI/ML play a role in all these priorities. They are core capabilities underpinning the Department's operational and business analysis and decision making in support of the Secretary of Defense's (SECDEF) priorities to Defend the Nation, Take Care of Our People, and Succeed Through Teamwork. They are also core capabilities in the execution of Joint warfighting functions, especially Joint All-Domain Command and Control (JADC2). The CDAO is focused on using data, analytics, and AI/ML to advance these top Department priorities.

To that end, when I arrived as CDAO in June 2022, my team and I first assessed data, analytics, and AI/ML activities and needs at all levels of the DoD. We studied the comprehensive recommendations from the National Security Commission on Artificial Intelligence (NSCAI). We assessed existing and emerging digital technologies within DoD, partner organizations, and commercial industry. We talked to experts and stakeholders to understand digital transformation in the context of DoD's mission and environment. From these efforts, we identified a Digital Hierarchy of Needs (Figure 1), four areas necessary to accelerate and scale data, analytics, and AI/ML adoption in support of DoD priorities:

- Improve data quality
- Enable advanced analytics
- Provide AI/ML services
- Cultivate key enablers

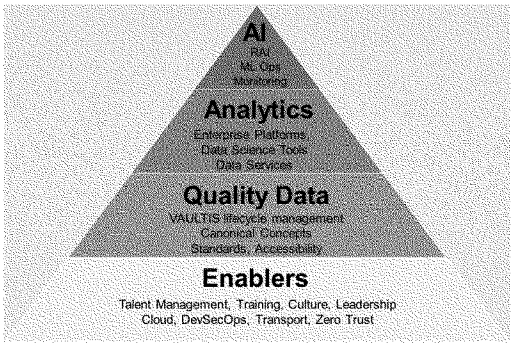

Figure 1. Digitial Hierarchy of Needs

More detail on each of these areas follows.

<u>Quality Data</u>

The foundation of every effective analytic and AI capability is quality data. That is why improving data quality is the CDAO's top priority. Quality data that is usable for analytics and AI must possess the seven "VAULTIS" attributes:

- Visible – Consumers can locate the needed data

- Accessible – Consumers can retrieve the data
- Understandable – Consumers can recognize the content, context, and applicability
- Linked – Consumers can exploit data elements through innate relationships
- Trustworthy – Consumers can be confident in all aspects of data for decision-making
- Interoperable – Consumers have a common representation/ comprehension of data
- Secure – Consumers know that data is protected from unauthorized use/manipulation

Over the last few years, DoD has established a solid foundation for data quality, and we are leading initiatives to scale that work. For example, as a result of the 2020 DoD Data Strategy and 2021 Creating Data Advantage memo, data silos that were once ubiquitous across the Department are now coming together in a federated data ecosystem. The ecosystem allows components to find and access data from sources across the Department and develop analytics and dashboards to support mission needs. The Advancing Analytics (ADVANA) platform has provided key capability in this area. ADVANA provides a centralized data lake using manual and semi-automated collection and aggregation of prioritized data across the DoD enterprise. Today, ADVANA has connected more than 390 DoD data sources with almost two petabytes of data; it has 31,000+ users across 190+ organizations and 12+ functional communities; it has saved DoD more than $11B from improved auditability; and it has allowed DoD to improve its response to crises like COVID-19, Afghanistan withdrawal, and Ukraine assistance.

In addition to providing an enterprise data platform, we are improving data quality through mission-focused initiatives. By applying data and analytics to solve real operational problems, we identify and then improve data quality in a way that immediately impacts mission outcomes. For example, through the Accelerating Data and AI (ADA) initiative, we are embedding digital teams within Combatant Command (CCMD) CDOs to improve CCMD decision support. ADA teams enable rapid data discovery and analytic development efforts across a range of capability areas. ADA teams have developed applications to automate and improve business and operational processes within and across CCMDs in various areas, including personnel, logistics, and financial management. We are implementing a similar approach with OSD Principal Staff Assistants (PSAs) by embedding digital teams within PSAs to help them access and use high-quality data to support SECDEF and DSD decisions on implementation of the National Defense Strategy and Strategic Management Plan.

We are also improving warfighting data quality, focused on enabling Joint All-Domain Command and Control (JADC2). The CDAO is developing a Joint data integration layer to improve access to, and interoperability of, data required for C2 at the strategic, operational, and tactical levels of war. We understand the strategic value of the American technology sector and are committed to unlocking DoD data so it is easier for software companies to develop applications for DoD warfighters to use in JADC2. We are also leading iterative experimentation and assessment of the data integration layer through a series of Global Information Dominance Experiments (GIDE) focused on Joint Warfighting Concept key operational problems, emphasizing the pacing challenge in the Pacific and globally-integrated deterrence. Our first CDAO-led GIDE event concluded in February, and we are applying lessons and insights into future experiments, which are planned about every 90 days.

There is more work to do to scale data access and improve data quality beyond the data used in ADVANA, JADC2, and ADA and PSA use cases. We are leveraging and empowering the Department's Chief Data Officers (CDO) at every command to improve data quality by managing data as a product. Managing data as a product means data stewards actively provide data they produce or manage to customers in a way that directly meets customers' needs. It is a shift from traditional program management functions that DoD uses to develop and deliver hardware systems. A data product manager's job is never done; they must iteratively and agilely work with customers from across the DoD enterprise to ensure their data products meet mission needs as they evolve. To orchestrate better data quality, we are also improving data governance through our DoD-wide CDAO Council, and with allies and partners through the Five Eyes CDO Council.

DoD is committed to treating data as a strategic asset, and the CDAO is committed to making trusted, high-quality data widely and readily available for business and warfighting decision-makers and mission partners.

Advanced Analytics

In speaking with military commanders across the force this past year, the most requested digital capabilities were more advanced analytics and dashboards to help them visualize and make better decisions about how to manage their resources, readiness, people, and operations. Analytics provide the ability to measure, visualize, and sometimes predict the various factors that impact a decision. If quality data is available, data scientists and other analysts both in DoD and in the commercial sector can build and tailor models to explore variables and offer unique data-informed insights to leaders.

The DoD analytics environment has traditionally consisted of many disparate business intelligence capabilities that used siloed data, focused on only one functional domain, and existed in on-premises computing environments. Most analytic applications relied on old data, collected at monthly or even quarterly intervals, and senior governance and decision-making bodies relied on PowerPoint slides instead of real-time analytics.

Over the last few years, DoD has made significant progress in integrating data and providing commercial state-of-the-art tools for organizations to create their own analytics and dashboards to support decision makers. DoD is also using real-time analytics in key senior decision meetings up to the SECDEF and DSD levels. The ADVANA platform, described above, has been instrumental in this progress. ADVANA has enabled development of analytics in financial, contracting, readiness, logistics, medical, personnel, and other areas. A key benefit of the ADVAVNA environment is how makes data from multiple sources accessible to both DoD analysts at all levels to create their own dashboards and analytics, and commercial software providers on contract with DoD organizations to develop more sophisticated applications.

Today, the CDAO is scaling ADVANA efforts beyond current use cases to support decision making across all SECDEF priority areas. We developed "Pulse," a performance management application that connects data and provides analytics to measure progress on SECDEF priorities, including the implementation of the National Defense Strategy and the Strategic Management Plan. As a result of this work, the Department is increasing transparency in execution and improving the quality of its measures, moving from input metrics to output metrics on the majority of its priorities. There is endless opportunity to apply advanced analytics to the broad and diverse aspects of DoD business and operations. ADVANA has given DoD a foundation of quality data and analytic tools so leaders can make data-driven decisions to improve Department effectiveness and stewardship of taxpayer resources.

The CDAO is also applying analytics to JADC2. In addition to developing a Joint data integration layer to unite Service, Intelligence Community, and mission-partner data and make it discoverable and accessible across echelons, C2 nodes, and operational forces, we plan to use the acquisition authority Congress authorized for us to make it easier for industry to develop software applications for Combatant Commands and Joint users. Our approach will assert government rights over DoD data while giving CCMDs and Joint users a reliable acquisition path to leverage innovative industry software solutions that convert data into decision advantage.

AI/ML Services

Since DoD released its first Artificial Intelligence Strategy in 2018, DoD has made significant strides in bringing AI/ML to the warfighter and business decision maker. The CDAO established an ML development environment with tools, like Sage-Maker and Databricks, which provide integrated development environments for composing ML workflows to bring AI/ML to enterprise and business applications, including procurement, human resources monitoring, and investments. We have seen great value in computer vision use cases, such as vehicle detection and tracking in support of force protection missions; natural language processing to automate the search of large amounts of policy and contract documents; predictive maintenance capabilities to maximize up-time for air, land and sea fleet vehicles; and fraud monitoring to enhance business operations by detecting anomalous patterns in contractual money flows.

To scale AI/ML development across DoD, the CDAO is defining the appropriate enterprise scaffolding to facilitate development in the most effective, secure, responsible, and sustainable way. By 'scaffolding,' we mean the enterprise infrastructure, data, tools, services, and best practices that any AI/ML developer – whether in government or industry – can leverage to produce AI/ML capabilities for the national security mission. Scaffolding elements include data labeling as a service, federated model catalogs, an enterprise feature store, a common library of AI packages, and test and evaluation (T&E) capabilities.

Our keystone T&E effort is establishing the Joint AI Test Infrastructure Capability (JATIC). JATIC provides an interoperable set of state-of-the-art software capabilities for AI algorithm testing & evaluation. JATIC will test model robustness, resiliency to adversarial attack, the ability of humans to understand and trust model outputs, and competence. It will also ease model deployment, integration, and compatibility, thus integrating seamlessly into the various AI/ML pipelines that different DoD organizations have adopted.

An integral component of our AI/ML adoption plan is promoting the tenets of responsible AI. The Department's desired end state for responsible AI is trust. Trust in DoD AI will enable the Department to modernize its warfighting capability across a range of combat and non-combat applications and consider the needs of the DOD's internal and external stakeholders. Trust is also critical to our relationships with like-minded nations as we expand partnerships and collaboratively set new international norms for AI usage which respect democratic values such as privacy and civil liberties, while defending against adversarial aggression. The CDAO is either the lead or participating in over 40 of the 64 lines of effort designed to develop capacity with partner and allies and is guiding or executing alongside responsible AI leaders. We are also working closely with NATO, FVEY partners, and the 16-nation AI Partnership for Defense initiative, which we lead to advance the responsible development and use of AI in defense around the world.

Key Enablers

While getting the technology right is why the CDAO was created, none of this can be sustained without taking care of the people and providing enablers that drive digital transformation, breaking down technological and acquisition barriers, and drive the growth of our network of highly skilled personnel and international relationships.

The CDAO is managing digital talent by attracting, recruiting, hiring, and employing highly talented individuals. As the lead office for the data, analytics, and AI work roles in the cyber workforce, the CDAO is championing the effort to expand the DoD Cyber Workforce Framework (DCWF). In partnership with DoD CIO, the CDAO established 10 data and AI work roles across the DoD which collectively include 106 new tasks and 80 new knowledge, skills, and abilities (KSAs) deemed important for strengthening DoD's innovation workforce. To promote the culture and infrastructure for digital talent in the Department, the CDAO is designing and implementing the Defense Digital Corps (DDC) pilot program to create a cadre of DoD digital talent that will be available to meet surge demand and tackle key problems. CDAO will manage the DDC, providing mentorship, networking, and professional development aligned with skillsets, while creating a pipeline to attract, recruit, flexibly hire, and creatively employ digital talent from across the Nation.

CDAO is using its acquisition authority to transform acquisition processes within the Department in support of AI expertise, joint synchronization, agile contracting, and stronger relationships with industry and academia. We are breaking down barriers in the acquisition process in order to quickly and repeatedly identify and acquire critical AI technologies from traditional and non-traditional DoD partners. The use of innovative and decentralized procurement vehicles such as T&E Blanket Purchase Agreement and TryAI Commercial Solutions Opening allow CDAO to rapidly purchase and deliver key AI services and enabling tools. CDAO's Tradewind platform leverages an Other Transaction Authority to identify, acquire, and operationalize critical AI technologies from traditional and non-traditional DoD partners, quickly and repeatedly. Tradewind is available throughout the DoD and has successfully awarded contracts to multiple services and components.

Conclusion

The CDAO was created to provide lasting value to the Department. We are focused on pursuing an integrated strategic approach across data, analytics, AI/ML, and enabling activities. These activities include fostering an educated, empowered workforce; leveraging the strengths of commercial software development; continuing iterative experimentation and assessment to determine the right capabilities and architecture to support mission needs; and effectively integrating our data and activities with allies and partners. I look forward to working closely and transparently with the Subcommittee on these issues, and others, as we enable DoD's current and future use of data, analytics, and AI/ML for national security.

Dr. Craig Martell
Chief Digital and Artificial Intelligence Officer

Dr. Craig Martell currently serves as the Chief Digital and Artificial Intelligence Officer (CDAO) for the Department of Defense. His appointment as the CDAO brings extensive industry experience and expertise in artificial intelligence (AI) and machine learning (ML) to the Department. Dr. Martell's experience in AI/ML includes serving as the Head of Machine Learning for Lyft, the Head of Machine Intelligence for Dropbox as well as leading a number of AI teams and initiatives at LinkedIn, most notably the development of the LinkedIn AI Academy. Previously he was a tenured computer science professor at the Naval Postgraduate School specializing in natural-language processing (NLP). Dr. Martell has a Ph.D. in Computer Science from the University of Pennsylvania and is the co- author of the MIT Press book *Great Principles of Computing*.

WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING

MARCH 9, 2023

RESPONSE TO QUESTION SUBMITTED BY MR. RYAN

Dr. MARTELL. The initial prototype (version 1.0) for the data integration layer, that CDAO is building in the classified cloud for experimentation, will be available by the end of May 2023 for usage in GIDE 6 (June and July). This sustained experiment will allow for CDAO to assess the performance of the data layer and measure the impact of its services to warfighter workflows. Subsequent revisions of the data layer will be deployed quarterly to align with the ongoing series of experiments. [See page 13.]

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

MARCH 9, 2023

QUESTIONS SUBMITTED BY MR. GALLAGHER

Mr. GALLAGHER. Between the war in Ukraine, persistent counter-terrorism operations, and recent brazen actions by the CCP, the need for advanced data, algorithmic and AI capabilities is more urgent than ever. Some Combatant Commanders are really leaning in here. For example, GEN Kurrilla's team is discussing leveraging data-driven technology at CENTCOM to create new warfighting concepts and GEN Van Herck's team is discussing something similar at NORAD/NORTHCOM. I understand much of this work is on the back of significant congressional investment in Project Maven and continued through the CDAO. What is your plan to expand the capabilities the DoD has employed there across the Combatant Commands? Are there any funding issues that will prevent accelerating the expansion?

Dr. MARTELL. In FY23, CDAO received $36.8M for the tactical integration of AI in combatant commands. This resource supported a limited rollout of Maven Smart System to each of the geographic combatant commands on certain networks through the end of Q1 FY24 as an R&D activity. CDAO put heavy emphasis on INDOPACOM, EUCOM, CENTCOM, and NORTHCOM to match NDS priorities and meet ongoing user demand. In aggregate, the FY23 $36.8M appropriation will not meet CCMD demand for integrated software solutions that enable decision advantage within the combatant commands, as the user demand for advanced digital solutions continues to skyrocket.

Therefore, for FY24, CDAO has requested $225.5M for its JADC2 Project Management team. A notional breakdown of funding follows: (actual costs will depend on negotiated contract rates)

- CCMD mission applications (~$127.5M)—Establishing an enterprise business model for procuring existing mission command applications to improve the acquisition approach (e.g.,safeguarding government data rights), ensuring efficient allocation of development and sustainment licenses, and standardizing best practices within mission applications across Combatant Commands. This will include, as appropriate, the Maven Smart System or alternative capabilities as determined in partnership with the Combatant Commands, warfighters, and appropriate contracting and acquisition officials.
- Data Integration Layer for JADC2 (~$54M)—Developing data mesh services and enabling capabilities to integrate data across CCMDs, the Joint Staff, and the Services to ensure accurate, timely, and secure data flow across DoD organizations.
- GIDE Experimentation (~$44M)—Using user-centered experiments to test the effectiveness of workflow support applications and the data integration layer in achieving decision advantage. CDAO believes this approach to evolving data and applications in tandem with user-centered concepts, and measuring effec-

tiveness, is the best way to evolve JADC2 capabilities across organizations and domains, while also building a robust commercial marketplace for software providers to DoD. Building on our efforts in FY24, future efforts would expand to additional CCMDs in accordance with the priorities set out in the National Defense Strategy and would require additional funding.

QUESTIONS SUBMITTED BY MR. MOULTON

Mr. MOULTON. With the looming vulnerability of our nation's cryptographic enterprise due to advances in quantum computing, can you tell us the full scope of effort required to prepare for the continued protection of national security information?

Mr. SHERMAN. Ultimately, the full scope of effort will require the migration of our vulnerable national security systems to a quantum resistant capability. DoD components will accomplish this incrementally as technology and solutions become available for procurement and integration. Success also hinges on industry's timely commitment to adopt stronger algorithms. Our crypto modernization efforts must ensure the protection of information from the moment of transmission to the end of the intelligence life of the information from 25–50 years, depending on the classification of the information.

Mr. MOULTON. When will we know how much it will cost to get to continuous modernization of encryption, to include post-quantum, and how do you assess the 'critical path' to get there?

Mr. SHERMAN. Crypto Modernization (CM) is an enduring effort that includes recurring procurement, integration, and sustainment costs. These efforts are driven by Chairman of the Joint Chiefs of Staff guidance for CM planning and the retirement dates for cryptographic algorithms also referred to as the last year of use date. DoD components are beginning to specify their CM requirements for the FY25 Program Objective Memorandum (POM). We anticipate DoD organizations will have improved cost projections in their FY26 POM projections as the next generation of Quantum Resistant (QR) cryptographic capabilities become available for procurement.

Also, as NSA publishes the formal cryptographic modernization requirements for the CM2 initiative later this year, DoD organizations will also begin to program funding to modernize and replace their currently fielded systems. Although NSA has released its full list of high-assurance quantum resistant algorithms specifications for use in NSS, the National Institute of Standards and Technology (NIST) will not release their list of medium assurance public QR algorithms until mid-2024. This timing gap will impact many NSS programs' ability to POM for future encryption devices as many of these cryptographic devices rely on the NSA high grade algorithms to protect data transmitted or stored, and require the public medium assurance algorithms for software, firmware, and user authentication.

QUESTIONS SUBMITTED BY MR. FALLON

Mr. FALLON. Mr. Sherman, the reality of today's workforce requires personnel to use their own devices to conduct business for the Department of Defense. This is especially true for members of the National Guard and Reserves. 13 other federal agencies have developed programs to secure personal devices and allow them access to their networks, but not the DoD. What steps are you taking to develop a "bring your own device" policy that would allow for necessary flexibility while maintaining security? Have you contemplated moving to a device or application-centric security model that would allow for necessary access and isolate threats to a single application instead of the entire DODIN?

Mr. SHERMAN. On August 10, 2022, the DoD CIO released policy guidance to DoD components that allows them to develop and tailor their Bring Your Own Device (BYOD) solution(s). The DoD policy allows users to voluntarily participate in the BYOD initiative. DoD components are responsible for following and integrating all applicable Security Technical Implementation Guides (STIG) and the DoD CIO's guidance for use of non-government mobile devices, excluding laptops. The DoD CIO's office is currently refining a mobile applications policy to ensure the protection of information on mobile devices.