[H.A.S.C. No. 117–50]

HEARING

ON

NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2022

AND

OVERSIGHT OF PREVIOUSLY AUTHORIZED PROGRAMS

BEFORE THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS

ON

DEPARTMENT OF DEFENSE INFORMATION TECHNOLOGY, CYBERSECURITY, AND INFORMATION ASSURANCE FOR FISCAL YEAR 2022

HEARING HELD
JUNE 29, 2021

U.S. GOVERNMENT PUBLISHING OFFICE
45–433 WASHINGTON : 2021

SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS

JAMES R. LANGEVIN, Rhode Island, *Chairman*

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

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

JOSH STIEFEL, *Professional Staff Member*
SARAH MOXLEY, *Professional Staff Member*
CAROLINE KEHRLI, *Clerk*

CONTENTS

DEPARTMENT OF DEFENSE INFORMATION TECHNOLOGY, CYBERSECURITY, AND INFORMATION ASSURANCE FOR FISCAL YEAR 2022

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON CYBER, INNOVATIVE
TECHNOLOGIES, AND INFORMATION SYSTEMS,
Washington, DC, Tuesday, June 29, 2021.

The subcommittee met, pursuant to call, at 4:02 p.m., in room 2118, Rayburn House Office Building, Hon. James R. Langevin (chairman of the subcommittee) presiding.

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

Mr. LANGEVIN. The subcommittee will come to order. So I want to welcome everyone to today's hearing on the Department of Defense information technology, cybersecurity, and information assurance. This is the subcommittee's first hearing on the Department's current IT [information technology] efforts and the requested investments for fiscal year 2022.

Since this subcommittee was formed at the start of the 117th Congress, our members have been eager and encouraged to see the Department of Defense approach its information technologies with a prioritization that has been lacking in the past. Of the many lessons from the pandemic, we have seen clearly that technology can revolutionize how we conduct our business, whether that is in Congress, or in the Department of Defense. However, it also requires that the infrastructure which enables our technology is prioritized and secured in a commensurate way.

In my many years in Congress, I have witnessed firsthand the progress that the Department has made in improving the ways in which it can utilize technology. Nevertheless, there is still tremendous work to do. Year after year, we have leaders from across the Department tell us that they consider IT to be a priority before immediately pivoting to discuss how much funding they need for more flight hours, or more aircraft, or more tanks.

Quite frankly, I would like to think that technology will truly be a priority when, for example, the Chief of Naval Operations says that the Navy can live with one less fighter aircraft in favor of greater IT investment.

Through multiple National Defense Authorization Acts, the Congress has judged it prudent to empower the chief information officer [CIO] in managing the Department's technology portfolio.

Today, the CIO is a Senate-confirmed position, has oversight over each of the service's IT budgets, and manages not only the Department's networks, but also its electromagnetic spectrum enterprise and command and control and communications efforts. This places the CIO in a unique operationalized role, contributing to success in the Department's "no-fail" missions.

At the same time, there are still questions about how the Department of Defense defines the roles and responsibilities for cyber matters. If the Secretary of Defense is asked who is in charge of buying weapons for the Department, the answer is unequivocal: it is the Under Secretary of Defense for Acquisition and Sustainment.

Conversely, if the Secretary is asked who is in charge of keeping DOD networks safe, the fact that there isn't a single correct answer is troubling. The Secretary could respond with the chief information officer, or the commander of Cyber Command, or even the chiefs of the military services, and he wouldn't technically be wrong in any of these responses.

So if we can teach every one of our new officers about the criticality of clear command and control, why can't it apply—apply this to the highest levels of the Department?

So with that as the context, I want to welcome Mr. John Sherman, who appears in front of the subcommittee today. Mr. Sherman serves as the acting chief information officer. And while we have had the pleasure to work together since assuming the role in January, this is his first appearance before a HASC [House Armed Services Committee] hearing. He is a career member of the senior intelligence service and previously served as chief information officer of the U.S. intelligence community.

So, I thank you, Mr. Sherman, for your service and your commitment to the United States and the work that you are doing in DOD [Department of Defense].

But before we get to you, I would like to now yield to Mr. Franklin, who is stepping in for Ranking Member Banks. Scott, the floor is yours.

[The prepared statement of Mr. Langevin can be found in the Appendix on page 29.]

STATEMENT OF HON. C. SCOTT FRANKLIN, A REPRESENTATIVE FROM FLORIDA, SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS

Mr. FRANKLIN. Thank you, Mr. Chairman. Thank you, Mr. Sherman, for your time here with us today.

The Department's information technology and cybersecurity budget may not be the most riveting subject, but it is certainly one of the most critical. IT undergirds every Department, or every part of the Department, whether it is protecting our Defense networks from adversaries; managing the DOD's spectrum to ensure swift, clear communication with our troops around the world; or deploying IT or software—secure software, IT is foundational from weapon systems to financial management.

In an enterprise as large as the Department of Defense, with its many missions, different systems, and multiple stakeholders, we are fortunate there has not been a catastrophic IT failure rendering our equipment no better than paperweights, or allowing adversaries to sit in our networks and capture sensitive information.

I am encouraged by the direction of the Department, but this is not an area where we can afford to slow down. Without strategic vision, resourcing, and investment in the workforce, and buy-in from leadership in the Department, failure is possible.

The IT and cyberspace budget represents roughly 7 percent of the DOD budget. So every dollar must be used wisely. I look forward to hearing your views and justifications for the budget and how you are using the dollars to pursue modernization, efficiencies, and security.

The Department of Defense has a technology deficit. And unless we make both the necessary investments and prioritizations, we risk weakening our national security, and none of us here wants that.

With that, Mr. Chairman, I yield back.

Mr. LANGEVIN. Good. Very good. Thank you, Mr. Franklin.

With that, I want to turn it Mr. Sherman for his opening statement.

STATEMENT OF JOHN SHERMAN, ACTING CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF DEFENSE

Mr. SHERMAN. Thank you very much, sir. Good afternoon Mr. Chairman, Ranking Member, and members of the subcommittee. Thank you for the opportunity to testify before the subcommittee today on the current efforts underway pertaining to the Department's information technology and cybersecurity. I am John Sherman, the acting Department of Defense Chief Information Officer.

The President's interim national security strategic guidance, as well as Secretary Austin's priorities drive the key areas I will highlight regarding the Department's cloud, software and network modernization, cybersecurity workforce, command control communications, and data.

In what I see as a critical step for the whole enterprise, we have made cloud computing a fundamental component of our global IT infrastructure and modernization strategy. With battlefield success increasingly reliant on digital capabilities, cloud computing satisfies the warfighters' requirements for rapid access to data, innovative capabilities, and assured support.

Furthermore, we remain committed in our drive toward a multivendor, multicloud ecosystem, with our fiscal year 2022 cloud investments representing over 50 different commercial vendors, including commercial cloud service providers and system integrators.

The Department's cloud conversancy and ability to leverage this technology has definitely matured over the last several years, and we are driving hard to accelerate the momentum even more in this space.

Software capabilities and networks are also critical to our success. I am pleased to announce that we will release a software modernization strategy later this summer that builds on already-developed guidance, such as DevSecOps 2.0 guidance released last month. We are dedicated to delivering resilient software capability at the speed of relevance. The fiscal year 2022 budget includes investments to enable software modernization, with cloud services as the foundation to fully integrate the technology, process, and people needed to deliver next-generation capabilities.

Meanwhile, the COVID–19 pandemic crisis changed the way we all work. The Department deployed a commercial-based collaboration capability to enable the rapid transition to remote work. While cloud access and remote work introduces a significant burden to the DOD networks, we continue to deploy secure and agile solutions.

All of these efforts must address cybersecurity from the start. The Secretary previously discussed the Department's investment in cybersecurity and cyberspace operations that will maintain the momentum of our digital modernization strategy. The fiscal year 2022 DOD cybersecurity budget maintains enhanced funding levels established in fiscal year 2020 and fiscal year 2021 for key enterprise cybersecurity capabilities that will enable us to advance our focus on Zero Trust and risk management and drive our new investments to enhance resiliency and cyber defenses. We take our responsibilities in this area very seriously given the threat landscape we face.

While all divisions on our CIO team support warfighting, it is command, control, and communications, or C3, that might be most closely linked to the warfighter on the ground, sea, air, and space domains. The critical capabilities in this portfolio, positioning, navigation, and timing, or PNT; electromagnetic spectrum enterprise, or EMSE; and 5G, are a key priority for the enterprise, especially as we face threats from our near-peer competitors.

Finally, we often note that data is the ammunition of the future. The Department has prioritized ensuring the timely, secure, and resilient access to data needed for military advantage and all-domain operations. While data management is not directly tied to specific program elements in the fiscal year 2022 budget request, we are identifying, assessing, and tracking our data-related investments as part of the budget certification process that I lead.

In closing, I want to emphasize the importance of our partnership with Congress in all areas, but with a particular focus on digital modernization and IT reform.

Thank you for the opportunity to testify this afternoon. And I look forward to your questions.

[The prepared statement of Mr. Sherman can be found in the Appendix on page 31.]

Mr. LANGEVIN. Thank you, Mr. Sherman.

So, we are going to go member questions now as we recognize in order of seniority for 5 minutes. And I will start with myself.

Mr. Sherman, first question I have, and I am going to be direct, the Department released a comprehensive summary document of its IT and cyberspace activities budget, totaling 30 pages. This year, that same document is six pages, only two of which contain any substance. Separately, this committee has made your office aware that the IT and cyberspace activities portion of this year's defense budget overview was nearly a carbon copy of the 2020 defense budget overview.

I have to be honest with you. If the Department of Defense were a high school student, I would have called this plagiarism. So with all due respect, if your office cannot be troubled to put together the necessary materials for this committee's oversight, how can we trust the stewardship of this critical portfolio?

Mr. SHERMAN. Mr. Chairman, thank you for the question. And I appreciate everything you are saying. And your staff had raised this with us a couple of weeks ago.

So, a couple of things happened on this as I have dug into this in my 6 months into the job, and particularly as it was raised recently. Part of the reduction in the length of the documents had to do with the CUI, or controlled unclassified information, designator that was put on it that, in a way, perhaps restricted the number of pages on there.

But your point, sir, about the carbon copy is something I take very seriously. Your staff has raised this with me. And I will own this and ensure we get it better next time. And, indeed, I have been laser-focused on the technology and cybersecurity, but we need to do a better job in CIO working with comptroller and other Department colleagues in the level of product we share with you. So sir, I will take this guidance on and make it a priority going forward. And I appreciate you flagging it, sir.

Mr. LANGEVIN. Without that level of detail, just to understand, we can't fulfill our oversight responsibilities. We are in the dark otherwise. And that is unacceptable going forward. So I take you at your word and we will go from there.

Also, in reviewing the Department's budget materials, it would appear that there are significant challenges between all of the various DOD entities in harmonizing how the Department categorizes its cybersecurity and IT investments. For example, the Navy does not categorize endpoint device management tools as cybersecurity funding, yet the Air Force does. As a result, it is nearly impossible to get a comprehensive picture of how resources are being spent. How can our members help you accelerate the efforts to create greater compliance and consistency in understanding the Department's investments?

Mr. SHERMAN. Sir, thank you for that. I think some of this is what we need to be doing on our own within the CIO enterprise, working with our service and other colleagues as we work the budget year to year.

To your point, and I took this once I got in the seat here, that our $5.5 billion for cybersecurity thereabouts doesn't, indeed, represent the totality of cybersecurity throughout the Department. It is a large portion of it, but to your point about endpoint security—and I will give another example, what we have done with DOD or Office 365, and some of the cybersecurity features we bought from the vendor on there are reflected in our enterprise and not cyber budget.

Cybersecurity is my top priority as CIO, along with the other modernization activities. But to be able to reflect the totality of that is something we need to do a better job of. And I think we have the tools and wherewithal internally to work with our colleagues to make sure we can reflect this more accurately. But this is something, sir, I have noticed recently, because the $5.5 billion, while an accurate assessment of cybersecurity, there are some more in the budget that we need to be able to reflect in there. So sir, we will take that on board as well.

Mr. LANGEVIN. It is important. Having that common understanding is going to help us better understand, you know, where we are lacking capabilities, where are we investing in the right place, and how our dollars are being spent.

In the statement you submitted to the committee, you noted that you serve as the Department's lead for industrial control systems [ICS] cybersecurity. You also noted that the Department is working to build cybersecurity expertise in the cyber workforce and developing capabilities to monitor ICS systems. So I have a few questions about this.

First, does the Department use the term ICS and operational technology, or OT, interchangeably?

Mr. SHERMAN. To my understanding right now, we do, sir. This is an area of late that I have wanted to really dig on, both back when I was the principal deputy CIO at the time and now as the acting CIO. To answer your question, I believe we use those interchangeably. I am working with our chief information security officer, just as recently as this week, to start to gather the documentation we have on this to ensure that we, at the departmental CIO level, have the right sort of guidance and the articulation of terms, right what you are getting at, sir, as we are using IO—and I will throw IOT, internet of things, in there as well, along with industrial control systems, operational technology, et cetera, to get at the main issue that we are not creating seams in our cybersecurity activities between the cyber defenders and our facility managers, where an adversary could go after things like HVAC [heating, ventilation, air conditioning], elevators, and other places that would allow cyber vulnerabilities. So that is where we are at right now, sir.

Mr. LANGEVIN. And what is the difference between defense cyber workforce, and cyberspace operations forces?

Mr. SHERMAN. The—I want to make sure I get this one right. The defense cyber workforce would include the way we characterize the work roles, include the cyber workforce, I believe in there, sir. So the defense cyber workforce is based only the framework of the occupational series we have, I believe there are 54, of any type of individual military or civilian operating in cyber work roles in terms of whether you are a coder, a cyber defender, et cetera.

So this gets to the blocking and tackling we have been doing over the past couple of years to get our arms around the totality of our cyber workforce. So, I will take that for the record to ensure I am being correct on this, sir. But the cyber operators that are working for CYBERCOM [U.S. Cyber Command] and elsewhere included in our broader Cyber Workforce framework that we have put together to allow us to get the fidelity we need on these occupational series, and the work roles so we can look all the way across the dozens of work roles with the fidelity we need to be able to characterize the tens of thousands of individuals we have in this area, sir.

[The information referred to can be found in the Appendix on page 45.]

Mr. LANGEVIN. And last question I have—and then I am going to yield to the ranking member, and hopefully, we will get a second round in, too—but do the efforts that your statement describe extend to the cyber mission force, and/or the cyber operation forces?

And will the cyberspace operations forces have dedicated elements for OT cybersecurity?

Mr. SHERMAN. Sir, I want to take that one for the record and make sure I give you the right answer on that. I would see the IOT, the industrial control system, absolutely involving our CYBERCOM colleagues on this, but in terms of how we are going to structure this, it is frankly early in the movie on this, and I want to make sure I get the right answer for you on that, sir. But this a priority for me, especially post-Colonial Pipeline. This was a wake-up call. And again, the Department has been on this, but what can be done to ICS? I want to ensure we are putting all the piece parts to this together. So I will need to take that one for the record as well, sir.

[The information referred to can be found in the Appendix on page 45.]

Mr. LANGEVIN. We look forward to getting the follow-up from you for the record.

With that, I am going to hold there and yield to the ranking member.

Mr. FRANKLIN. Thank you, Mr. Chairman.

Mr. Sherman, it is my understanding that the Department of Defense allows unpatched software to remain on the network for 120 days before being removed. When our adversaries are increasingly looking to attack us from the cyber domain, can you highlight what the Department's doing to reduce this timeframe, and make sure our systems are not vulnerable? And then part two of that, do you have the authorities necessary to require the services and components to act?

Mr. SHERMAN. Thank you, sir. I believe we do absolutely have the authorities we need on this. And this gets into the broader cybersecurity push we have. Looking at things like our risk management framework, the standards we have about how long software can remain on our network, and, indeed, one of my absolute main priorities is we move to a Zero Trust architecture getting after things like unpatched software, but also, an overall holistic approach to how we structure our networks and making it assume that the bad guys are going to get on there, and how do we segment things, ensure it is patched as quickly as possible, and have the very best tools and approach on this. So sir, this is something 120 days is probably too long. We would need to take a look at that, but this gets to the broader push.

I've also got the CISA [Cybersecurity and Infrastructure Security Agency] working on to how can we do this better to ensure as we look at peer competitors and non-state actors that know they are coming at this, that that is not what we want to be able maintain there, sir. So we will be looking at that.

Mr. FRANKLIN. Very good.

In your testimony you state that not all priorities can be satisfied in each budget. That is pretty much a standard for all the different departments that come before us. But can you highlight what is not being satisfied in the President's budget? And what risks are there associated with those unfunded priorities?

Mr. SHERMAN. Well, sir, I would say the main priorities are all being answered in the President's budget. We do have some risk areas that bother me, though, as CIO. And these have been enduring and I think my predecessors would have said the same thing. You mentioned about the software patching, that is something immediately on our networks. Working with our colleagues in Acquisition and Sustainment, I really want to put our shoulder in to weapon systems, and critical infrastructure, recognizing that our adversaries are going to be coming after those, too, and moving just beyond the Department of Defense Information Network under my charge, but looking again at weapon systems and elsewhere where we can work with General Nakasone's team at CYBERCOM, work with A&S [Under Secretary of Defense for Acquisition and Sustainment]. And those are some risk areas that because some of these programs were started in the 1990s when cybersecurity was in a different place, we have a better way to come at this. That is the type of area, sir, where I think we are carrying some risk that I want to do a better job of working with our colleagues in the Department.

Mr. FRANKLIN. Okay.

And one final question for this round. Recent cyber attacks, such as those on the Colonial Pipeline and water treatment facility back in my home State of Florida, have highlighted that critical infrastructure and utilities are becoming more integrated with traditional IT networks, and therefore, can be more exposed to cyber risks. How could the DOD's mission be impacted by such attacks on critical infrastructure and utility operations technology? And what are the Department's plans to ensure an adequate level of protection to those assets that is commensurate with the risk?

Mr. SHERMAN. Yes, sir. That gets exactly to what I was mentioning with the chairman's question on this as well. ICS, industrial control systems, operational technology, and we will get the terminology all right on this, but exactly what you are talking about, a cyber attack not necessarily launched on our networks, but against our water supply, our heating and cooling, on a data center somewhere that could be the same as a kinetic kill on something, and shutting the water off for cooling. Any number of things that affect our operations on our installations.

What I didn't appreciate until I got into this job was there could be seams we need to address. And so again this is one of our priorities is I am having our team do a close look at what policies we have in place. Is it directive enough? Is it suggestive? And we need to roll in harder on this? What I don't want to have happen is any seams between the outfield so to speak, between facilities, cybersecurity, and elsewhere, where our adversaries could find a gap and get after us and hurt our facilities in the NCR [National Capital Region], or one of our installations, or overseas, or our warfighting ability. So this is a priority, sir, and it is in progress as we are looking at this. And again, as recently as this week, we have been working on this.

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

Mr. LANGEVIN. Thank you, Mr. Franklin.

Mr. Larsen is now recognized for 5 minutes.

Mr. LARSEN. Thank you, Mr. Chair.

Mr. Sherman, it is good to see you. In your testimony, on page 10, you—on page 9 and 10, you discuss 5G; in particular, that, I think you say that the Department's ready to make available 3.45 to 3.65, but you have concerns about the 3.1 to 3.45. Is this a setting in which you can explain some of your concerns about the mission operational impact on the 3.1 to 3.45?

Mr. SHERMAN. Yes, sir. At a high level, so the 3.45 to 3.65 are areas we have actually been able to vacate, or are in the process of vacating. The other one, the 3.1 and up to 3.45, this other band has quite a bit of DOD activity in it in the continental United States and our territories for radars and other capabilities that are used for training, as well as real-world operations, homeland security, and so on. Whereas we have been able to vacate, or in the process of outright vacating those other bands, this one is going to be trickier, where we're gonna need to learn and be able share that, where we can have some sort of relationship if this becomes available working with the FCC [Federal Communications Commission] and Commerce, NTIA [National Telecommunications and Information Administration] to where—I will give you an example of the kind of vision we have on this, would be, say, an *Aegis*-class cruiser down in Norfolk needs to be able to bring up their very powerful radar, but not every day, maybe certain days of the months. But when that illuminates, it can go well into the Tidewater region, as I understand it.

Well, hopefully, we are able to walk and chew gum where we can work out arrangements where on those days that cruiser has to bring the radar up, there could be some sort of sharing of that spectrum. That is what I am getting at with that band, that 3.1 to 3.45, recognizing there is a lot. And I just used a naval example. There are plenty of others that operate in that space, where our soldiers, sailors, airmen, Marines, and guardians have to be able to operate in that space. And again, some of this is for real-world operational activity, AWACS [Airborne Warning and Control System] is an example.

So that is what we are looking at. We want the U.S. to be a 5G dominant Nation, but we also have to maintain these DOD operational needs. But we think we can work this out and that is what we are looking at in that band, sir.

Mr. LARSEN. You might know, we have been trying to help you all work that out as well. It has been fits and starts a little bit.

So can you discuss, does CIO have a role and what would you assess the progress of the 5G pilot projects? You don't have to go through all 12, but do you have general thoughts right now?

Mr. SHERMAN. Yes, sir. We absolutely have a role. So we work with our Research and Engineering colleagues, USD R&E [Under Secretary of Defense for Research and Engineering], they have the lead. We work it from the CIO side with the standards piece, working it closely with them. And working it—I don't want to say at a more strategic level, but there is a very close partnership where they are working directly with the services. And, sir, you are aware of all 12.

Mr. LARSEN. Yeah.

Mr. SHERMAN. Logistics, and healthcare, and aircraft maintenance, and everything else. Well, we are working the standards piece and working with the higher level interlocutors at FCC, and Commerce, and elsewhere. So it is a very good coupling between their leadership, working with the stakeholders on the pilots, and us working it from a CIO standards, policies—I don't want to say oversight yet, but that piece of it, so we do have a very close part.

Mr. LARSEN. When those are done or when there is some assessment, I would note in your testimony, it said, CIO gets those in 2024. So will you—will the CIO office be taking the operational role at some point?

Mr. SHERMAN. I think we need to define exactly what that means, sir. But yes, I think we are going to have that, as mentioned in my written submission. And by 2024 and what does that look like? And as our colleagues in R&E move on to 6G, and Next G, and keep leading us in that direction to stay ahead of our adversaries. So, yes, sir. I see us as having the overall baton, but to be honest, we have to define exactly what that is going to look like.

Mr. LARSEN. But that makes a broader assumption as well that CIO will be, for lack of a better term, you will be the repository for 5G, not military operations, but you will be the keeper of 5G for the Department once we are using it.

Mr. SHERMAN. Yes, sir. That is based on that assumption, subject to administration and departmental guidance and legislation from you all, sir.

Mr. LARSEN. Yeah. That is great.

I only have 20 seconds, so I will ask the question, but we may be able to come back. So I will give you a heads-up. It is a question about the JAIC [Joint Artificial Intelligence Center], and specifically the AI [artificial intelligence] education strategy that was part of the 2020 NDAA [National Defense Authorization Act]. So if you have an update on that. And specifically on that as well, any information on the DOD's—your perspective on the National Security Commission on AI and identification to be AI-ready by 2025 and will we be ready?

With that, I will yield back. And you can chew on that while we work through the first round.

Thank you, Mr. Chair.

Mr. LANGEVIN. Thank you, Mr. Larsen.

Mr. Moore is recognized for 5 minutes.

Mr. MOORE. Thank you, Chairman. Thank you all for being here.

The intelligence community through its commercial cloud enterprise initiative recently moved away from its previous approach of utilizing one cloud provider, and has, instead, adopted a new approach to cloud computing. Generally, I am in favor of increasing competition and innovation. I believe this ensures access to the latest emerging technologies and the benefit of price competition, as well as the ability to procure services based on specific workload. And the needs with that.

I am interested in learning how the Pentagon has approached cloud computing in order to maximize the benefits of competition, while balancing the needs of managing highly sensitive, often classified, DOD materials. So my question to Mr. Sherman, the Pentagon's $10 billion JEDI [Joint Enterprise Defense Infrastructure] program has been in ongoing yearslong litigation. One of the key objectives for the JEDI contract is to move at the speed of relevance to support the delivery in sharing information real-time for our Nation's warfighters, but with years of delays that has still not happened. I know that JEDI is in litigation, and your comments may be short on specifics, but can you speak generally about how the Office of CIO is approaching cloud currently? And what plans are in place or being made for the Department for future cloud services?

Mr. SHERMAN. Yes, sir. So, starting with cloud writ large, we went from a situation where we had maybe almost a 1,000 flowers blooming, to really starting to consolidate down where we have roughly a dozen as we would call them fit-for-purpose clouds. You have heard of some of them: milCloud 2.0, the Air Force's Cloud One, the new cloud Army, cARMY as they call it, and I can go into some others, where we are using those as platforms for software development for some of the AI activity at the unclassified and secret level, in some cases. Some are on premises, some are off premises. But this gets into that in my opening statement about the cloud conversancy in the Department moving from a capital expenditure or CapEx model, to where we maintain all the infrastructure and all the hardware to an OpEx or an operations expenditure model which we would use a cloud setting. So it is not only having the software development, the DevSecOps, workloads, but learning how to live and operate in a cloud environment. And that we have done. So we have been able to work on that across the services, across the enterprise, and with the Defense agencies and field activities.

To your point, we still also have an urgent unmet need for an enterprise cloud capability at all three security levels—unclassified, secret, and top secret—that extends all the way from headquarters all the way to the tactical edge. And that has not gone away at this time.

And as Deputy Secretary Hicks made some recent public statements, we are continuing to assess our next steps vis-a-vis, the what comes next or what should we be doing with that enterprise cloud urgent and unmet need. And that is where we are now on the cloud and we will be pending your further questions.

Mr. MOORE. Would leveraging public-private partnerships help in that regard? Given the fact that a healthy majority of cyber infrastructure in this country is owned by the private industry, do you see an opportunity to leverage that with those particular challenges and moving forward?

Mr. SHERMAN. I think some of the main challenges—and we do obviously want to work very closely with our industry partners on their best capabilities, gets into the cybersecurity realm as we move from different impact levels as we call from IL, or Impact Level 2, which is what we just did on that commercial virtual remote, that COVID-era remote work capability up now to what we call DOD 365 to get onto an Impact Level 5 enclave that in this case Microsoft helped set up for us in different tenants of which we have 13 of them. So, sir, a lot of that—we appreciate the public-private partnership, but for the Department of Defense and for our mission, cybersecurity is going to be paramount in that discussion.

Mr. MOORE. Yeah. And I would agree with that. I mean, it started—the questioning—we are talking about the intelligence community, and absolutely respect that.

I look at our Space Force, right? And how our Space Force is able to leverage so much from the private sector, just thinking about how we can create more efficiencies and leverage it. Obviously, paramount is the classification and ability to do that.

So with 20 seconds left, I will yield back. And thank you very much.

Mr. SHERMAN. Yes, sir.

Mr. LANGEVIN. Thank you, Mr. Moore.

Ms. Houlahan is now recognized for 5 minutes.

Ms. HOULAHAN. Thank you, Mr. Chair. And I just would like to say I find this testimony riveting. And, so, I appreciate the conversation. And I am glad to be here to ask you questions.

I guess my first question has do with a letter that I recently sent to Secretary Austin with several of my colleagues, and asked the DOD to implement a mandatory training on digital literacy and cyber citizenship within the DOD. The proposed defense budget would set aside $30.8 million to help the Pentagon improve tools to identify and address extremism amongst troops and to enhance training at all levels. It also included $9.1 million to take initial steps to fight extremism and insider threats.

I was wondering if you might be able to share a little bit of detail on what sort of tools there would be possibly, and trainings there would be possibly, and what they might look like?

Mr. SHERMAN. For digital literacy, ma'am ——

Ms. HOULAHAN. Yes, sir.

Mr. SHERMAN [continuing]. Or countering extremists specifically?

Ms. HOULAHAN. Digital literacy. The idea here, sir, is that we need to make sure that everybody has understanding of how to assess truth. And literacy is a set of skills that is not just reading, but it is also numeracy, it is financial literacy. It is also just kind of civics engagement and understanding how to understand when you are being not told the truth. And so, the digital literacy would be for our troops in that area.

Mr. SHERMAN. Ma'am, at a high level, I will say I know there are training opportunities all across the enterprise in terms specifically for those operating. And, ma'am, I know you have got a lot of experience of this from Hanscom [Air Force Base] and elsewhere for those operating in the digital space. But in terms, I would like to take this for the record to give you a holistic answer. Because I am going to be honest with you, I haven't had a chance to drill down on exactly how much we have for the—everybody's digital, of course, but if I am not working in the information technology or cybersecurity, and if I'm in operations let's say, which I think is what your letter is getting at, I would like to get back to you and take a look at that and see exactly what we have on the shelf and what we can do to expand what you are getting at to beyond the standard, computer-based training on things like avoiding cybersecurity threats.

Ms. HOULAHAN. Sure.

Mr. SHERMAN. But avoiding or doing the right thing. So, ma'am, I would like to take that for the record and come back to you with that.

[The information referred to can be found in the Appendix on page 45.]

Ms. HOULAHAN. No. I appreciate that. And I would love to follow up with you on that.

My next question is about investment in STEM [science, technology, engineering and mathematics] to make sure that we have competitive cyber professionals that are able to meet our Nation's workforce demands. And so, I am really interested in your Cyber Excepted Service. At the hearing in April before the Senate Armed Services personnel committee, the Acting Secretary for Defense for civilian personnel testified that cyber exceptional service was important and that authorities have been able to enhance recruitment of cyber professionals. He pointed to the flexibility in compensation and classification of work requirements as examples of how this program has been able to better meet targeted cyber needs.

We also received testimony in the subcommittee from the U.S. CYBERCOM commander that the mission and the opportunity to work with colleagues of such caliber provides the most unique and important competitive advantage than compensation when competing with the commercial industry.

So, I would like to hear your take on what it is—what is and what isn't working with Cyber Excepted Service from an IT perspective, rather than from a personnel perspective. Do you agree with the assessments that we have heard previously? What would you like Congress to know about what is and what isn't working as we continue to examine these and other authorities to meet the DOD's cyber needs?

Mr. SHERMAN. I think at a higher level I think CES [Cyber Excepted Service] is working well. I think, and as I put in my written testimony, we got about 9,000 civilian positions that it could apply to, and we have got about 6,500 that have been converted. This has been, as us at an enterprise level, learning how to use this capability to the best advantage, getting it out there to the different services and components on how to use it. And also, as we use the targeted local market supplement, TLMS, to the best advantage, and the other capabilities that CES provides us for expedited hiring, and benefits, and so on to get that talent in the door.

I would say this really does have to be nested in a broader cyber workforce strategy, which I have actually launched, and we aim to publish early next year on what is it we are trying to do with CES and all these other tools in our toolkit here, and to increase the diversity, the capability, the conversancy of our workforce for the 21st century threats. And also leveraging back to the STEM training, things like the NSA [National Security Agency] scholarship program they have, and being able to fit that in, and also the accreditation they have for institutions around the country from junior colleges up to 4-year institutions. So what I saw lacking was we didn't have one place, we had a little bit in our cyber strategy. We need a cyber workforce strategy. And as a matter of fact, I chaired the first—I need to make sure I get this right—the CWMB, the Cyber Workforce Management Board. We hadn't held one in a year. I said we need to hold one, which I co-chair with personnel resources and PCA [principal cyber advisor] to be able to start to look as these hard problems that you are getting at, ma'am, with CES and some of these other talent issues we have got to get right.

Ms. HOULAHAN. I know my time has expired, and I yield back. Thank you.

Mr. LANGEVIN. Thank you, Ms. Houlahan.

Before we go to the second round, is there any member who has not asked a question in the first round that wants to ask a question? Any of our members remotely? Okay.

Hearing none, we are going to move to the second round. And I will recognize myself for the first round of second questions.

So out of the 17 unfunded priority lists submitted by DOD components and commands, there are a total of $1.2 billion in IT-related requests. Obviously, no small number. As the DOD is officially responsible for compiling and certifying the Department's IT and cyberspace activities budget, what does it say that the various components have identified IT and cyber requirements may judge to be critical, but do not prioritize them enough in the normal budget process to make sure that they are in the President's budget?

Mr. SHERMAN. So as a CIO, this is an ongoing thing we need to always be looking at. We have certified the budget as required for sufficiency to ensure that as we look at our digital modernization priorities, that the components submitting, the services and so on, have funded sufficiently to reach that, as well as within the submitted budget, the increase roughly I think 5 or so percent since last year we have seen an in—our submitted increase to get after what we need to get to. But to your point about UFR [unfunded requirements], sir, being able to be have the governance to work with them to ensure that this is being submitted properly and not outside of what we are certifying is something I will continue to focus on as CIO to ensure we can get this right. But I feel that we have certified a good budget, that we have what we need to cover down on digital modernization priorities. And we will continue to watch this closely with our component colleagues.

Mr. LANGEVIN. So I have consistently advocated for more dedicated senior leadership and focus for electromagnetic spectrum operations at the Department. Mr. Sherman, in your written testimony, you wrote that the CIO has been assigned and designated as senior official for long-term implementation of the 2020 spectrum superiority strategy. When will this implementation plan be released? And how do you intend to carry it out? And why would this plan be successful while others have fallen short?

Mr. SHERMAN. So on the question, we expect the implementation plan to be signed very soon by the Secretary. I don't have an exact date. But we have got this teed up, ready to go. And in terms of why it will be successful, the commitment from the Department, from the Joint Chiefs to the OSD [Office of the Secretary of Defense] side, in recognizing that we have got to get this right in a near-peer competitor environment, not that we haven't been focusing on this during the wars in Afghanistan and Iraq, but as we look at China, and Russia, and other adversaries in that regard, electromagnetic spectrum is going to be critical, just as critical as kinetic long-range fires, space, cyberspace, and so on. We've got to be successful.

So the commitment from the Chairman, the Vice Chairman, Secretary, Deputy Secretary, and everybody has been very strong. So we are confident that we are going to have what we need.

And back, I think, to your middle question, sir, we are the main overseeing official for this. The Vice Chairman through the Joint Staff is leading a CFT [cross-functional team], a functional team working on this. And come start of fiscal year 2022, we are going to take the baton as the implementing office for this.

So we are the overall lead responsible official for the Department, Joint Staff is working the CFT and we are ready to pick that up. And sir, I feel we have the commitment on this across the services and the seriousness recognizing the threats we face right now.

Mr. LANGEVIN. Very good. Thank you, Mr. Chairman.

With that, since Ms. Bice has not asked a question yet, I will yield to Ms. Bice for 5 minutes.

Mrs. BICE. Thank you so much, Mr. Chairman, for holding this important hearing today. Mr. Sherman, thank you for being here.

The DOD's cloud strategy calls for three clouds: milCloud 2.0, a secure premise cloud; the Defense Enterprise [Office] Solution, cloud-based secure collaboration solution; and the JEDI, general purpose cloud. Fourth Estate agencies were directed to move to the milCloud 2.0, but adoption has been incredibly slow. Today, only 3 percent of the targeted workloads have migrated to the milCloud. This has delayed realization of enhanced security, which is paramount in light of the most recent Colonial Pipeline and Solar Winds cybersecurity attacks.

A little bit back of background. I come from a family business that has dealt in the technology space. And I recognize the critical need for us to protect our assets, especially in the cyberspace. Will the DOD enforce the 2018 mandate directing milCloud 2.0 migration by the Fourth Estate?

Mr. SHERMAN. We are going to ensure that it is being used where it can be used and ensuring that the DAFAs, the Defense agencies and field activities, that need the on-prem capability that it provides are going to use it.

In terms of what was directed in 2018, I am frankly, from my seat, going to take a more nuanced approach on this. MilCloud 2.0 is a powerful capability on-prem. To your point, it operates at IL 5. It is not yet accredited at IL 6 secret. And roughly 25 percent of the DAFA migrations that have occurred from legacy to cloud-based solutions have gone to milCloud 2.0. It is a powerful arrow in our quiver, but not the only one. And, so, that is the approach I am taking on this. It is definitely a good capability to have, but it is not our only capability. And so, that is how I am approaching this, ma'am.

Mrs. BICE. If I may follow up. So you are suggesting that only 25 percent has migrated to milCloud. What is the other 75 percent doing?

Mr. SHERMAN. They are going to other cloud-based capabilities. Amazon, Microsoft, and DISA [Defense Information Systems Agency] provided cloud capabilities to get off of legacy platforms.

Mrs. BICE. Do you feel like the migrating to those particular platforms provides a security that you feel comfortable with?

Mr. SHERMAN. Yes, ma'am, It does.

Mrs. BICE. A follow-up question to that, if I can. Our adversaries have made it known that they plan to use artificial intelligence to gain a competitive advantage in cyberspace. What is the DOD doing to match and exceed any capabilities our adversaries might develop in this space to defend our assets, and ensure DOD can effectively carry out its mission? What keeps you up at night?

Mr. SHERMAN. What keeps me up at night are cyber threats of the kind we are seeing across the country, not only against the government, but against the private sector. This is the main reason I am so committed to moving out with the Zero Trust implementation at the Department of Defense. I want DOD to be a leader in this space.

Zero Trust has been bandied about for years. Some in the private sector may have achieved this at some level, but no department has at the level I am suggesting. With an assumption that the adversary is on the network, we must segment in a way we never have before. Instrument the network in a way we haven't, and using things like identity credentials access management, endpoint security, comply to connect. And it is not one thing you buy, but a host of capabilities. I know what the Chinese and Russians want to do to our networks and this is the most important role I have as CIO, along with our types of modernization for our warfighters, keeping our networks safe.

I have often noted that right now, the offensive side has all the capability. And we on the defensive side have got to run a new defense, to use one of my football terms. We are going to run a new defense. That is what keeps me up. And it is going to involve making it about the data in the systems as well as, ma'am, artificial intelligence, how we can bring that to bear, so we don't segment ourselves and have to have tens of thousands of defenders doing the work that a set of AI algorithms can do. So that is going to be part of Zero Trust as well.

Mrs. BICE. Mr. Sherman, I appreciate your answer.

One of the concerns I have, however, is looking at, as a freshman legislator, I am probably bringing a different perspective, the time that it is taking to actually get these services migrated to either cloud-based solutions or other that can protect our assets. We talked about milCloud 2.0 being implemented in 2018, and here we are 3 years later with a very small percentage that have been migrated. How can we effectively speed things up in a way that will make sure that we are doing it in a thoughtful way but we are also protecting our assets?

Mr. SHERMAN. Ma'am, I would just add, of the Defense agencies and field activities, the first 14 of them, in our first tranche, we moved 97 percent of their applications off legacy to cloud of the four areas I talked about, as well as the services have made great progress, shut down legacy data centers, and got to manage services like cloud. We are moving aggressively in this direction, recognizing the vulnerability of legacy to cybersecurity threats. So we appreciate your comments on that, ma'am.

Mrs. BICE. Thank you.

Mr. Chairman, I yield back.

Mr. LANGEVIN. Thank you, Mrs. Bice.

Mr. Larsen is now recognized for 5 minutes.

Mr. LARSEN. Thank you, Mr. Chairman. Mr. Sherman, thanks for sticking around for my second round of questions. I appreciate it.

I had a question regarding, first off, section 256 of the fiscal year 2020 NDAA, which required the DOD to develop an AI education strategy. And JAIC is responsible for that effort. Do you have an update on that?

Mr. SHERMAN. Sir, I am going to have to take this for the record. As the JAIC no longer reports to me directly, they are close colleagues.

We work hand in glove with them. But some of their specific initiatives, sir, I wouldn't feel comfortable articulating. I would defer that to General Groen and the JAIC leadership. So I would like to take that for the record to give you an accurate answer back on that, sir.

[The information referred to can be found in the Appendix on page 46.]

Mr. LARSEN. That is fine.

And then to follow up on some AI. I mentioned earlier, I asked if the DOD CIO had perspective on whether or not we are AI-ready. The National Security Commission on AI has a variety of goals, including to be AI-ready by 2025. Do you think the Department will be AI-ready by 2025?

Mr. SHERMAN. Yes, sir. I think holistically we are doing the right things to be AI-ready. We talked about cloud a little bit here in terms of what we have for cloud to host AI capabilities and algorithms. The cybersecurity pieces I have talked about with Zero Trust are going to be critical for artificial intelligence. I will come back to our urgent and unmet need for an enterprise-wide cloud capability from headquarters to the tactical edge. That is going to be important for AI, and it will go to what Deputy Secretary Hicks announced last week with the AI and Data Accelerator initiative, or AIDA, as we are calling it, to be able walk across combatant commands, and unlock the power of AI for the COCOMs [combatant commands] as well, using cloud-based technology. So I think we are leaning in the right direct, but we have with got some work to do.

Mr. LARSEN. So on that point, though, then who is responsible, for lack of a better term, educating the COCOMs on the use of algorithms for purposes they define?

Mr. SHERMAN. I think this is exactly the AIDA initiative that Deputy Secretary Hicks announced with these AI teams that will be going to the COCOMs, as well as data teams, ODTs, operational data teams, working together on both the data side and the AI side, starting at places like NORTHCOM [U.S. Northern Command], INDOPACOM [U.S. Indo-Pacific Command], and so on. Getting in there with the users and the various J-code staffs and so on, and working on everything from the algorithm development, building on say what Maven has done, and also on the data side working on thing like Advana [advanced analytics], and what the data capabilities are and merging that together, so these teams that are coming out are going to be a key accelerator for that, sir.

Mr. LARSEN. Yeah. I might have missed it, but maybe I didn't, do you have an update, or are you directly involved with CMMC [Cybersecurity Maturity Model Certification], with the role cybersecurity plays with these smaller suppliers?

Mr. SHERMAN. Sir, only insofar as I had one of my senior executives participate in the CMMC review which was conducted by A&S as a subject matter expert to contribute to that. And then only as CMMC connects to our broader defense industrial base security that we are working through the strategic cybersecurity program. But directly, no, sir. CMMC I am aware of, but not directly leading.

Mr. LARSEN. I understand. We will follow up with other folks on that.

With that, Mr. Chair, I will yield back.

Mr. LANGEVIN. Very good. Thank you, Mr. Larsen.

The ranking member, Mr. Franklin, is going to be recognized.

Mr. FRANKLIN. Thank you, Mr. Chairman.

Two follow-on questions. All of the services who have come before us have talked about the need for more folks trained in the area of cybersecurity. It is a hot job market in the outside private sector. What difficulties are you facing in hiring individuals with the skill sets you need? And what are you doing to address any shortfalls?

Mr. SHERMAN. Sir, I think about this almost every day as I look out my window over at Crystal City, and as I walk out to my truck and look over at Rosslyn and the number of our private sector partners who are competing for some of the very same talent here. This gets to the cybersecurity workforce strategy I spoke about a minute ago. We have got to come at this differently here.

We are using the Cyber Excepted Service as mentioned to get talent in here. We are using things like NSA educational programs to get to the colleges and institutions. We have to broaden the aperture on this, sir. I feel very strongly about this. This is going to take a whole-of-Nation approach. We talk about diversity is critical. And I mean diversity and not only race, gender, but also geographic placement. We can't keep going to the same wells and recruiting in the same places. I want to broaden the aperture of the sort of talent we can bring into the Department of Defense.

We may need to think differently, too, working with our P&R [Under Secretary of Defense for Personnel and Readiness] colleagues about, I am not sure if we want to hire a data scientist for 30 years. Maybe she comes in for 3 or 4 years, gets the skills there, gets the patriotic duty for DOD and returns to the private sector, and then comes back to us in some number of years. We are going to have to work with our colleagues in Intelligence and Security on how we work clearance issues with that.

I am both excited by this, but also daunted, because of the competitive environment in which we live with our private sector colleagues and the whole-of-Nation approach this is going to take to stand up against our adversaries, sir.

Mr. FRANKLIN. One last question. In the physical domain, a commander would be held accountable if he or she lost equipment or mishandled it. To what extent do you believe commanders are held sufficiently accountable for not caring for DOD information and system in their care?

Mr. SHERMAN. Sir, this is an evolving era that we have talked about quite a bit. Part of the issue, and I felt passionately about this myself, if you roll out of a motor pool without proper ammunition, or fuel on your fighting vehicle, or off pushing the ship off the dock, et cetera, you are held accountable for that. Part of it has to get on how we can ensure that there is instrumentation and that the commanders, and the ship drivers, and the maneuver commanders, and others know what is going on on their weapons platform.

So, if there is gonna be accountability with this, we have got to be able to monitor what is actually going on there. And then what does it mean in terms of readiness? So that is an evolving discussion we are having again with our P&R colleagues on this.

But what does cyber accountability mean? But one key thing on this, sir, that I am working to do, and this is an area that I want to inject with here with you all on the legislative side, and industry partners, and elsewhere, we use terms like cyber hygiene, which can make people glaze over. Sir, I know you are a former operator. Sometimes cyber hygiene my people go, Well, that is something for the CIO, or the 6, the J6. I want to use a term called cyber survivability, this is something—as a former Bradley guy myself, this will get my attention, that if I am going to be taken down by this by an adversary, we have got to change how we think about cybersecurity. So sir, these are the kinds of things we are looking at. We need different tools in our tool box working with P&R. And we have brought this up to our leadership and we have some work to do on it, sir.

Mr. FRANKLIN. Thanks. And I agree. From a Navy standpoint, it has just always been known that the captain is ultimately responsible. It doesn't matter if he or she is on the bridge, if the ship goes aground, you are relieved of command. And at some point I think we are going to have to understand that the potential damage from cyber intrusions are going to be just as serious as any of those. But I appreciate your comments there.

I yield back, Mr. Chairman.

Mr. LANGEVIN. Very appropriate comments, too, I would say.

Thank you, Mr. Franklin.

And Ms. Houlahan is now—before I go to Ms. Houlahan, I just want to remind members that as soon as we adjourn here, we will be going up to 2212 for the classified portion of this hearing. So I hope everyone can go up there for the classified portion.

With that, Ms. Houlahan is now recognized for 5 minutes.

Ms. HOULAHAN. Thank you.

My last and final question has to do with our allies. And I had the opportunity to meet with several of their defense attachés. And they were talking about how their nations have implemented effective cybersecurity protocols, or at least what they believe to be effective cybersecurity protocols and managing potential cyber attacks and intrusions. And in their opinion, sometimes better than the United States. Has the DOD sought to work closely with our allies to determine what cybersecurity practices are working for other nations?

Mr. SHERMAN. Absolutely, ma'am. One of things I am privileged to do is work, for example, with our Five Eyes defense CIOs. As a matter of fact, just 2 weeks ago, we would have been meeting in person, but for COVID. But we held a multiday virtual conference going over not only cybersecurity, but how we can work together to modernize. As I work with my colleagues in the Five Eyes, but other nations as well, such as Singapore I had a meeting with recently.

As we talk about things like Zero Trust, there may be different terminologies, but how do we segment networks? How do we instrument things? How do we train our workforce, back to the talent piece? So yes, ma'am, we have robust conversations. And one thing coming from the intelligence side having the privilege to work with allies for many years, we in the United States do a lot of things right, but we have a lot to learn from allies, too. And I value that highly. And many of them are women and men who have great experience in the private sector before they went to their governments. And, so, we do have very active discussions on this area, ma'am.

Ms. HOULAHAN. Has there been discussion in the DOD or with our allies about developing a formal comprehensive approach to cybersecurity or global cyber infrastructure?

Mr. SHERMAN. So some of this would get into probably—in terms of cybersecurity, I don't think that we have talked formally about that. I would also have to defer to General Nakasone through CYBERCOM, some of those channels, what he may be setting up. So I will take that one for the record and make sure we get you a whole answer. But from the CIO side, we do have a lot of engagements, but maybe not quite to the level of a formal structure that you are getting at on that, ma'am.

[The information referred to can be found in the Appendix on page 46.]

Ms. HOULAHAN. Thanks.

And my last question is something that you talked about with kind of the workforce coming in and out, starting with you all as an example, and then going to the private sector and then perhaps looping back around later on mid-career, and you talked about something that is an important part of that, which is clearances.

Can you reflect for a little bit on what does that mean? How do—I am a person who held a TS/SCI clearance decades ago, came back around, and now I am here again, and we have a very different process, which we can talk about later on, how we reestablish those clearances here. But how would that happen? And is there anything congressionally or federally that we can be doing to make that easier for people?

Mr. SHERMAN. Ma'am, I would really have to defer to my colleagues in Intelligence and Security and DCSA [Defense Counterintelligence and Security Agency], but I would just flag, as someone who has worked in intelligence and now seen how this would work, we are going to have to get our head around this. As a person leaves government service, works in a private sector, academic setting, they are necessarily going to have foreign contacts in a globalized—and I know you are well aware of this, ma'am, and when they come back, let's say they want to come back at a higher rank, maybe a slightly different role, we are going to have to figure out how we don't make them wait 12-, 18-plus months. And so I think this is something we need to look at.

And, again, on the cyber workforce strategy, this is something I want to start to put some markers down as really firm requirements for us to think differently because the more we reflect on this, 30-year careers may work for some, but as we look at the digital and cyberspace, this is not going to be best for us, back to as we were talking, from a whole-of-nation approach.

So I don't know if we need anything legislatively just yet, but I think we need to get our head around kind of what the steps of this would look like, ma'am.

Ms. HOULAHAN. Thank you.

And one final comment, I really was interested in the ranking chair's comments about, kind of how we have responsibility to understand what the liabilities are and, frankly, the punishments are for people who are in command and control of cyberspace, so to speak, and I am really intrigued and would look forward to learning more about that with everybody on the committee.

Mr. SHERMAN. Yes, ma'am. And nothing to add on that, but just recognizing cyber accountability, maybe a new term, is something we definitely need to consider the same as poor maintenance or poor training as before a unit pushes out.

So thank you, ma'am.

Ms. HOULAHAN. Thank you. I yield back.

Mr. LANGEVIN. Thank you, Ms. Houlahan.

Mr. Moore is now recognized for 5 minutes.

Mr. Moore is still with us?

Okay. I will hold there. I am going to yield to Ms. Bice for 5 minutes.

Mrs. BICE. Thank you, Mr. Chairman.

And I actually want to really tack on to Representative Houlahan's comments about the clearance process. I think one of the things that we have heard over and over is that it is taking too long, and sort of to that point, when we are talking about recruitment, we often think of sort of the high-tech universities, maybe west coast universities, the Stanfords of the world to go recruit from.

What are you all doing to really look at other institutions of higher learning that have a fantastic program that maybe hadn't been thought of in the past? And I will use a university in Oklahoma. The University of Tulsa has a fantastic cyber program that they are really doing some innovative work in. How are you looking at this from a workforce standpoint?

Mr. SHERMAN. So I will tell you how we are looking from CIO, and I think our P&R colleagues could absolutely amplify this with greater detail. The NSA accreditation—and I don't have the list here in front of me of several hundred institutions, again, from junior colleges, and I would have to look in the State of Oklahoma, ma'am, but I know there is several there, to be able to—and partner institutions together to help bootstrap each other, as some have gotten the accreditation to get the students there, and this is what I really feel strongly about. I come from a rural area myself, La Ward, Texas. You know, everywhere from very rural areas to urban areas, from mainland U.S. to U.S. territories, it is going to take us looking very broadly.

So to your point, that is one thing I am trying to push as CIO through this upcoming workforce strategy. I will say I believe recruitment has expanded over the last several years into these areas, and the NSA accreditation that General Nakasone's team lead has helped, again, anywhere from 2-year junior colleges up to 4-year institutions, major Big 12 or Big Ten schools and SEC [Southeastern Conference], and so on, all across the Nation, to be able to do that. So that is what we are trying to do to broaden the aperture, and also maybe looking at—we do have a new tool we are looking at, kind of matching talent to job positions, looking more broadly beyond just the degree they have, what types of experiences they have, to be able to get folks in there. And this is, of course, something that the private sector, I know you noted, ma'am, is looking very carefully at, too, in terms of what degree requirements does someone really need to be a coder? How do we get them in the door?

So those are the kind of things I am, again, excited and daunted by. But I think if we get this right, this is what is going to give us the advantage on the PRC [People's Republic of China] and others. We have got the talent out there. We just have got to get them in the door.

Mrs. BICE. It is fantastic to hear you talk about that. And Representative Houlahan and I sit on the Supply Chain Task Force that has been talking a lot about workforce and how do we engage various, you know, young people and getting engaged in this that may not be going to a 4-year college, but still have the aptitude to be able to engage in these conversations. So I appreciate your comments on that.

If you could kind of pivot for a just a minute. Can you talk a little bit about how you are coordinating with other government agencies, CISA for example, to really look at a whole-of-government approach in protecting our assets and addressing cybersecurity issues? We have seen all of these intrusions lately. And, so, it is not just DOD that could be impacted, but you have all of these other agencies that are also kind of coordinating. Can you talk a little bit about that?

Mr. SHERMAN. Yes. Well, there is the interagency process. My friend and colleague, Anne Neuberger up at the NSC [National Security Council] is a Deputy National Security Advisor up there and, of course, we have Mr. Inglis is the National Cyber Director. Through their various forums through the National Security Council, and so on, we have the new cyber executive order has been a good thing to help us unify as a government on these things. And, of course, there is other governance fora we have. The Federal CIO has meetings as well as with the Federal CISO [chief information security officer]; and also the kind of informal networks we have with DHS, CISA, with other agencies, and, of course, with where I come from, the intelligence community, governance bodies we have on national security systems, on things like accreditation and looking at policies and practices.

So there is quite a bit—you noted CISA, obviously, close work and they have the .gov and helping secure the Federal side. And then also, we have what we are doing through the Joint Force Headquarters, DODIN, JFHQ–DODIN [Joint Force Headquarters Department of Defense Information Network], that General Skinner leads, has much contact with them. So I think there is robust dialogue back and forth, and best practices. And I do have to say, the cyber EO [executive order] and the focus that we have there has helped us kind of unify around some best practices, everything from Zero Trust supply chain to how we are going to look at these problems, ma'am.

Mrs. BICE. Thank you.

Mr. Chairman, I yield back.

Mr. LANGEVIN. Thank you, Ms. Bice.

That concludes the member questions as I understand it. So with that, the subcommittee will recess, and then we will immediately reconvene in 2212 for the classified portion of this hearing.

The committee stands in recess.

[Whereupon, at 5:09 p.m., the subcommittee proceeded in closed session.]

APPENDIX

JUNE 29, 2021

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

JUNE 29, 2021

Opening Statement for Chairman James R. Langevin
Cyber, Innovative Technologies, & Information Systems Subcommittee
Department of Defense Information Technology, Cybersecurity, and Information Assurance for Fiscal Year 2022
June 29, 2021

The subcommittee will come to order. Welcome to today's hearing on Department of Defense Information Technology (IT), Cybersecurity, and Information Assurance. This is the subcommittee's first hearing on the Department's current IT efforts and the requested investments for Fiscal Year 2022.

Since this subcommittee was formed at the start of the 117th Congress, our members have been eager and encouraged to see the Department of Defense approach its information technologies with a prioritization that has been lacking in the past. Of the many lessons from the pandemic, we have seen clearly that technology can revolutionize how we conduct our business, whether that's in Congress or in the Department of Defense. However, that also requires that the infrastructure which enables our technology is prioritized and secured in a commensurate way.

In my many years in Congress, I have witnessed firsthand the progress that the Department has made in improving the ways in which it can utilize technology. Nevertheless, there is still tremendous work to do. Year after year, we have leaders from across the Department tell us that they consider IT to be a priority, before immediately pivoting to discuss how much funding they need for more flight hours, or more aircraft, or more tanks. I'd like to think that technology will truly be a priority when, for example, the Chief of Naval Operations says that the Navy can live with one less fighter aircraft in favor of greater IT investment.

Through multiple National Defense Authorization Acts, the Congress has judged it prudent to empower the Chief Information Officer in managing the Department's technology portfolio. Today, the CIO is a Senate-confirmed position, has oversight over each of the Services' IT budgets, and manages not only the Department's networks, but also its electro-magnetic spectrum enterprise and command, control, and communications efforts. This places the CIO in a unique operationalized role, contributing to success in the Department's "no-fail" missions.

At the same time, there are still questions about how the Department of Defense defines the roles and responsibilities for cyber matters. If the Secretary of Defense is asked, "who is in charge of buying weapons for the Department?" the answer is unequivocal: it is the Undersecretary of Defense for Acquisition and Sustainment. Conversely, if the Secretary is asked, "who is in charge of keeping DOD networks safe?" the fact that there isn't a single correct answer is troubling. The Secretary could respond with the Chief Information Officer, or the Commander of Cyber Command, or even the Chiefs of the military services, and he wouldn't technically be wrong in any of these responses.

If we can teach every one of our new officers about the criticality of clear command and control, why can't apply this at the highest levels of the Department?

With that as the context, I want to welcome Mr. John Sherman who appears in front of the subcommittee here today. Mr. Sherman serves as the acting Chief Information Officer, and while we have had the pleasure to work together since assuming the role in January, this is his first appearance at a HASC hearing. He is a career member of the Senior Intelligence Service and previously served as Chief Information Officer of the U.S. Intelligence Community.

With that, I'd like to now turn to Mr. Franklin, who is stepping in for Ranking Member Banks. Scott, the floor is yours.

STATEMENT BY

JOHN SHERMAN

DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER, Acting

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS

ON

“ Department of Defense Information Technology, Cybersecurity, and Information Assurance for Fiscal Year 2022”

JUNE 29, 2021

NOT FOR PUBLICATION UNTIL

RELEASED BY THE HOUSE ARMED SERVICES COMMITTEE

Introduction

Good afternoon Mr. Chairman, Ranking Member, and distinguished Members of the Subcommittee. Thank you for this opportunity to testify before the Subcommittee today on the current efforts underway pertaining to the Department's information technology (IT) and cybersecurity. I am John Sherman, the Acting, Department of Defense (DoD) Chief Information Officer (CIO).

As you know, the DoD CIO serves as the principal advisor to the Secretary of Defense for information management; IT; cybersecurity; communications; positioning, navigation, and timing (PNT); spectrum management; senior leadership communications; and command, control, and communications (C3) matters. This portfolio is unlike that of most CIOs in both scope and scale. During this time of transition, we have made it a priority to maintain the momentum in transforming the foundations of the Department's digital capabilities, while innovating at scale to bring new initiatives, such as Zero Trust (ZT) and DevSecOps, into wide scale use across the Department. This is essential to support both our forward deployed forces and global capabilities that our nation's adversaries have shown the will and capability to target. These efforts are focused by the President's Interim National Security Strategic Guidance and the Secretary's Message to the Force priorities memo.

The DoD CIO coordinates on a daily basis directly with the DoD Principal Cyber Advisor (PCA), U.S. Cyber Command, the Joint Staff J6 counterparts at the Military Departments (MILDEP), and various Defense Agencies and Field Activities (DAFA) at leadership and staff levels. Additionally, the CIO holds a bi-weekly meeting of MILDEP CIO principals to coordinate initiatives, and a monthly meeting of DAFA CIO principals to achieve the same goal.

The DoD CIO annual budget review and certification authority, in accordance with section 142 of Title 10, United States Code, as amended by the National Defense Authorization Act for Fiscal Year 2018, provides a critical avenue for a more strategic and methodical approach to prioritize resources toward capability requirements within the areas I am responsible for. To ensure a clear, manageable and repeatable scope for the review of the proposed DoD budget, my office issues annual programming guidance to the DoD Components identifying the investments of focus for the CIO assessment of their fiscal year budget, consistent with the National Defense Strategy and Defense Planning Guidance, for strengthening and accelerating the modernization of the Department's IT and Cybersecurity digital capabilities. Components are asked to build their budgets consistent with the CIO guidance, and as part of the Department's broader budget guidance and deliberations. My office assesses their budget submissions against our priorities and the guidance. DoD CIO has successfully completed three fiscal year budget assessments and determinations beginning with the FY 2020 President's Budget. The Department is making consistent progress toward increasing the focus and priority toward transforming the foundations of the Department's digital capabilities, which I will discuss in more detail today. I recognize that not all priorities can be satisfied in each budget, so part of the certification process is to identify areas where the budget is adequate but still present some risk to transforming the Department's digital capabilities. Focus for future budget certifications will continue to be these modernization efforts, working with the Military Departments and other DoD Components to address areas of concern in future budgets.

The DoD FY 2022 Information Technology/Cyberspace Activities (IT/CA) Budget Request is $50.6B, including $12B in cyber/ classified IT/CA investments and $38.6B in unclassified IT investments. The FY 2022 request reflects an overall 4% increase from the DoD FY 2021 enacted IT/CA Budget.

Today I would like to speak to you on a number of critical initiatives that exemplify the key elements of the Department's effort to transform and innovate in support of the warfighter globally. First, I'd like to discuss our activities in the areas of cloud computing, software modernization and network optimization. Second, I'll provide a brief assessment of our cybersecurity posture and discuss key initiatives including ZT, the Strategic Cybersecurity Program (SCP), Risk Management Framework (RMF), and Industrial Control Systems (ICS). I will provide an update to earlier testimony on initiatives related to the Department's Cyber Workforce as well. Then I'd like to discuss critical initiatives in the Department's ongoing effort to develop a more resilient PNT capability to support warfighting in degraded environments, spectrum sharing, our work on 5G, and updates to leadership communications. Finally, I'd like to provide you a brief overview of the actions underway to make data a strategic asset and increase its availability for leaders across the Department, from the boardroom to the battlefield.

Cloud-Enabled Warfighting

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

The Department continues its commitment to cloud computing with the $1.48 billion total FY22 budget representing a 10% increase in cloud investments from the prior year. This growth includes continued investment in cloud services (infrastructure, platform, and software), application and system migrations, and additional cybersecurity measures to protect DoD data in the cloud. Progress includes DAFA cloud and data center optimization reform with 90% of planned migrations and closures expected by 4QFY21 and the remaining to complete in FY22 for a total of 926 systems migrated or decommissioned and 42 data centers closed. While making progress, work remains to drive accelerated modernization and adoption. In addition to the 10% growth in the FY22 budget, the Department continues to require double-digit growth in the future years to maintain this momentum.

The Department remains committed in its drive toward a multi-vendor, multi-cloud ecosystem with FY22 cloud investments representing over 50 different commercial vendors, including commercial cloud service providers, and system integrators. With the ongoing delays associated with the JEDI enterprise cloud contract acquisition, optimizing the Department's cloud acquisitions remains challenging. However, centralized cloud contracts issued by MILDEPs and the enterprise-level milCloud 2.0 contract help fill the gaps and provide a more streamlined and cost-effective approach to DoD cloud adoption.

Software Modernization

The Department continues to learn from its modernization efforts and to gain a better understanding of the IT requirements for the future battlespace. Based on this understanding, the Department is focused on Software Modernization, an initiative that builds upon cloud with the vision of delivering resilient software capability at the speed of relevance. Extending the cloud with capabilities such as DevSecOps and enterprise services, and incorporating a focus on delivering cyber resilient systems, Software Modernization provides for the full integration of technology, process, and people needed to deliver next-generation capabilities.

The FY22 budget includes investments to enable Software Modernization with cloud services as the foundation. As one example, the Air Force's Platform One provides multi-tenant capabilities to critical weapon and business systems that include the F-35 fighter, the Advanced Battle Management System, and the B-21 bomber. Platform One's latest demonstration was the edge deployment of Artificial Intelligence/Machine Learning (AI/ML) capability to the U-2 reconnaissance aircraft in just 12 days. The Department will continue to place emphasis on Software Modernization with the publication of a strategy later this summer, building on DoD DevSecOps guidance already developed and early implementation success of that guidance by the Military Departments.

Network Modernization

Today's joint warfighter requires a globally-accessible and adaptable network infrastructure that provides resilient data transport in real-time across Service, operational domain, and security classification boundaries to joint, allied, and other mission partners. We must have the ability to rapidly collect, analyze, and share information from multiple tactical, operational and strategic locations and make decisions in real time.

In response to the COVID-19 pandemic crisis, the Department rapidly deployed Commercial Virtual Remote (CVR) a commercial based collaboration capability to enable the remote work force and lessen the demands on the Department's networks. CVR, intended as an interim measure until a more secure and enduring platform was deployed, was decommissioned on June 15. The Department recently implemented DoD365, a platform that represents a more secure collaboration environment and more comprehensive integrated suite of office productivity tools (Email and MS Office). The DoD365 planning and deployment efforts were led by the DoD CIO and CDR, USCYBERCOM. Informed by limited deployment and cybersecurity testing, the initial capability provides users with Direct Internet Access through a Web Browser into the DoD365 environment. The intent is to increase capability over the next 12 months with Components developing and testing solutions to deliver managed and unmanaged Bring Your Own Approved Device with internet based access to DoD365. To date, the initial deployment of DoD365 has reached nearly ~2.2 m users of the targeted ~2.8m user base.

Cloud access and remote work introduces a significant burden to the DoD networks. To counter that demand, DoD365 enables Direct Internet Access through a web browser now and is working to incrementally deliver direct internet access on managed and unmanaged mobile and desktop devices. During the COVID-19 pandemic the Department was able to sustain day to day operations by greatly expanding the VPN capacity and by providing a large number of additional VPN services.

Additional modernization efforts underway or planned will reduce the number of network connections needed at any given Base/Post/Camp/Station by optimizing to an all-Internet Protocol (IP) infrastructure that can be virtualized for specific mission needs and cybersecurity protection. The Department's network modernization efforts will deliver greatly enhanced bandwidth capacity and increase network resiliency to enable advanced warfighting initiatives. It will also support the use of DoD-wide services and consolidation of critical IT systems, applications, and services from local installations to core data centers and the DoD enterprise cloud environment. To this end, the Department is conducting experiments with industry partners to determine how they can help DoD enhance the resilience and performance of its IT infrastructure. These experiments will also identify ways to improve base and wide-area connectivity required to meet the increased network demands resulting from operations in the Commercial Cloud.

Tomorrow's war fighter will require the ability to collect and fuse information in new ways and make that information available instantaneously across geographically-separated forces spanning the strategic to tactical levels of combat. In spite of the enterprise infrastructure successes, more needs to be done to eliminate vulnerable network systems, implement mandated Internet Protocol version 6 (IPv6) capabilities for next generation network management, and establish resilient, high speed capabilities to support Joint All Domain Command and Control (JADC2) and cloud access at DoD locations.

The Department's many network modernization efforts will provide the ability to fully harness the cloud and compute capabilities, as well as establish an efficient and effective information technology environment.

Cybersecurity

The cybersecurity posture of the Department is a complex quantity to assess. The Department of Defense Information Network (DoDIN) is a massive infrastructure supporting multifarious missions each having a range of threat actors, and consequences of failure. At the same time both the technologies comprising the DODIN and the capabilities of threat actors is evolving at an ever increasing rate.

In this complex and dynamic context, any posture assessment must look at risks across the current fight and into the future across the spectrum of conflict. In this regard, the Department has established powerful cyber defensive technologies and operational capabilities that have proven capable in the past, and appear capable in the present fight; however, with ever decreasing margins. It is the context of the future fight that it is most challenging to assess. As we pivot from counter terrorism to near peer competition the risks increase, as they do for every war fighting capability.

It is clear, that for the future fight, the steps being taken in technology and operations will be fully sufficient for the low-tier threat actors of tomorrow while their margin against near-peer competitors will remain slim and uncertain. The steps being taken by DoD, for instance, to achieve ZT across all mission capabilities of the DoDIN, the modernization of DoD cryptography, and to operationalize defensive cyber operations are in the large placing DoD in the right posture for future conflict. The success of these programs and their ability to maintain critical margins depend on resourcing decisions made across the Future Years Defense Program (FYDP).

The Secretary previously discussed the Department's investment in cybersecurity and cyberspace operations to maintain the momentum of the Digital Modernization Strategy. Expanding on those comments, the Department's ZT framework assumes that the DoDIN is compromised, and employs existing and emerging cyber defense capabilities to derive a data, applications, and systems-centric security model that "denies by default." The $5.6B FY22 DoD Cybersecurity budget maintains enhanced funding levels established in FY20 and FY21 for key enterprise cybersecurity capabilities, including Identity, Credential, and Access Management (ICAM); endpoint security, including comply to connect (C2C) and Automated Continuous Endpoint Monitoring (ACEM); and User Activity Monitoring (UAM) have enabled DoD to begin to implement the ZT framework across the DODIN.

New investments to our IT and cybersecurity infrastructure will also be necessary to achieve a robust implementation of ZT. Some examples include software defined environments, continuous multi-factor authentication, micro-segmentation, artificial intelligence/machine learning (AI/ML), and user behavior monitoring. Once fully implemented, the DoD ZT framework will provide a new hardened architecture for the DoDIN which will significantly enhance resiliency and cyber defenses, requiring the adversary to invest considerable offensive resources to gain exceedingly limited access, if any at all, to data and resources.

Risk management will continue to be a key pillar of the DoD security program, and the DoD Risk Management Framework (RMF) assessment and authorization process ensures the Department designs, evaluates and monitors IT system compliance with ever improving security requirements. The DoD is starting to implement the Continuous Authority to Operate (cATO) within its Risk Management Framework to ensure that the IT systems connected to DoD's networks maintain the appropriate level of cybersecurity controls in light of a dynamic cyber threat environment. cATO allows us to continually monitor and respond to changes in the risk in our systems much faster. This results in fielding capabilities quicker for our warfighters, but also allows the Department to respond to the constantly changing cyber threats that we are facing.

As we look to further manage risk, DoD is working to mature the Strategic Cybersecurity Program (SCP) that addresses the requirements of the FY 2018 NDAA Section 1640 and FY 2021 NDAA Section 1712 to ensure that the DoD is always able to conduct the most important military mission of the Department. It is achieving these requirements through close collaboration of DoD CIO, USD(A&S), NSA and the DoD PCA. The DoD is undertaking pathfinders for twelve critical fielded systems. DoD will apply a seven step process that performs mission-based, threat informed risk reduction planning through a focus on the mission impacts of system vulnerabilities and the ability for adversaries to exploit them.

Encryption and Cross Domain Solutions (CDS), foundational cybersecurity capabilities, continue to be a high priority for the DoD. Building on enhancements in FY20 and FY21, the Department continued to increase investment in cryptographic modernization by funding next generation cryptographic algorithm development. Additionally, the Department has continued sustaining investment in CDS modernization, driving implementation of the CDS Raise the Bar (RTB) strategy.

Industrial Control Systems (ICS) has been a frequently overlooked technology across the government and industry. As the lead for control systems cybersecurity, DOD CIO is working hard to address risks in these systems. The Department has clarified that ICS is covered under our cybersecurity program and the cybersecurity standards that we have for traditional systems apply to control systems. We have published guidance to help ICS systems implement cybersecurity programs. Additionally, the Department is working to build cybersecurity expertise in our Cyber Workforce and are developing capabilities to monitor ICS systems. This is a tough problem that requires the DoD CIO to work with new partners. We are working with the National Institute of Standards and Technology (NIST) and the Cybersecurity and Infrastructure Security Agency (CISA) to develop cybersecurity standards for these technologies. We are strengthening our working relationships with the mission and system owners for these system to help them understand the threats and risks; and develop mitigations. The cyber vulnerability assessments the Department conducted of Defense Critical Infrastructure in response to FY2017 NDAA, Section 1650, have helped identify the nature of cyber vulnerabilities that are associated with our most important critical infrastructure. We have a significant amount of work left to do, but we've implemented many of the foundational principles and are moving to maturing our practices and capabilities.

Defining the Cyber Workforce

The Secretary discussed the importance of developing a diverse workforce that draws on "the full range of talent that the United States has to offer." Nowhere is this truer than in cyberspace. The Department must continue to modernize our approach to recruit, retain, and maintain Cyber Workforce talent. In the modern cyber environment, the race to recruit and retain the most innovative individuals with high-demand skillsets is a top priority for government and industry leaders alike. Emerging cyber talent are faced with an abundance of employment opportunities across the private sector where lucrative incentives are available to those with high-demand skillsets. To maintain a viable cyber-talent pipeline, the DoD CIO is focused on a strategy and key initiatives to attract these workers while encouraging increased diversity. The CIO is developing seven key initiatives to advance the Cyber Workforce.

First is the 8140 Policy Series to facilitate strategic Cyber Workforce management activities. This series will drive implementation of the vision for a robust and trained workforce necessary to meet our current and future cyber challenges. These policies accomplish this goal by providing a targeted, role-based approach to identify, develop and qualify cyber personnel leveraging the Defense Cyber Workforce Framework (DCWF).

Second is the Cyber Excepted Service (CES) mission-focused personnel system that supports the human capital lifecycle for civilian employees engaged in or in support of cyber-related missions. This program offers flexibilities for the recruitment, retention and development of cyber professionals across DoD. CES applies to ~9,000 civilian positions with ~6,500 positions converted to the program. CES includes a monetary compensation tool called the Targeted Local

Market Supplement (TLMS). It is used to incentivize critical work role coded positions that are faced with excessive vacancy and attrition rates. TLMS functions similarly to Locality Pay, where a predetermined percentage of pay is added to an employee's base pay, though the TLMS is scoped to work role coded positions and not occupational series or localities. This feature helps DoD be more competitive with industries and agencies hiring individuals with similar skill sets.

The third initiative is our ongoing series of Zero-Based Reviews (ZBR) of the workforce as required by section 1652 of the FY 2020 NDAA, which tasked DoD components to conduct a ZBR of cyber and IT positions. This review includes providing resource, technological, and funding information, as well as providing recommendations to improve capability and resource efficiencies. The DoD Tri-Chair (DoD CIO, PCA, and OSD P&R) created a funded course of action (COA) to accomplish the review that scoped down the level of effort while keeping with the intent of the congressional requirement. The Marine Corps was the first component to initiate the ZBR (phase 1), while the remaining components have recently initiated their efforts (phase 2). A ZBR interim update to Congress on initial observations from the Marine Corps will be provided in the coming days.

Fourth is an initiative we are calling Cyber 101, which utilizes the DC3 Cyber Training Academy to develop training to provide DoD personnel with a foundational understanding of the six common core knowledge, skills, and abilities (KSAs) required for each of the 54 DCWF work roles. This program will establish foundational cyberspace training to assist Components/Services in qualifying the workforce to DCWF positions and standards of DoD Manual 8140 "Cyberspace Workforce Qualification & Management Program."

Fifth, the DoD CIO has a goal to develop tools to assess cyber aptitude and differentiate/predict current employees and potential candidates' abilities or skills to perform cyberspace work. Aptitude testing enhances DoD's recruitment ability by identifying individual potential while predicting performance, behavior, and attrition. This will allow the Department's current Cyber Workforce to keep pace with technology trends and reskill the non-Cyber workforce to close mission critical cyber skill gaps. The DoD CIO partnered with Army Research Institute (ARI) to broaden validation efforts for the Common Cyber Capabilities (C3) Test. This partnership is enabling the DoD to leverage ongoing work to deliver a government-owned solution for use with personnel across the four Military Services. The DoD CIO was able to fund roughly $500K for this initiative in FY21, however additional funding is required to first, maintain current delivery and second, ensure the Department can leverage a viable platform for administration of the assessment planned through FY22.

The sixth initiative uses the Advanced Analytics platform known as ADVANA to better understand the workforce. We are developing a series of interactive dashboards through the platform to enable flexible, transparent and meaningful analysis of DoD's Cyber Workforce. These Cyber Workforce dashboards will merge data pulled from authoritative manpower and personnel systems and generate the real-time data required for managing the civilian Cyber Workforce. This initiative will use the data gathered from the Services and Components to enable the generation of a suite of Key Performance Indicators (KPIs) as well as real-time trend and predictive analysis.

The final initiative is the Cyber Workforce Strategy, our team in DoD CIO, in conjunction with colleagues in USD(P&R), will publish a new Cyber Workforce strategy by March 2022. The workforce strategy will shape the future Cyber Workforce to incorporate emerging technologies (AI, Data, Control Systems, and Machine Learning) and provide an authoritative foundation for digital workforce talent management. In order to ensure future workforce development capabilities, the DoD Cyber Workforce Strategy will increase diversity by expanding how talent is acquired and leverage developmental and educational programs. Our focus will be on innovative and creative personnel practices to increase entry level opportunities while adopting flexible retention models. The intent is to provide alternatives to the traditional 30-year career.

Command, Control, and Communications

Command, Control and Communications (C3) is part of the DoD CIO portfolio that makes the office unique and differentiates it from a civilian CIO position. While all divisions in the CIO, and aspects of the Digital Modernization Strategy, support warfighting, it is C3 that is most closely linked to the warfighter on the ground, sea and airspace. The critical capabilities in this portfolio are a priority for the enterprise.

The PNT enterprise is an essential contributor to cybersecurity and a critical element for any advanced weapon system to operate effectively in today's competitive environment. As the Secretary noted in his posture hearing, "modernization of all segments of GPS [Global Positioning System] to ensure precision and availability" is a priority for the Department. The investment that the Department requested in the FY22 budget will enable our progress in this area. It will fund GPS, including related "M-Code" modernization in DoD platforms/systems, as well as other complementary and alternative resilient PNT capability efforts. The Department understands the reality that while GPS remains the revolutionary cornerstone for worldwide PNT services to the Joint Force, it has increasingly become a target for disruption and denial by adversaries. Accordingly, the Department has been developing alternatives and complements for fielding in order to increase resiliency and survivability of the force. The Implementation Plan (I-Plan) for these PNT capabilities and applications addresses the FY 2021 NDAA Section 1611, *Resilient and Survivable PNT Capabilities*.

DoD CIO is also the Department's lead for the Electromagnetic Spectrum Enterprise (EMSE) and the designated senior official for the long-term implementation of the 2020 Spectrum Superiority Strategy. This strategy includes five high-level goals that will drive policy harmonization, I-Plan and workforce oversight, and enterprise governance. In accordance with the strategy, the Electromagnetic Spectrum Operations (EMSO) Cross Functional Team (CFT) developed an Electromagnetic Spectrum Superiority Strategy (EMSSS) I-Plan. Our team in DoD CIO will assume the EMSSS I-plan oversight from the EMSO CFT, in keeping with my role as the Principal Staff Assistant (PSA) for EMS and EMSE, subsequent to the Secretary's approval of the I-plan.

DoD continues to work with interagency partners to make available mid-band spectrum to support U.S. leadership in 5G. The Department has already made available the 3450-3650 MHz band for 5G and, under the new Emerging Mid-Band Radar Spectrum Sharing (EMBRSS) effort, has already begun the process of assessing the feasibility of sharing the 3100-3450 MHz band. DoD cannot vacate the 3100-3450 MHz band without significant mission and operational impact; however, the Department is studying opportunities and procedures to share this critical national resource. DoD will be assessing different courses of action based on different sharing frameworks that inform the Administration, federal regulators, and DoD senior leadership decision on the best way forward.

During his recent testimony, the Chairman spoke of a vision of future warfighters using "local and expeditionary 5G networks" to gain and maintain an information advantage in conflicts though connected sensors and weapons in resilient battlefield networks. We in the DoD CIO continue to work with USD(R&E) on a variety of 5G pilots to advance this vision for the future. These pilots explore the use of 5G technology in the areas that include standards, security, networks, and spectrum. Additionally, we're actively participating in the USD(R&E) CFT, which will transition leadership of 5G initiatives to us in CIO by 2024.

Finally, leadership communications in a denied, disrupted, intermittent and limited (DDIL) environment is of paramount importance during competition, crisis and conflict. To this end we have placed great emphasis on preparing to provide our leaders with the right information at the right time under all conditions. The FY22 budget includes $14.5M to continue the Pentagon and Raven Rock Information Technology Modernization efforts. This year we continue to modernize and update the locations' network access points and active directory as well as consolidate and modernize the servers that support multiple networks at both locations.

Data

Data is the ammunition of the future. Under Secretary Austin's leadership, the Department has prioritized ensuring the timely, secure, and resilient access to data that enables advanced warfighting capabilities needed for military advantage in all-domain operations. While data management is not directly tied to specified program elements in the FY22 budget request, we are identifying, assessing, and tracking our data-related investments as part of the budget certification process that I lead. The Department must measure, manage, and modernize its data assets to create new operational advantages and remain effective against near-peer competitors. Becoming a data-centric organization is a top priority for DoD.

The Department is aggressively implementing the actions described in the recent DoD Data Strategy and the Deputy Secretary's recent guidance entitled "Creating a Data Advantage." The Data Strategy provides a clear vision, principals, objectives, and focus areas for data management. We need to make DoD data visible, accessible, understandable, linked, trusted, interoperable and secure. The recent guidance from the Deputy Secretary helps accelerate this transition by via a series of five "Data Decrees" to guide the force in the transition to an open data standard architecture and strategic use of data.

Last fall, the CDO established a Data Council composed of all the Department's data leaders, and he also meets regularly with data leaders from across the Combatant Commands, our interagency teammates, and our "Five Eyes" (FVEY) partners. The CDO's office has also established key data related policies, guidelines, and processes on topics such as data cataloging, sharing and protection.

The DoD is implementing the ability to use live data to inform senior leader decision-making. Forums such as the Deputies Management Action Group (DMAG) now use data-driven analytics and metrics to track progress on all the Department's top priorities. The signal from the top, including frequent emphasis by the Vice Chairman, is that all organizations need to provide, manage, and share decision-quality data. Components are getting the message and treating data as a resource.

Similarly, the warfighting community is collaborating to solve the interoperability challenges posed by Joint All Domain Operations and new operational concepts. CDO is partnering with Combatant Commanders, Services, Joint Staff, and international partners to enable JADC2 and provide the warfighter with data whenever and wherever needed. This shift to a data-centric approach is urgent, underway, and already leaving a lasting impact on the Department.

Conclusion

I'd like to note the importance of our coordination and partnership with Congress in all of these areas and many others. Today we have discussed key initiatives in the areas of cloud enabled warfighting, software and network modernization, cybersecurity, the Department's Cyber Workforce, C3 and data. I look forward to continuing to work with Congress through the authorization and appropriation process and beyond as we continue to evolve to maintain the Department's information advantage. Thank you for the opportunity to testify this afternoon, and I look forward to your questions.

John Sherman
Acting Department of Defense Chief Information Officer

Mr. John Sherman is a career member of the Senior Intelligence Service, serving as the Acting Department of Defense Chief Information Officer (DoD CIO) since January 2021. In this capacity, Mr. Sherman serves as the primary 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.

Prior to assuming the role of the Acting DoD CIO, he served as the Principal Deputy, DoD CIO from June 2020 to January 2021.

Before joining DoD CIO, Mr. Sherman served from 2017-2020 as the Intelligence Community (IC) CIO. 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.

WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING

JUNE 29, 2021

RESPONSES TO QUESTIONS SUBMITTED BY MR. LANGEVIN

Mr. SHERMAN. The DOD defines the Cyberspace Workforce in DOD Directive 8140.01 as "personnel who build, secure, operate, defend, and protect DOD and U.S. cyberspace resources; conduct related intelligence activities; enable future operations; and project power in or through cyberspace." It is comprised of 54 work roles and 5 elements: Information Technology (IT), Cybersecurity, Cyberspace Effects, Intelligence (Cyberspace), and Cyberspace Enablers. The Cyber Operations Forces (COF) are included in the broader Cyberspace Workforce and consist of "Units organized, trained, and equipped to conduct offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), and DOD Information Network (DODIN) operations." The DOD CIO, in coordination and consultation with U.S. Cyber Command (USCYBERCOM) and the Components, has developed foundational qualification standards for the Cyber Workforce in accordance with DOD Directive 8140.01. USCYBERCOM is authorized to augment Enterprise qualification requirements with focused training requirements to meet specialized mission objectives, which extends to the COF. [See page 6.]

Mr. SHERMAN. Regarding whether Cyberspace Operations Forces will have dedicated elements for IOT cybersecurity, the DOD Cybersecurity Program is applicable to all DOD systems and technology types. Likewise, the Cyber Mission Force is organized, trained, and equipped to operate, protect and defend in all mission environments. Dedicated forces solely for "operational technology (OT) cybersecurity" are not feasible as most DOD systems are comprised of many different technology types. To enhance the cybersecurity risk posture of all systems and ensure readiness, the DOD CIO and U.S. Cyber Command are integrating the DOD Cybersecurity Program and the Cyber Operations Program. This integration will inform and mature the skill sets of the cyber mission force to ensure they have the requisite skills to protect and restore critical systems that enable the Department to successfully accomplish its various missions and operations in a cyber-contested environment. [See page 7.]

RESPONSES TO QUESTIONS SUBMITTED BY MS. HOULAHAN

Mr. SHERMAN. At the awareness level, the primary purpose of Cyber Awareness Challenge, mandated to be taken by all DOD personnel annually, is to influence behavior, focusing on actions that authorized users can engage to mitigate threats and vulnerabilities to DOD Information Systems, and that the users themselves are a critical link protecting DOD information and information technology (IT). The Cyber Awareness Challenge content works to encourage cyber citizenship and digital leadership by providing users with an awareness needed to maintain a degree of understanding about cybersecurity policies and doctrine commensurate with their responsibilities. All users must be capable of 14 appropriately reporting and responding to suspicious activities and know how to protect the information and IT systems to which they have access. The course provides an overview of cybersecurity threats and encourages users to maintain awareness of and stay up to date on new cybersecurity threats. The training also reinforces best practices to keep both DOD and personal information secure and stay abreast of changes in DOD cybersecurity policies. Course content is based on the requirements addressed in Congressional Legislation, Federal and DOD policies, and from DOD Component community input from the DOD CIO chaired Cyber Workforce Advisory Group (CWAG). An example below of new DOD Component community input that will be added to 2022 version to be fielded on October 1, 2021 is content on disinformation. "Adversaries exploit social and other media to share and rapidly spread false or misleading news stories and conspiracy theories about U.S. military and national security issues. Using fake accounts on popular social networking platforms, these adversaries:

- Disseminate fake news, including propaganda, satire, sloppy journalism, misleading headlines, and biased news
- Share fake audio and video, which is increasingly difficult to detect as the creation technology improves

- Gather personal information shared on social media to devise social engineering attacks
- Most media messages intend to influence you, if only to attract traffic.

Ask yourself:

- Who provided the information, and why?
- How does the information provider want you to act?
- Whose interests would your reaction serve?"

The depth of understanding of the Cyber Awareness Challenge is mapped to the Cybersecurity Essentials concept as described in the Information Technology Security Learning Continuum Model found in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800.16. The Draft NIST SP 800–16 Revision 1 (3rd Draft), titled "A Role-Based Model for Federal Information Technology/Cyber Security Training," dated March 2014, describes Cybersecurity Essentials. Cybersecurity Essentials, in addition to knowledge gathered via security awareness, provides a general introduction to cybersecurity. The concept of Cybersecurity Essentials is not computer literacy as this concept refers to an individual's familiarity with a basic set of knowledge that is needed to use and maintain a computer. Cybersecurity Essentials refers to an individual's familiarity with—and ability to apply—a core knowledge set required to protect electronic information and systems. [See page 12.]

Mr. SHERMAN. DOD's approach to cybersecurity with respect to allies is directed by the classified International Cyberspace Security Cooperation Guidance. Along with the Department of State, DOD seeks like-minded partners who will stand with us to reinforce responsible state behavior in cyberspace and push back on the authoritarian regimes that seek to control access to information and expand the surveillance state. The Department has been quite active in sharing its views about the cybersecurity risks of telecommunications infrastructure provided by companies with ties to authoritarian regimes. Further, the Department has expressed the importance of countries building 5G networks that rely on infrastructure and equipment that meets our cybersecurity standards. [See page 20.]

RESPONSE TO QUESTION SUBMITTED BY MR. LARSEN

Mr. SHERMAN. The Department of Defense Artificial Intelligence Education Strategy, developed in response to Section 256 of the FY20 NDAA, is the foundation for the JAIC-led pilot training programs based on AI archetypes and concentrations designed to differentiate AI learning needs across the entire DOD workforce, from the AI developers to the administrative assistants. Since October 2020, the JAIC has launched four pilots—they target DOD leadership, product managers, acquisition professionals, and data scientists. A present, three of the pilots are currently underway, and one has successfully been completed. Each of the pilots are designed to improve the skill sets of the current workforce and to encourage cross collaboration across the commands through the interaction of its students in a common learning environment. The JAIC is currently evaluating these early pilots to assess their effectiveness in meeting the DOD needs of AI education at scale. As the Department moves toward further implementation and integration of AI capabilities, it will be paramount for the DOD to adopt scalable training and education practices. DOD stands at a critical juncture in history, where adopting AI capabilities at speed and scale is essential to maintain military advantage. DOD must not only develop world class AI practitioners to make AI real at the Department, but must also ensure the entire DOD workforce is ready and capable to employ AI capabilities in their respective areas of responsibility. It is important that the DOD AI training strategy is constantly updated to ensure new developments in the field are incorporated into the training to ensure DOD's competitive edge against our adversaries. [See page 17.]

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

JUNE 29, 2021

QUESTIONS SUBMITTED BY MR. BANKS

Mr. BANKS. Mr. Sherman, Purdue University and Carnegie Mellon University, in partnership with industry, recently launched a research effort to study the use of AI for intrusion detection in resource-limited embedded systems.

Artificial intelligence, as you know, is one of the most effective methods to detect undesired or anomalous behaviors within systems. However, traditional AI requires significant computing resources that may not be available in challenging operating environments, like aircraft engines, where high-temperatures, high-vibration and high-noise levels require robust, and often less-sophisticated, embedded systems.

Given your view of the future threat environment, and the DOD's intention to procure new combat systems—like hypersonics—how critical is it that we fund and develop threat detection capability for embedded systems that can operate in harsh environments?

Will you commit to working with Purdue, and their partners to ensure we mature this capability?

Mr. SHERMAN. The Department concurs that employment of threat detection capability for embedded systems that can operate in harsh environments is critical. Artificial intelligence (AI) at-the-edge, where data can be analyzed in near-real time or real time, will provide key insights into current or future performance for critical systems such as aircraft engines. However, the data with which these algorithms are developed, trained, and tested can be as important (if not more so) than the algorithms themselves. Sensors currently exist that enable real-time data collection in these highly-dynamic, harsh environments. This data can be leveraged in compute-rich environments to develop AI/machine learning (ML) models for deployment to the edge. Once deployed, these embedded algorithms can analyze this critical data to provide predictions and analytics in a future threat environment. DOD has partnered with universities and companies looking to leverage AI and anomaly detection to enhance the cybersecurity of embedded sensors and software. At a high-level, this is very similar to how the DOD cyber protection teams are using AI/ML today; with tools developed by the JAIC and others. Since data is the foundation for AI, each of these sensors/embedded systems become a potential target for corrupted or manipulated data; and from an autonomous cyber perspective, they each could be a potential inject point for a cyber exploit. 2 DOD CIO has identified threat detection in this environment as critical to assuring the safety of our warfighters and success of our mission. DOD CIO and the Defense Information Systems Agency (DISA) recently initiated the deployment of an AI/ML-based cybersecurity capability for industrial control systems (ICS) defense. This work is based on the capability to monitor spacecraft behavior that exhibits the same methodical and well-characterized traffic that ICS exhibit. DOD CIO is committed to working with OUSD(R&E), the Services, the Defense Industrial Base (DIB), academia, DISA and the Joint Artificial Intelligence Center (JAIC) to employ diverse partnerships, such as with Purdue, Carnegie Mellon, and others, to enhance our cyber-secure future.

Mr. BANKS. Mr. Sherman, mobile devices are the current and future of compute—with massive investment and innovation from the commercial sector. How is the Department using mobile devices today? What plans do you have to leverage technologies like 5G in order to support the use of mobile devices within the broader national security infrastructure? How are you securing those devices? Many governments, including the United States, ban commercial smartphones and tablets in secure spaces due to security risks, which impacts accessibility, productively, and the ability of the Department to recruit people who have become reliant on their mobile devices. What is your plan to securely enable mobile devices at work, at home and on the move? Finally, how does the Department control RF emissions and our adversaries' use of them to target mobile users?

Mr. SHERMAN. The DOD is employing mobile devices today. With our Microsoft Office 365 (O365) deployment of e-mail, chat, and communication tools, the Department is taking a measured approach that balances accessibility and security. Government-furnished mobile phones provide access to O365 tools through the native application. There are also multiple ongoing pilots by the Army, Navy, Air Force, National Guard, and Defense Information Systems Agency (DISA) to enable access from personal mobility devices utilizing modern commercial cybersecurity tools, or via virtualization from a remote, secure infrastructure. DOD is also planning for technologies like 5G to support mobility. The deployment of 5G will significantly broaden the use of mobile devices across all aspects of the Department's infrastructure—including in physical security, logistics, transportation, maintenance, training, command and control, and combat operations. We are currently piloting each of these applications in 10 experiments across 11 DOD installations in the Continental United States and Hawaii. The results of these projects will be foundational for the plan to transition 5G technology to operational use within DOD, as stipulated in Section 224 of the Fiscal Year 2021 National Defense Authorization Act. To secure these devices, DOD is actively implementing cybersecurity principles and techniques in all aspects of its 5G technology development and deployment—including in supply chain risk management, zero-trust network implementation, and the use of highresiliency operational techniques. 3 DOD actions to secure the 5G supply chain are consistent with the National Strategy to Secure 5G and are in accordance with the DOD 5G Strategy Implementation Plan. The DOD is engaged in Defense Industrial Base (DIB) consortiums established to protect national security interests. Further, DOD is developing 5G-specific Supply Chain Risk Management standards through the North American Alliance for Telecommunications Industry Solutions (ATIS). DOD makes extensive use of mobile devices at home and on the move. The Department also makes extensive use of properly secured laptops and tablets at work, including in secure spaces. There are numerous issuances that govern the use of commercially available unclassified and classified mobile devices and technologies in DOD-accredited classified spaces. DOD balances the risk of compromise of classified information with mission capability very carefully. In many cases, the risk is determined too great to integrate mobile technologies in these spaces. During the COVID–19 pandemic, the Department adapted to remote work through largest deployment of Microsoft Teams in history. As we plan for a return to work, DOD is diligently working to find the correct balance between capability and security. DOD goes to great lengths to keep foreign adversaries from introducing radio frequency (RF) listening devices, or "bugs," into our classified environments. DOD personnel bringing smartphones and tablets into these spaces could enable hostile monitoring of classified conversations through embedded and undetected malware, doing our adversaries' work for them. Physical security issuances provide guidance for RF shielding protecting classified spaces as well as restrictions on the introduction of mobile devices to prevent compromise of classified information.

QUESTIONS SUBMITTED BY MS. HOULAHAN

Ms. HOULAHAN. Back in April, I sent a letter to Secretary Austin with several of my colleagues asking the DOD to implement mandatory training on digital literacy and cyber citizenship within the DOD. The proposed defense budget would set aside $30.8 million to help the Pentagon improve tools to identify and address extremism among troops, and enhance training at all levels. It also includes $9.1 million to take initial steps to fight extremism and insider threats.

Can you share in a bit more detail what these tools and trainings would look like?

Mr. SHERMAN. DOD CIO supports OUSD(I&S) efforts to take essential steps to fight extremism and insider threats through the proposed Non-Secure Internet Protocol Router (NIPR) User Activity Monitoring (UAM) program described in the $9.5 million request. UAM provides a technical capability to observe and record the actions and activities of an individual at any time on select Non-Secure Internet Protocol Router (NIPR) devices accessing U.S. Government information in order to detect insider threats. The NIPR UAM capability provides the Department with the ability to detect and monitor leading indicators of concern on the unclassified IT system. The Departments 'Countering Extremist Activity Working Group' is exploring multiple actions to enhance Insider Threat (InT) awareness training which are still being reviewed. While those recommendations are being finalized, the Office of Under Secretary of Defense for Intelligence & Security (OUSD(I&S)) is: (1) collaborating with the Common Military Training Working Group to include InT awareness training and requirements for the services in an efficient and effective manner; (2) reviewing the Cyber Awareness Challenge and InT trainings provided by Defense Counterintelligence and Security Agency (DCSA) Center for Development of Security Excellence (CDSE) for recommended updates to address extremist activities/behaviors; and (3) partnering with Department stakeholders to produce additional training tools, including graphic novels and leadership training videos, to assist with identifying, addressing, and mitigating extremist activities and other behaviors of concern. The $30.8M is contained within the Defense Counterintelligence and Security Agency (DCSA)'s FY 2022 President's Budget request, as follows:

- User Activity Monitoring: +$9.5M/3 Full-time Equivalents (FTEs) in O&M, DW (DCSA OP–5 Increase Statement #1) 5
- Vetting Risk Operations Center: +$12.5M O&M,DW/7 FTEs (DCSA OP–5 Increase Statement #5); +$8.8M in RDT&E,DW (DCSA RDT&E, DW Line 230, PE 0305128V, Security and Investigative Activities)

Additionally, the Vetting Risk Operations Center (VROC) incorporates Publicly Available Electronic Information (PAEI), including social media, into background investigations in accordance with Security Executive Agent Directive 5 (SEAD–5) and aligned to the Trusted Workforce 2.0 personnel vetting reform initiative. PAEI also fulfills the Secretary's requirements to improve the vetting of International Military Students who intend to or are currently receiving training within the continental U.S. This effort funds collection, analysis and reporting of PAEI, including social media, in support of national security eligibility determinations. The PAEI investment will deliver a capability to support DOD requirements for enhanced personnel security as directed in the Intelligence Authorization Act for Fiscal Year 2016 (division M, P.L. 114–113), and aide in the execution of continuous vetting in accordance with direction of the Security and Suitability Executive Agents

Ms. HOULAHAN. I recently met with several defense attachés who shared how their nations are implementing effective cybersecurity protocols and managing potential cyber attacks/intrusions, some times better than the United States.

Has the DOD sought to work closely with our allies to determine what cybersecurity practices are working well for other nations?

Has there been any discussion in the DOD or with our allies about developing a comprehensive approach to cybersecurity or a global cyber infrastructure?

Mr. SHERMAN. The DOD continues to share US Government (USG)-approved cybersecurity standards such as the National Institute for Standards and Technology (NIST) framework with partners. However, the Department is always interested in learning how are allies are tackling problems of interest to DOD too. We regularly engage on a bilateral and multilateral basis to share best practices with mission partners and to proliferate cybersecurity best practices and standards. Of note, DOD generally cites the NIST standards both in our international engagements and when developing security cooperation cyber security programs with partners. Also, DOD CIO publishes a cybersecurity reference and resource guide for the department that is just as applicable for international partners. DOD's approach to cybersecurity with respect to allies is directed by the classified International Cyberspace Security Cooperation Guidance. Along with the Department of State, DOD seeks like-minded partners who will reinforce responsible state behavior in cyberspace and push back on the authoritarian regimes that seek to control access to information and expand the surveillance state. The Department has been quite active in sharing its views about the cybersecurity risks of telecommunications infrastructure provided by companies with ties to authoritarian regimes. The Department has expressed the importance of countries building 5G networks that rely on infrastructure and equipment that meets DOD's cybersecurity standards.

Ms. HOULAHAN. During my time in Congress, I have advocated vigorously for investment in DOD STEM to ensure cyber professionals remain competitive and meet the needs of the future's workforce. To that end, I am interested in your perspective on Cyber Excepted Service.

At hearing in April before the Senate Armed Services Personnel Subcommittee, the Acting Secretary for Defense for Civilian Personnel Policy testified on how important Cyber Excepted Service authorities have been to enhancing recruitment of cyber professionals, pointing to the flexibility in compensation and classification of work requirements as examples of how the program has been able to better meet targeted cyber needs. We've also received testimony in this Subcommittee from the U.S. CYBERCOM Commander that mission and the opportunity to work with colleagues of such high caliber—provides the most unique and important competitive advantage than compensation when competing with the commercial industry. I'd like to hear your take on what is and isn't working with Cyber Excepted Service from an IT perspective rather than a personnel perspective. Do you agree with these assessments? What do you want Congress to know about what is and isn't working as we continue to examine these and other authorities to meet DOD's cyber needs?

Is the program equally effective from both a recruitment and retention perspective? How are we making these cyber positions competitive to retain highly qualified individuals and prevent them from moving on to the private sector?

Mr. SHERMAN. The Department of Defense is appreciative of the authorities and flexibilities afforded by Congress to implement the Cyber Excepted Service (CES). Since October 2018, US Cyber Command (USCC) continues to see positive improvements to the recruiting and hiring timeline with the use of CES authorities. Some metrics provided below:

- Since CES implementation, USCC conducted 19 recruiting/hiring events resulting in 150+ job offers (including same-day offers during the hiring events on 18 May, 2018, and 28 August, 2019), met over 3,300 candidates and built a repository of 5,000+ resumes.
- CES authorities decreased their hiring timeline by 45 percent. The average timeline to receive a Tentative Job Offer started at 111 days prior to CES and reduced to less than 60 days pre-COVID. This is separate from the security clearance process and associated timelines. 8
- Despite the nation-wide impacts of COVID–19, USCC found alternative ways to onboard new talent. In 2020, USCC added over 70 new cyber warriors to their formation.
- In 2019, the Command offered $270K in recruitment incentives and over $80K in relocation incentives.
- In 2020, USCC offered over $375K in recruitment incentives and over $40K in relocation incentives to attract high-quality civilians with competitive compensation packages.
- In 2021, USCC offered $219K in recruitment and retention packages. A key program enhancement has been the development of CES Target Local Market Supplement (TLMS), a monetary compensation tool used to incentivize seven critical work roles. The TLMS addresses recruiting and retention challenges of these critical work roles due to excessive vacancy and attrition rates.
- To date, USCC paid $40K in support of TLMS and anticipates paying $60K by the end of this FY.
- The Department continues to explore this new authority and use it as a tool to attract our best and brightest cyber warriors.

QUESTIONS SUBMITTED BY MR. MOORE

Mr. MOORE. Now that a Federal judge recently rejected the government's motion to dismiss the JEDI protest, what is the DOD doing to meet this pressing need?

Mr. SHERMAN. The Department continues to have unmet cloud capability gaps for enterprise-wide, commercial cloud services at all three classification levels that work from the home front out to the tactical edge, at scale. In the three-and-a-half years since the Department developed its enterprise cloud needs, the cloud computing industry has undergone significant technical advancements and marketplace changes. The Department has itself matured in its cloud technology utilization. Additionally, a number of new programs, including Joint All Domain Command and Control (JADC2) and the Artificial Intelligence (AI) and Data Acceleration (ADA) initiative, have impacted the Department's enterprise cloud needs. As it exists, the JEDI Cloud solution no longer supports the technical requirements of the Department. In a commitment to filling our unmet capability gaps, on 6 July, 2021, the DOD canceled the JEDI Cloud Request for Proposals (RFP), began the process to terminate the JEDI contract, and issued a Pre-Solicitation Notice for a new contract action, the Joint Warfighting Cloud Capability (JWCC). The JWCC is a multi-award/multi-vendor cloud solution with a performance period of no more than five years, if all the options are exercised. The JWCC will allow for vendor competition at the task order level and will help drive innovation and pricing to the benefit of the Department. Additionally, in a multi-vendor environment, DOD Components will be able to consider varying approaches to their specific cloud computing needs and will be able to choose the vendor whose capabilities best suit their missions. DOD is actively pursuing the JWCC contract and is in the process of completing its market research by conducting technical engagements with each of the U.S.-based hyperscale Cloud Service Providers (CSPs) to evaluate if they meet DOD's requirements. The intent is to provide the Warfighter with an enterprise multi-vendor cloud solution as quickly as possible. The Department intends to make awards within the next 8–12 months.

Mr. MOORE. The DOD OCIO's December 2020 report on the status of implementation of 21st Century IDEA states that the Department "is working to ensure each department or command has selected a 21st Century IDEA designee responsible for coordinating the implementation of IDEA requirements."

What is the status of this requirement? Has every required department or command identified a 21st Century IDEA lead? Can you provide that list to the committee? Will the Department be requesting funding in future year budgets to meet these requirements?

Mr. SHERMAN. The Department identified a 21st Century IDEA designee from each required Service CIO, Washington Headquarters Service, and relevant Defense Agencies and Field Activity. To further support the implementation of the IDEA requirements, DOD CIO established the 21st Century IDEA Working Group that meets quarterly to coordinate on OMB and Congressional reporting. The Department is committed to meeting the legal requirements of the IDEA act and has established an environment that fosters open communication and sharing of ideas, lessons learned, and dialog for future opportunities for standardization. The DOD CIO plans to utilize the 21st Century IDEA Working Group to continue open dialog on the improvement and standardization of customer experience and digital services, and ensure that resource gaps are identified and addressed.