[H.A.S.C. No. 116–7]

HEARING

ON

NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2020

AND

OVERSIGHT OF PREVIOUSLY AUTHORIZED PROGRAMS

BEFORE THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES
ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES HEARING

ON

DEPARTMENT OF DEFENSE INFORMATION TECHNOLOGY, CYBERSECURITY, AND INFORMATION ASSURANCE

HEARING HELD
FEBRUARY 26, 2019

U.S. GOVERNMENT PUBLISHING OFFICE
36–233 WASHINGTON : 2019

SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES

JAMES R. LANGEVIN, Rhode Island, *Chairman*

RICK LARSEN, Washington
JIM COOPER, Tennessee
TULSI GABBARD, Hawaii
ANTHONY G. BROWN, Maryland
RO KHANNA, California
WILLIAM R. KEATING, Massachusetts
ANDY KIM, New Jersey
CHRISSY HOULAHAN, Pennsylvania
JASON CROW, Colorado, *Vice Chair*
ELISSA SLOTKIN, Michigan
LORI TRAHAN, Massachusetts

ELISE M. STEFANIK, New York
SAM GRAVES, Missouri
RALPH LEE ABRAHAM, Louisiana
K. MICHAEL CONAWAY, Texas
AUSTIN SCOTT, Georgia
SCOTT DESJARLAIS, Tennessee
MIKE GALLAGHER, Wisconsin
MICHAEL WALTZ, Florida
DON BACON, Nebraska
JIM BANKS, Indiana

JOSH STIEFEL, *Professional Staff Member*
PETER VILLANO, *Professional Staff Member*
CAROLINE KEHRLI, *Clerk*

CONTENTS

DEPARTMENT OF DEFENSE INFORMATION TECHNOLOGY, CYBERSECURITY, AND INFORMATION ASSURANCE

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES,
Washington, DC, Tuesday, February 26, 2019.

The subcommittee met, pursuant to call, at 2:05 p.m., in room 2212, 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 INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES

Mr. LANGEVIN. The subcommittee will come to order.

I want to take this opportunity, first of all, to welcome our witnesses here today. And we welcome 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] status, its modernization efforts, and its strategic direction for the foreseeable future.

Our witnesses today are Ms. Lisa Hershman, the Acting Chief Management Officer; Mr. Dana Deasy, the Department's Chief Information Officer; and Brigadier General Dennis Crall, the Deputy Principal Cyber Advisor.

The Defense Department's IT infrastructure is as important to the mission as the weapons platforms that our service members employ. We cannot expect the services to maintain combat superiority if the technology that we rely on is deficient, outdated, insecure, or inoperable. IT should never be considered a back-office function as it may have been in previous eras.

The challenge of managing the Department's IT is highlighted best by the sheer number of topics that we will be hearing about today, including cybersecurity, business systems, artificial intelligence, data management, JEDI [Joint Enterprise Defense Infrastructure], and the Cyber Excepted Service.

IT reform and modernization require appropriate stewardship by the Department's leaders, many of whom are seated here today. Over the past several years, Congress has endeavored to ensure that the Department is structured in a way that gives senior leaders the authorities that they need to carry out their responsibilities.

For example, Congress created and elevated the position of CMO [Chief Management Officer] and gave that individual the responsibility for business systems. Additionally, Congress provided new standard-setting and budget authorities to the CIO [Chief Information Officer] that took effect at the beginning of the calendar year. All of this was done with an understanding that the PCA [Principal Cyber Advisor] also has a critical role to play with respect to cybersecurity of such systems.

Given how dynamic the IT space is, it is reasonable for this subcommittee to continually take stock of how the Department is implementing statutory changes and whether the outcomes match congressional intent. For this reason, I am eager to hear from the witnesses how the new roles, responsibilities, and authorities are being implemented and whether any of the changes made in recent years ought to be modified further. This includes discussion of the resources dedicated to the office of the PCA and coordination mechanisms.

In addition to organizational changes, the Department is taking positive steps to embrace new technologies. Initiatives such as the Joint Artificial Intelligence Center and the Joint Enterprise Defense Infrastructure cloud initiative seek to capitalize on emergent technologies with significant potential benefits for the Department. This subcommittee is invested in the success of these efforts, if managed correctly, and with an understanding of how these dollar investments at the OSD [Office of the Secretary of Defense] level coincide with efforts by the services and agencies, such as the other 300-plus cloud computing initiatives.

Success of the Department in the IT space is predicated not only on the software and hardware that we buy and maintain, but equally on the workforce that we employ. The Pentagon cannot succeed in this new era if we are not recruiting and retaining the very best possible workforce. So I am pleased that the workforce is consistently raised as a priority issue and flagged as one of the premier lines of effort in the DOD [Department of Defense] Cyber Strategy.

The competition for talent, of course, in this space we know is fierce, which is one of the reasons Congress created the Cyber Excepted Service [CES], a personnel system built specifically to attract top-tier talent with competitive salaries. The DOD CIO was designated as the Department's lead in crafting this new personnel system. To date, CES has only been implemented at U.S. Cyber Command Joint Forces Headquarters, DOD Information Networks, and DOD CIO Cybersecurity. Today provides us an opportunity to ensure the appropriate resources are dedicated to swift implementation across the entire Department.

Finally, I remain concerned about cybersecurity across the Department. While we have made significant progress in securing the DODIN [Department of Defense Information Network], particularly as U.S. Cyber Command matures, the theft of DOD data from contractors and the security of weapon systems themselves are both challenges that we absolutely have to address. Congress has taken steps in recent years to evaluate the risk posed by our DIB [defense industrial base] supply chain, but I am going to be interested

to hear more about how the CIO's office is leveraging its position and expertise to take more steps to mitigate this risk.

So, with that, I look forward to hearing from our witnesses today about how they are posturing the Department for success. And before we go to our witnesses, I would like to now turn it over to the ranking member—or the acting ranking member, Mr. Scott, for any opening statements that the ranking member may have.

[The prepared statement of Mr. Langevin can be found in the Appendix on page 33.]

STATEMENT OF HON. AUSTIN SCOTT, A REPRESENTATIVE FROM GEORGIA, SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES

Mr. SCOTT. Thank you, Chairman Langevin, and welcome to our witnesses here today. Ranking Member Stefanik is delayed due to a markup proceeding that is taking place on the Education and Labor Committee. I would simply ask that her entire statement be entered into the record, and yield back to the chairman so we can hear from our witnesses prior to votes. Thank you.

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

Mr. LANGEVIN. I would like to turn it over to our witnesses. Ms. Hershman, we will start with you. Thank you.

STATEMENT OF LISA HERSHMAN, ACTING CHIEF MANAGEMENT OFFICER, OFFICE OF THE SECRETARY OF DEFENSE

Ms. HERSHMAN. Thank you, Chairman Langevin, Ranking Member Stefanik, and other members of this subcommittee, for the opportunity to testify today on the Department's information technology, cybersecurity, and information assurance. I am Lisa Hershman, the acting Chief Management Officer. Today, I would like to outline my roles, responsibilities, and priorities, the Department's aggressive work to reform and modernize business operations, and the monumental changes in our management of data throughout the enterprise.

As acting CMO, it is my responsibility to deliver optimized business operations to assure the success of the National Defense Strategy. This is only made possible by the elevation of the CMO as the number three in the Department and the increased authorities granted by the National Defense Authorization Act [NDAA]. My goal as acting CMO aligns directly with the intent of the NDAA, efficiency for lethality, which is executed by reforming the Department's business processes, systems, and policies, to gain increased effectiveness, higher performance, and reprioritized resources.

Integrity and consistency of every measure is a cornerstone of my approach. Working closely with the comptroller and military departments, we define standards to reform in execution—for reform—and have validated our efforts in the budget. Because of this effort, the Department has realized a total of $4.7 billion in program savings in fiscal year 2017 and 2018. However, reforming the business operations of the Department must not only be focused on financial savings, but also on creating a sustainable impact by es-

tablishing a culture of continuous improvement focused on results and accountability.

The Department's priorities of reform are based upon the fiscal year 2019 NDAA, the President's Management Agenda, the senior leader Reform Management Group, and the first DOD-wide financial audit. While we execute reform in many areas, IT infrastructure, business systems, and data management have some of the most significant opportunity for improvement.

Our current IT and business systems environment is extremely complex, with hundreds of business systems, thousands of data centers, hundreds of cloud efforts, and thousands of applications, in addition to 65 CIOs. It is extremely difficult for us to deliver an effective, innovative, or secure IT environment. As the CIO for Defense Business Systems, working closely with the PCA and the CIO, it is our collective responsibility to reverse this environment.

We are executing business systems reform in three major areas: eliminating redundant systems, maximizing shared service delivery, and streamlining business operations in areas like procurement through category management. Through initiatives in these areas, we have already made progress towards simplifying the IT landscape, reducing operational costs, and enabling business process integration.

As we execute reform, we remain ever mindful that the goal is delivery of secure, relevant, clean data to support business decisions, while IT infrastructures and business systems act as vehicles by which the data travels.

I want to personally thank you for supporting the data needs of the Department through the NDAA. This law provided CMO with the framework to establish common enterprise data and data management and analytics as a shared service. To ensure data management had the full dedication it requires, I hired the Department's first chief data officer, Mr. Michael Conlin.

As outlined in my implementation plan for common enterprise data, we will make decisions based on accurate, timely business data as opposed to internal boundaries and past experiences. This is a monumental shift in the way the Department conducts its business operations, and I am committed to ensuring the priority of data management in my role.

Thank you for the opportunity to outline my roles, responsibilities, and priorities, and provide details of our work in reforming the Department's IT, business systems, and data management. I welcome your questions.

[The prepared statement of Ms. Hershman can be found in the Appendix on page 37.]

Mr. LANGEVIN. Thank you, Ms. Hershman.

And now turn it over to Mr. Deasy.

STATEMENT OF DANA DEASY, CHIEF INFORMATION OFFICER, OFFICE OF THE SECRETARY OF DEFENSE

Mr. DEASY. 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 Dana Deasy, the Department of Defense Chief

Information Officer. Today, I would like to highlight key areas of the Department's digital modernization, including cloud, AI [artificial intelligence], C3 [command, control and communications], and cyber, as well as a separate effort on IT reform.

Earlier this month, the Department submitted its cloud report and strategy. As stated in that submission, DOD will remain a multicloud environment with both general purpose and fit-for-purpose clouds as part of our long-term strategy. As I have discussed with some of you previously, JEDI is a pathfinder, general purpose, enterprise-wide cloud. As part of our strategy, JEDI will enable DOD to learn how to implement an enterprise cloud solution, taking advantage of economies of scale and enhanced data-driven decision making.

The National Defense Strategy makes clear that the character of warfare is changing. Competitors like Russia and China are investing heavily in modernization in AI to refine the future of warfare. DOD must do the same. The AI strategy emphasizes the need to increase speed and agility, which will deliver AI-enabled capabilities, the importance of evolving our partnerships with industry and academia, and the Department's commitment to lead military, ethics, and AI safety. The Joint Artificial Intelligence Center [JAIC] is the focal point for carrying out the DOD AI strategy. JAIC will accelerate DOD's delivery and adoption of AI to achieve our global mission.

The emergence of digital technologies has introduced new challenges to the traditional C3 landscape. In order to take advantage of the new digital capabilities and to protect our warfighter from corresponding weaknesses, we must modify and modernize our C3 systems. In order to facilitate economic growth while accounting for national security, DOD CIO, working with OUSD(R&E) [Office of the Under Secretary of Defense, Research and Engineering] and Federal partners, will play a key role in the Department's effort in the implementation of 5G.

Turning to cyber, DOD released its 2018 Cyber Strategy this past September. The Cyber Strategy articulates how DOD implements the National Defense Strategy in cyberspace. DOD's CIO, working closely with DISA [Defense Information Systems Agency] and PCA, implements the DOD Cyber Strategy, in close coordination with the military departments and component CIOs. DOD CIO and PCA co-lead weekly meetings focused on cyber issues with the Deputy Secretary of Defense, military departments, and OSD [Office of the Secretary of Defense] principals present.

The Department has created the Cyber Top Ten, which help us to prioritize where and how we apply resources and innovation to execute our Cyber Strategy. The Cyber Top Ten focuses on remediation strategies for a complex cyber landscape, with components ranging from information networks to our cyber workforce and supply chain risk management, and beyond.

DOD CIO works closely with the Protecting Critical Technology Task Force to identify technical solutions to enhance protection of the defense industrial base. For the first time, DOD CIO is reviewing and certifying all IT budgets, which includes cyber, across the Department.

DOD CIO now has the authority to set and enforce IT standards across the Department. The Department's cyber workforce is critical to our mission success. Authorities provided by Congress, such as the Cyber Excepted Service, has allowed the Department to adjust existing personnel policies and to implement new policies that account for this dynamic need in an increasing important mission area. DOD CIO is working closely with the CMO to modernize business systems and to eliminate legacy networks, infrastructure, and applications.

In closing, I want to emphasize the importance of our partnership with Congress in all areas, but with particular focus on digital modernization and IT reform. I look forward to continuing to work with Congress in these critical areas. Thank you for the opportunity to testify this afternoon, and I do look forward to your questions.

[The prepared statement of Mr. Deasy can be found in the Appendix on page 49.]

Mr. LANGEVIN. Thank you, Director.

And, General, the floor is now yours.

STATEMENT OF BGEN DENNIS CRALL, USMC, SENIOR MILITARY ADVISOR FOR CYBER POLICY AND DEPUTY PRINCIPAL CYBER ADVISOR, OFFICE OF THE SECRETARY OF DEFENSE

General CRALL. Thank you, Chairman, Ranking Chairman, and members. I appreciate the opportunity to come here and talk to you a bit and answer your questions from an implementation or outcome side of this equation here in front of you.

So I am honored to lead the Office of the Principal Cyber Advisor's cross-functional team. This was put in motion in NDAA language back in 2014, section 932. And while that predates by a few years language in the 2017 NDAA, section 911, which gets after cross-functional teams writ large and encourages that in the Department, I think it meets the vision, or at least I hope it does, that Congress was looking at in a cross-functional team.

And I am going to say this with some measured enthusiasm, because while I am excited about what I would consider to be our launch point and where we are right now, there is a lot of really heavy lifting ahead. And the measure of our effectiveness is really yet to be proven, but I am optimistic that we are going to get to where we need to be. So it is a really good start for the team and getting after the strategy that was just mentioned.

So to the point, the cross-functional team is focused on outcomes. It doesn't do us a lot of good to have a Cyber Strategy or a Posture Review that shows gaps and not really have a means to close those gaps and show outcomes and improvement. That is what I am focused on 24/7, is the team looking at getting the outcomes and implementing the strategy and learning from that as we go through our process.

We are also taking a hard look at our measures of effectiveness. I have made comments before that I used to think that one of the hardest things to do in this line is to start new work. I have learned that it is to stop work that is currently in progress. So to make good decisions where maybe things have gone past their point of good investments, and the Department needs to be more

flexible to turn to those things which really pay bigger dividends. We are looking at all of those.

So, really, what is the recipe? Just very quickly, what makes, I think, our efforts unique this go-around than maybe what you have seen in the past. There are only a few ingredients, the first of which I would say is we have got really good team members. We are allowed to pick them, and they come from a good cross-section across the Department. And because we are looked at normally as not having a bias, because we have so much diversity in background, that we are normally a trusted entity that can defuse some of these problems and move the Department forward.

We have got a solid strategy, as Mr. Deasy mentioned. Strategies are only good if the lines of effort within them are actionable, that you can do them. Not just, you know, proclamations or really good statements you can pin to a wall or aspire to, but things you can actually measure your progress against. We have got a good strategy.

We also have a very good Posture Review. The gaps that are included in there are very honest and allows us to put resources against those gaps and really provide substance to the way that we are working and moving forward.

We also bring together all the stakeholders. We are at this table for a reason. Work very closely with the DOD CIO, the CMO, with CAPE [Cost Assessment and Program Evaluation], the Joint Staff, services. These aren't just tangential things or passing in the hallways but integrated into our planning efforts and daily battle rhythms. So we work just not with each other but closely with each other, which I think is important.

We also have great leadership within DOD. We have got an Acting Secretary of Defense who has been laser focused on this in his previous role and current role and who is performing the duties of the Assistant Secretary of Defense now that are really focused on a battle rhythm where we are in front of them at least in a formal meeting every other week, going through what our scorecards, our outcomes, challenges and successes are. So we have very close interest within the Department.

And lastly, I would say, and certainly not least, is the interest here in this body. Congress has done us well to establish the cross-functional team and put us on a good glide slope to achieve results. So I thank you for the language that we have in the NDAA, and also your staffers who are sitting in the back. I assure you this: They know what I do as well as I know what I do, because they have been in my office spaces, they have read through our work, they have seen our product and how we are moving forward, and they have been extremely helpful at keeping us on path.

So, with that, I thank you for the opportunity, and look forward to taking your questions.

[The prepared statement of General Crall can be found in the Appendix on page 60.]

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

And I thank our witnesses for your testimony. We will now go to questions. We are expecting votes around 2:30, so we are going to get through as many as we can and then we will recess and then we will be coming back.

As is the case with the full committee, the chair and ranking member are not on the clock, but it is up to us to keep ourselves in check. After that, we will recognize members according to seniority, according to who was here first at gavel.

So, with that, let me start on the Cyber Excepted Service. So obviously, we touched on this topic. I am glad you all have mentioned it. Congress created the Cyber Excepted Service for the Department of Defense to be able to hire a skilled and talented cyber workforce. I understand, though, that less than five individuals from your office are dedicated to implementation of this authority, which is significantly delaying utilization of new hiring authorities across the Department. So as I noted in my opening statement, the workforce is the pinnacle of IT reform, modernization, and assurance.

So, Mr. Deasy, I am going to go to you first. Can you please describe the resources your office has dedicated to implementation of CES and why not more dedicated—why we have more dedicated implementation authority that might be needed?

Mr. DEASY. So first off, so as General Crall pointed out, this is a very important tool set you gave us. I will tell you that as I dug into this, this isn't a case of the volume of people we need inside of my respective organization or working on General Crall's cross-functional team. This is about competencies that need to exist in them. This is a new way of doing business.

And, more importantly, the P&R [Personnel and Readiness] organization and the respective mil [military] services need to train up, I think, at a faster rate the people that they need to bring on board to actually accelerate Cyber Excepted Service. If you look at where we are today, as you pointed out in your opening remarks, U.S. Cyber Command, DISA, DOD CIO office is well on its way. Where we need to up the game and up the speed is inside the respective mil services.

Now, General Crall here is living this on the front line each and every day, in terms of how we are tackling this, so I respectfully would see if he would want to add any comments to this.

General CRALL. Thank you, sir.

I would add, sir, really to the point of your question, in our implementation experience thus far, we have identified inside the building, and I have a request that we are putting together now that will be making its rounds to Mr. Deasy here shortly, that asks for some more resourcing inside the building to get after unfolding this a bit faster. So that is one area, just to be blunt. We could do a little bit better inside the building to get after it, and I am articulating what those specific needs are. So that is forthcoming.

The second piece that we are looking at is for all the talk in implementation, one area that the Department is focused on that, again, we have got to pick up the pace a bit is in how we do security clearances. The onboarding process can be very frustrating. So while we might have four of the five elements of the recipe right in bringing people on, if we can't bring them on quickly because they are held up in the security clearance process, it is a potential that they lose some interest and we don't garner the result we are looking for. So there is an effort underway right now to get after both of those critical areas.

Mr. LANGEVIN. I am concerned about the slowdown with the security clearance process as well. And I know we are looking at alternatives, including using technology as perhaps a pilot project to see how the two would compare, using algorithms and data analytics to speed that process along more quickly. But I share your concern about the clearance process.

And I will be interested, General, to hear more about the resources that are requested to more fully implement the work that you are doing.

Ms. Hershman, has your office been able to utilize CES, and what is your perspective?

Ms. HERSHMAN. We have not to this point, so we don't have that perspective yet.

Mr. LANGEVIN. Why is that?

Ms. HERSHMAN. We are just actually about 6 weeks into managing the business systems piece.

Mr. LANGEVIN. Okay. Well, we are going to want to follow up with you on that and to see the degree you will be able to utilize CES.

To all of our witnesses, I mentioned in my opening statement, Congress has enacted major statutory changes regarding the position of CIO, CMO, and PCA over the years. How are such changes being implemented, and what challenges or overlap have been identified?

Ms. HERSHMAN. So Dana and I have from the very beginning worked very closely, primarily from the reform standpoint, but we have been able to come to an agreement on how the roles and responsibilities are bifurcated. In general, we as CMO manage all the business systems and the data pieces of the Department. The CIO manages the network.

If we use a little bit of a visual to describe this, if you picture walking into this room, you have lights, you have the microphones, you have the monitors that are working. CMO would own everything that you would see, the lights down to the plug, and then the CIO would manage from the outlet to all the wiring that is behind. We also have the data, non-weapon system data, but all the business data that feeds in and shares both of the organizations.

So Dana and I have worked closely together. He has been part of my Reform Management Group. We also meet regularly in one-on-ones to make sure that the roles, responsibilities, and so forth are clear. And to date, we are handling any exceptions. Not everything is always black and white. One of the, I shouldn't say issues, but topics that came up at an early point was, I think it was Microsoft Office, and we were wondering is that considered more of an application or is that more of a business tool.

So Dana and I work closely with our teams to manage by exception. We sit on each other's cross-functional teams. I am also a member of the CIO Cyber cross-functional team. They are members of our Defense Business Council, which reviews software applications and so forth and certifies them in terms of dollar and value. We also—I am trying to think on some of the other teams. My chief data officer meets regularly with his team. So we have formed a good partnership and, to date, haven't had any real issues.

One last thing that I will add that we have done with regard to reform, and it is something new that we have done with the fiscal year 2019 new year, is that it used to be that CMO was seen as the only one who owned reform. And this year, because many of my colleagues are responsible for implementation, we work closely with colleagues and partners like Dana where we share in the metrics and the outcomes of our reform efforts.

So, Dana, I would invite you to add.

Mr. DEASY. So specifically what I will talk about is the new authorities that kicked in as of January 1st this year, two types of authorities. One was I am now in a position to actually review the entire Department of Defense IT budget, which is at $40-plus billion. So we came up with a process this year to actually go through and look at the highest priorities, which you will hear us talk about today, and to identify where there are gaps or where there is full alignment around the execution towards that digital modernization strategy. I actually issued to the Secretary back at the end of January the first ever certified budget for the Department of Defense.

Second, the other part of that speaks to standards and frameworks. And we now have the authority to identify standards and frameworks. So far, I will actually say that I think that will probably be used by exception. If I have the right working relationships and we have the right alignment, my ability to have to use that right to actually overrule will hopefully not be the norm but will be the exception. To date, I have not had to actually execute that authority, as we have strong alignment on the digital modernization program activity. But at a point where we do need to do that, I will be sure to use that authority.

Mr. LANGEVIN. So the CMO mentioned governing by exception. How are we institutionalizing the CMO and CIO roles, respectively?

Mr. DEASY. I will start by saying that what we did was, as Ms. Hershman pointed out, there are growing pains any time you take activity and you split it across organizations. There is friction that occur. So we thought the right way to do this was to have our respective organizations sit down and literally map out what are all of the areas where you can step on and have cross activity.

We had a working team that went through that, and then at the end, she and I respectively signed a memo that describes the activity set that is going to be done by my office and the activity set that will be done by her office.

Mr. LANGEVIN. Is that something that you can share with us? Would that be appropriate?

Ms. HERSHMAN. Yes. Actually, we have that going through final signature and review now.

Mr. LANGEVIN. Okay. The thing is, we are really interested in to make sure that this all works well together, and that we want to get our heads around whether this is, you know, not just personality-driven, but it is process-driven, that we have this more institutionalized, if you will. So that the next people that will be occupying your roles, again, it is not personality-driven, but it is actually institutionalized going forward, and we take best practice or we take the best out of the work that you are doing and make sure that there is continuity.

So I am going to have additional questions, and it looks like we are going to votes right now, but I will turn to the ranking member for questions, and hopefully we can get through her questions and then we will recess after that.

Ms. STEFANIK. Thank you, Chairman Langevin.

I wanted to build upon your question, and also expand on your opening testimony, Ms. Hershman. You very clearly outlined the disparate, fractured, and duplicative nature of our current IT and business systems environment. We have more than 1,800 business systems across the portfolio, thousands of data centers, hundreds of cloud efforts, some 65 CIOs, and a total budget of almost $42 billion per fiscal year.

With all of these complications in terms of the Department's overall strategy to reform this area, what does this need to look like 5 years from now? And equally as important, how do you intend to get there?

Ms. HERSHMAN. What it is to look like 5 years from now is actually very difficult to project, only because of the changing nature of both technology and how we do business. What we all can agree on is that this needs to be less complicated so it is easier to manage, not only from a—you know, from using the systems within the organization, but also to ensure that data that flows through these multiple systems is also properly protected.

So one of the things that we have done is certainly align these initiatives with how it supports our National Defense Strategy. We also, from a reform perspective, are looking at what will create the biggest impact, create the greatest value, and what is the timing? In fact, some of these initiatives, we are taking a very different approach, in that we are not necessarily waiting all the way to the end of the project to produce results. We are actually taking iterative, prototype, minimum viable product type approaches to start deliver and test as we continue to go through the program or the project.

So we also have used—I was a—the CMO was a cosponsor for the comptroller's audit. We are using audit findings to also help inform reform. So those are just some examples of how we are collectively looking at what is most important, where are our biggest risks, what are our biggest vulnerabilities, and how can we mitigate or solve those problems, and are ordering or reordering our initiatives accordingly.

Ms. STEFANIK. Let me ask you about the efficiencies and cost savings that you talked about. Do you expect the cost of a modernized and efficient IT and cyber budget to remain at approximately $42 billion per year?

Ms. HERSHMAN. It is difficult to answer that question on the expectations for the budget, only because we are working with what we know now, and there are always new opportunities or new issues that could pop up. So I can't really speak to the budget and cost.

Ms. STEFANIK. Okay. And my final follow-up. Mr. Deasy, do you have anything to add? I would like to get your perspective on what this needs to look like 5 years from now. How do we get there? And the budget question, in terms of do we anticipate this costing $42 billion per year?

Mr. DEASY. Yeah. I would say that if we look at the emergent technologies, such as cloud, AI, modernization of C3, and what we are going to have to do to secure the Department of Defense, I think the question really is one of are we getting the most out of every dollar, not if $42 billion is right. It may be in the future that the Department of Defense budget, from an IT standpoint, actually needs to go up for what it needs to do for the business. To me, the real question is, are we getting the most out of every dollar? So that I would say is kind of part one to your question.

Two, what does the world look like in the future? I envision it a world where every new application will be cloud first. When we are going to look at consolidation of business systems, we will take the opportunity as we migrate on the cloud to do standardization and consolidation of business systems. We will use that opportunity to start using data management in a much more joined-up common way. And we will use things like AI robotics to actually help us deliver a much more efficient—back to my first question of how do you deliver a much more efficient budget.

Ms. STEFANIK. Thank you. I yield back.

Mr. LANGEVIN. Okay. So votes have been called. We will recess until about 5 minutes or so after votes.

So, with that, the subcommittee stands in recess.

[Recess.]

Mr. LANGEVIN. The committee will come to order.

Again, I want to thank our witnesses for testifying here today. Sorry for the delay getting restarted, but we are going to go now.

The gentlelady from Pennsylvania, Ms. Houlahan, is recognized for 5 minutes.

Ms. HOULAHAN. Thank you, Mr. Chairman.

Thank you so much to all of you for coming. I have a few questions for you. The first one is to Ms. Hershman. I was wondering a little bit about the capabilities of our domestic manufacturing. Twenty percent of our memory chips are only made in this country and the rest come from international sources. And I was wondering if you had any concerns that we need an organic source, a domestic source of these kinds of manufacture of these kinds of chips, to make sure that we are secure with the work that you do and also for business in general.

Ms. HERSHMAN. I would say, in general, we share your concerns. However, my role does not deal with that directly, so I will defer to Mr. Deasy or Mr. Crall.

Ms. HOULAHAN. Thank you.

Mr. DEASY. So do I believe that we need a domestic supply chain for key chip? Absolutely. All you have to do is look at things like 5G. And the need to have an industrial base in the U.S. where we can get secure technologies such as what you are referring to is something I think we need to focus more on, yes.

General CRALL. Ma'am, I wouldn't add any more to that.

Ms. HOULAHAN. So the following question is, what sort of legislative help can we as a Congress provide to you so that we can enable that to happen?

Mr. DEASY. I would tell you, I am not sure I am the right expert, being the CIO, to tell you what the policy requirements and how best that we legislate that. I would be happy to get the people en-

gaged inside the Pentagon that would be best able to address that particular question.

Ms. HOULAHAN. Thank you. My next question has to do with small businesses. In addition to being a veteran, I am also an entrepreneur. And we know that small businesses play a really critical part in our defense industrial complex, and they are obviously mostly supply chain-related in most cases. And they are largely fairly inadequately prepared to deal with issues of cybersecurity as they are growing or starting up.

And so my question is, how is the Department working with entities like small businesses and up and down the supply chain to make sure that cybersecurity practices and IT systems are protected from the threats that we know exist and that larger companies are capable of handling?

Mr. DEASY. So I share this concern. When we start talking about small businesses at what I will call tier two, tier three down in the supply chain, they don't have the wherewithal, the financial wherewithal, nor the knowledge domain expertise wherewithal at the sophistication levels of tier one.

A couple things that we are looking at in this space is, one is how do we use the NIST [National Institute of Standards and Technology] Framework and how do we take that framework to help educate the tier two and tier three in a way that is more effective for them to use. Two is, I am a firm believer in that we need to develop an independent standard, kind of like what we have for CMMI [Capability Maturity Model Integration] for development or ISO [International Organization for Standardization] 9000 for quality. I think this needs to be developed. I think if we could get this developed in this country, this would actually help better educate and focus small business on the talent they would then need to hire.

I think the last thing is we are looking at how do we use technology that we are starting to put in place maybe at cloud technology that would allow us, instead of passing data to them and then them having to secure it, how could we keep the data on our own premises and they could connect into it. So that is another thing that we are evaluating.

Ms. HOULAHAN. Excellent. Thank you very much.

And the last question I have is that my understanding from our briefings here and then also at the NSA [National Security Agency] is one of the biggest vulnerabilities for all of us employees, regardless of where we work, is spear-phishing attacks. And I am wondering what you have done to make sure that you are holding people accountable, if you are holding people accountable, for these kind of mistakes; and are there any practices that we can adopt from the accountability for individuals—are there best practices that we can adopt from accountability from individuals that you have found effective?

Mr. DEASY. Yeah, I will be happy to take that. So coming from private industry, one of the stats that we know exists out there is if you look at all the vulnerabilities that get created, both inside government as well as private industry, it is human error still tends to be the number one cause of the vulnerabilities. And at the top of that list is spear phishing or just general phishing.

To that end, I think best practices that I have seen in private industry have been around training programs where you actually create test-phishing campaigns. You use those. You actually then phish a set of employee base that you want to start with. And it is real time, because what comes back to them is the fact that they have just been phished. They get educated in real time on what they are seeing in that email that would have shown them the attributes of what a phishing looks like. And then you follow through with a round two, and you reach a point where if someone continues to fail, then you take other actions, which would include increased training.

Ms. HOULAHAN. Wonderful. Thank you.

I yield back. Thank you.

Mr. LANGEVIN. I thank the gentlelady.

Mr. Scott is now recognized for 5 minutes.

Mr. SCOTT. Thank you, Mr. Chairman.

And I appreciate the Department's total force perspective and using all facets of civilian and military forces to get ahead of our adversaries. We have granted new hiring authorities for Cyber Excepted Services, direct hire authority, and pay adjustments in salaries.

How far are we along with the implementation of this? And are there other barriers that are holding you back from recruiting and training the right people? If so, how do we intend to overcome these barriers? How are you working with universities, ROTC [Reserve Officers' Training Corps] programs to create a conduit of new talent for this career field? And what additional resources do you need from Congress in the way of either language in the National Defense Authorization Act or other forms of legislation to assist you in this field?

General CRALL. Sir, I would be glad to take that question. And I appreciate the scope that you just framed that, because those are really kind of a mixed bag for us on areas that I would say—and I will cover them—that I think we are doing better in some and not so well in others.

So I would like to take a look at really our target audience. The Department—and I have testified on this before, that the Department has to do a better job, and we are looking at ways to ensure we understand the market properly. In many cases, we think we know where we should be recruiting, and we may not be recruiting to the level that we should.

So understanding the type of applicant that we are searching for and the needs of those applicants, we need to bolster our understanding a little bit better. So we are looking at a way to kind of package that.

I think your comments are spot on on internships, for example. We do too few of them. Academia has proven their willingness to work with us, and as a department, we have just got to really take advantage of those where it makes sense. We have several of these near our bases that would be attractants to these things, and we are still underutilized.

I think on the ROTC front, we are doing a little bit better. And I realize that may not be a detailed or satisfying enough answer, but we are addressing that. And I talk to the services about how

they run their programs, and it is clearly an area of interest in the college environment.

But the last piece I would say is our biggest challenge, and we have covered this a little bit earlier today and I would just reemphasize it. Rolling this out at a level that is sufficient I think is a fair criticism where the Department has to do better. So the phase one of the Cyber Excepted Service was modest by design of under about 500 billets that we put out, to make sure that we knew what we were doing. Were we trained properly? Could we track those individuals properly?

And you are right, Congress has given us a lot of enhancements, from pay to direct hire, et cetera. This next phase, which we are in right now, is going to bring that exponentially higher in number. And the resources in the building are lacking for us to both internally and then at the service level to make sure we can handle that workload, and we are addressing it.

Mr. SCOTT. And when you say resources, do you mean money? Do you mean physical resources?

General CRALL. People, sir.

Mr. SCOTT. People.

General CRALL. Which could be viewed as money.

Mr. SCOTT. Sure. Yes.

General CRALL. But looking at people, to dedicate the right number and the mix to get after this at scale. And that scale has to change for us to meet pace.

Mr. SCOTT. Okay. Anybody else like to comment on that?

Mr. DEASY. So having spent most of my career in private industry, I would say that one of the problems is a whole-of-government issue we have to address, and that is most cyber people never come across government in their career. They just don't touch it. They don't intersect with government. What does that mean? That means when they are thinking about progressing their career and taking that next step, they don't stop to have a conversation with themselves saying, well, what about an opportunity of doing a career inside of government?

And I think that is one of the things that we in the DOD need to step up and address, but I think others are going to need to address as well is, how do we create exposure that even lets the average person in private industry even know what the opportunities could look like for them in government? Because once we do bring these people in and we expose them to the mission, they get pretty excited about it, but it is how do we create a better avenue of awareness I think is part of what we have to address.

Mr. SCOTT. I have only got about 30 seconds left, but you brought something up on the periphery of it has been on my mind. This issue where several employees of a company that we contract with did not want to push forward with the contract because it was a DOD contract.

I am very concerned about how few companies there are out there that are actually good in these fields that we are talking about. And when you have a small group of select employees, their ability to create problems with that contract and their perception of DOD I think is very wrong. I mean, it was the Department of Defense that went to Africa when we had the outbreaks of poten-

tially contagious diseases. I mean, we are in the business of helping people.

And I do hope that—I know you are paying attention to it and interested in further conversations about the private sector and the challenges there with select groups who do not want to work with us. But thank you for your time.

Mr. LANGEVIN. Thank you, Mr. Scott.

Before I go to Mrs. Trahan, General, if I could just follow up with you on Mr. Scott's question. You answered and you talked about resources you need, and you said people. Can you help the committee understand the amount of people we are talking about in numbers? Is it 10? Is it 50? Is it 100? Ballpark it for us. Not to hold you to that, but we are trying to get our arms around this as well, and your perspective would be helpful.

General CRALL. Yes, sir. So my evidence behind my number I am just going to admit is a bit sketchy. But to do service to your question, the Department had looked at having between five or six people full time to do the initial planning and rollout, which, again, was kind of modest.

So my ballpark estimation would be at least that number of 5 or 6 and likely something closer to the order of 10 internally if we are dealing with thousands that need to be, you know, brought in and the training that is required, because they have to travel to some of these places to make sure that training takes place and it is understood well. So that would be my ballpark estimate, sir.

Mr. LANGEVIN. That doesn't seem like a significant increase over what—so that seems to be eminently doable. You are talking about an additional number of people that are needed?

General CRALL. It does seem that way, yes, sir.

Mr. LANGEVIN. So which office needs to provide those resources?

General CRALL. Sir, I think that would come across several offices potentially to do that. And I am not an expert, but I think the requirement for that that I am piecing together, I am trying to answer that question now to submit to Mr. Deasy. So to be fair, he hasn't received my request, but I think that will rest with him eventually, and we will have to look within the Department as to where the resources come to get those hirees.

Mr. LANGEVIN. Okay. I appreciate it. Your candor is very helpful and it helps us to understand the scope of the challenge and what we need to do to get this right.

With that, let me recognize Mrs. Trahan from Massachusetts for 5 minutes.

Mrs. TRAHAN. Thank you, Mr. Chairman. Thank you.

You mentioned the opportunity in government and how some folks in the private sector don't even entertain that possibility. Given the recent shutdown, what is the value proposition? What is the—how are we going to attract and retain the best and the brightest from everything from MIT [Massachusetts Institute of Technology] to competitive community colleges to help us tackle this problem?

Mr. DEASY. So it is clearly the mission. And let me bring it to life through an example. We run a yearly competition where universities compete on a cyber challenge, and then we bring the winning university in for a day into the Department of Defense. And

in that, they get a chance to meet with my office. They get a chance to meet with several of the principals, the COCOMs [unified combatant commands], the military side. And by the end of this day, every single one of them says the same thing: I had no idea just how amazing it could be to do this sort of work if I had not had the opportunity to come in and spend a day and just get exposed and talk to people and hear firsthand from the people out in the field why cyber matters.

So I cannot stress the importance enough for a lot of young people if they never get exposure, they never talk to someone in uniform, they are just not going to put in the forefront of their mind coming and working for the DOD.

Mrs. TRAHAN. That is helpful. And are these employees that we are attracting, do they have that label essential/nonessential associated with them? How would they be affected by a potential shutdown, for example?

Mr. DEASY. I am not sure I could—I would have to look into the specific nature of how they are classified and come back and answer that.

Mrs. TRAHAN. That is great. I am interested in knowing what the consequences are when we shut down the government, how that is actually going to affect our cybersecurity strategy.

But I will shift gears. The success of our—I believe I just read something where you were quoted, Mr. Deasy, that the success of our AI initiatives relies on robust relationships with industry, with our allies, certainly with academia, to meet the needs of speed and agility specifically. What role do our allies play in that?

Mr. DEASY. So interesting enough, I just had a conversation with our Five Eyes CIOs just yesterday on this very topic. I would say, right now, we are clearly in the leadership role. And I think the biggest role that we are going to play is help to educate them and help them to understand what it took for us as a Department of Defense to establish a Joint Artificial [Intelligence] Center capability, as they are all looking to establish a like capability. So I think our role will be one of leadership and how we went about doing this.

Mrs. TRAHAN. Great. Thank you.

I yield back.

Mr. LANGEVIN. Thank you, Mrs. Trahan.

I recognize Mr. Waltz now for 5 minutes.

Mr. WALTZ. Thank you, Mr. Chairman.

I just wanted to thank you all for coming, by the way. And, General, I wanted to pick up, or, Mr. Deasy, on your comment about human capital and the challenges that you are having with human capital. What role do you see the Guard and Reserve playing in there?

It seems to me if there is any entity that flows back and forth between civilian and uniformed or even government service, it would be the Guard and the Reserve that can kind of, one, stay current on the civilian side as technology paces so quickly, but then flow back in as they come in and off of orders. Where do they fit in the broader strategy?

General CRALL. Sir, you know, the question is timely. We just had a chance to take the team down to Augusta, Georgia, and talk

to a lot of the units that are down there that are practicing this. And the Guard and Reserve is really a staple of the conversation, not an add-on. So a lot of the Guard and Reserve units are extremely active, very competent, cutting-edge technology trained, and a very integral part of what we do.

So I can't comment onto the adequacy, you know, if we are doing enough or not enough, but I know that many of those Guard units have quite a bit of operational time under their belt as well. So very proficient, very impressive. And we use them regularly, not just in their activated time periods, but in their civilian period as well.

And I would admit, I don't believe that is limited just to cyber. I think that is pretty common. In my, you know, noncyber experience in the Marine Corps, we have been augmented in almost every MOS [military occupational specialty] that I can think of by Guard units and Reserve units who have performed brilliantly.

Mr. WALTZ. Fair enough. But I would think that it would be quite unique to cyber, right, or at least the technology field, right? So you could have where that civilian skill set then is so—I can't think of anywhere else that on the civilian side is outpacing the military from a technological standpoint.

General CRALL. Well, maybe, sir, because here is an area where it depends on what kind of mission we are talking about. So if we are talking about defensive missions and those individuals have experience doing kind of our protection type of work possibly. On the offensive side, I would argue that I think within the military, that capability, it is really the only legal place you could do some of that work. And that allure is there. So it would depend on the skill set.

Mr. WALTZ. Fair enough. Switching gears to JEDI, and apologies if you have already answered some questions along these lines, but just talk to me about how critical JEDI is. How critical is the success of JEDI and other DOD enterprise cloud initiatives in supporting future AI?

And along those lines, then what are the—I am assuming you are going to say it is critical and you are going to tell me how critical. But then what are the drivers or delays to implementations, and what are we losing as implementation is delayed?

Mr. DEASY. So not specific to JEDI, but just what are the critical benefits. So what is the problem set we are trying to solve for inside the Department of Defense? Number one is if you look at what it takes today to stand up compute capability from the time that a service or a COCOM sees a need to the time that you bring the assets inside the Department, test them, stand them up, make them operational, that is a multi-month period.

Benefit number one of cloud is the ability to purpose and stand up compute capability in literally hours. So you solve for how do you solve for episodic needs where you need to stand up compute capability. That is very important, as you can imagine, to the Department.

Two is when we build capability today inside the Department, we always have to think about peak need. So you buy enough necessary hardware for that peak capacity. The second beauty of cloud is called elasticity. You ramp up and scale more compute as you

need it; and as you don't need it, you can scale it down, and it happens in real time.

The third one is resiliency. The idea with the cloud is that if you write your application from day one to be cloud native, you get built-in resiliency. As it finds itself in an unhealthy condition or as it finds itself needing to use other resources, it has the intelligence to do that. In a world where we can't have a not fail mission set, the resiliency, as you can imagine, becomes mission-critical.

Mr. WALTZ. What are we losing as this moves forward? I mean, I understand the process is moving forward, and——

Mr. DEASY. Yeah.

Mr. WALTZ [continuing]. You are not going to get into protests and, you know, all of the industry issues.

Mr. DEASY. No.

Mr. WALTZ. But what are we losing as this——

Mr. DEASY. The biggest thing we are losing right now is—the Department of Defense needs to bring data and integration together. It has been a constant conversation; it is not a new conversation. Our enterprise cloud, for the first time, allows us to establish a common platform where we can bring data together in a common way.

What will happen is, the longer we delay standing up a JEDI capability, you are going to—the military services are going to need to go solve for mission sets, and they are going to continue to stand up in their own individual environments. And I don't see that as being beneficial over the long term to the Department.

Mr. WALTZ. Thank you, Mr. Chairman. I have exceeded my time.

Mr. LANGEVIN. Okay. Thank you, Mr. Waltz.

We are going to go to a second round of questions now.

So, following up on the JEDI issue, obviously this is a big deal for the Department, something Congress is following very closely. I have been frustrated that we haven't moved it along more quickly.

But, Mr. Deasy, just last week, news reports emerged about a potential conflict of interest related to the JEDI program. It would be an understatement to say that I was frustrated that the subcommittee and our staff had to learn about the development, from what we understand, through a presser rather than from Department staff.

You know, given the significant congressional attention to the effort of ensuring that the transition of cloud is successful, we really do expect and anticipate better communication from the Department moving forward on this issue. And I wanted to ask for your commitment to improving communication with Congress to prevent a surprise issue like this happening again.

Mr. DEASY. Absolutely.

I will take it that I did not get back to you in as timely of a way as we should have. We were walking a very fine line between an ongoing conversation with the Department of Justice around what we could say and we couldn't say. We got the clarity on a certain day this last week, and as soon as I got that clarity, I called.

We did put a holding statement out to the press, but I wanted to be able to share with further clarity beyond the holding state-

ment with you. And that is what I was waiting to get from the Department of Justice.

Mr. LANGEVIN. Okay. Well, good communication and——

Mr. DEASY. Absolutely important.

Mr. LANGEVIN [continuing]. Timeliness is essential. And I would appreciate your commitment to doing that.

So, on this topic, again, the Department recently identified more than 300 cloud initiatives across the Department. So how does JEDI relate to those initiatives?

Mr. DEASY. We believe that inside those 300 initiatives are what I will call general purpose cloud computing, meaning that many of those initiatives do not need what I will call a unique cloud stack but they can be best served through something referred to as JEDI. And then we have some that sit inside there that are truly going to need what we call fit-for-purpose or unique cloud capability.

Until we can get a direct line of sight as to how soon we will be able to stand up a general purpose cloud capability, obviously, the cloud initiatives need to continue. As soon as we know within line of sight of what I will say is probably within 60 days of when we think we will actually be able to go live, then we will be able to go back to some of the early portions of those cloud initiatives, where they are still in the early days, and redirect them. That is our intent.

So the fine line we are walking right now is not to impede the need for mission success where people are standing up on the cloud, but as soon as we can provide clarity to the DOD on when the enterprise cloud will be available, to then redirect those activities onto JEDI.

Mr. LANGEVIN. So your best guess in, you know, the world of cloud, what percentage do you think are unique, specific to each of the departments, and what are more common, what percentage is going to be more common in cloud?

Mr. DEASY. Yeah, the way I like to have this conversation is, it depends if we are talking legacy or what I like to refer to as brownfield or if you are talking greenfield, new applications that need to be written.

I am a strong believer that the vast majority, probably 85, 90 percent, of all things in the future that we were to build could go onto either a fit-for-purpose or a general purpose cloud.

So then that begs the question, what about the world of all the applications you have today? Many of those applications, just the sheer cost and the magnitude of lifting them and reporting them onto the cloud would be cost-prohibitive, would be time-prohibitive, and would probably not serve the Department well.

So what you really have to do is you have to then go through your legacy estate based on the cloud we are eventually going to stand up—and that is actually a key statement—based on what it is we are going to stand up, and then be able to start targeting what would the services look to do what is called a report, where they are going to rewrite the application, or a lift and shift, where they are going to take the application and bring it over as is and put it onto the cloud.

So there are various ways we can move over. But the big thing hanging out there right now is, until we know what that architec-

ture in that cloud is going to look like, it is very difficult to start estimation exercises.

Mr. LANGEVIN. Okay.

And, Ms. Hershman, from your perspective on business systems, what capabilities will JEDI bring to reform? And how does the chief data officer you recently hired intend to utilize JEDI, and how is he working with the CIO on data management?

Ms. HERSHMAN. So, yes, sir, that it does have a big impact on what we are doing in CMOs. Mr. Deasy explained that it has an interrelationship with data.

So Mr. Conlin, our chief data officer, does work with Mr. Deasy and his team. We were very fortunate in that Mr. Conlin comes from industry and also has a cyber background, which makes him a very unique find.

What I also am struggling with, similar to my colleagues here, is those hiring authorities. While previously, before the business systems role, we had not looked purely at IT but just from a data management standpoint, we too have difficulty with the hiring.

There isn't—there are two—actually, there are two pieces to that. Number one is there isn't a single data scientist position description anywhere in government. So that is one thing that we need to refine and improve. We have also come under some challenges with hiring data scientists. All of industry is also looking for the same talent type.

So, while previously you asked me about the CES, we were looking more to align with hiring authority and the compensation freedom that an organization like DARPA [Defense Advanced Research Projects Agency] is able to have, which is why we are now looking at the CES to see if that applies to us.

So both from a reform standpoint and also to be able to support JEDI and what we need to contribute from a data standpoint, those resources are becoming very critical.

And just to anticipate what you had asked General Crall earlier as well, when we are talking numbers, we are also looking for just single digits.

Mr. LANGEVIN. Okay. Good to know. That is helpful for us to understand. Thank you for that.

The last question that I will have, and then I want to turn to the ranking member. General Crall, from your perspective, how would JEDI improve or impact cybersecurity efforts? And will cyber protection teams [CPTs] have the appropriate accesses to a commercial cloud if there is a security issue?

General CRALL. Yes, sir. I think, one, I am probably not best suited to talk about the CPT's accesses. I think U.S. Cyber Command would be in a better position to do that. And I can certainly take that back, sir, to give you a—to have them respond with a direct answer to the question.

[The information referred to can be found in the Appendix on page 67.]

Mr. LANGEVIN. Okay. So how do you, in your work, interact with the cyber protection teams?

General CRALL. So I would say maybe the first part of your question talked about my work and how JEDI might impact that would be maybe a more appropriate question for me to answer, sir. And

I will start with that and then come back to the second piece, if you are amenable to that.

Mr. LANGEVIN. Sure. Yes.

General CRALL. What I think would be a real help to us, when we start looking at how applications behave and what it means to get an authority to operate on the distant end, how do you move something through the system from design so that, secure and hosted, it really streamlines the ability and implementation in our strategy to get to our end state much faster.

We spend a lot of time at the service level doing some activities that are less than desirable, somewhat antiquated, and expensive to try and make up for what a cloud environment could provide us. So from a security implementer, for pieces of that cybersecurity strategy, that is a game changer for us.

Mr. LANGEVIN. Very good. Thank you. And then the other part of it?

General CRALL. Yes, sir. I think I would like to come back to you, again, on the CPT.

And my work specifically with CPTs, I am part of a team in a composite that looks at readiness. So when we start looking at readiness levels across the Department, that really has been my focus on both CMTs [combat mission teams] and CPTs, as Cyber Command continues to drive at setting those standards. We take a look at translating those standards into the way that we can evaluate those teams against those readiness metrics.

So I play a small role in that process within the Department to ensure those standards are clear, published, and we are driving to them.

Mr. LANGEVIN. Fair enough. Thank you.

I now yield to the ranking member for as much time as she may consume.

Ms. STEFANIK. Thank you.

General Crall, can you expand upon DOD's top 10 cyber priorities from the Cyber Strategy? I know we have an unclass [unclassified] slide here that I don't think we have gone over today.

And then if you could answer, which of the priorities do you anticipate will be the most difficult?

[The slide referred to is for official use only and retained in the committee files.]

General CRALL. Yes, ma'am.

So the cartoon graphic that you have in front of you really kind of lays out the areas that do have our focus. And maybe the takeaway from this is, I understand it is imperfect, right? It is two-dimensional. It is meant to be read linearly, maybe left to right, when, in fact, some of these things appear in many parts of our network. But it is just a simple way to frame what we are talking about.

If you look at the gold box of network and information-sharing, that is where some of the immediate efforts we have, even here in fiscal year 2019. And those callout boxes in gray and blue describe in the areas of endpoint management, identity, our enterprise development operations, and our cyber workforce where they have the attention of the Department.

So the way that we are looking at this—and maybe the takeaway is, if you pressurize one set of this or if you try and handle security or effectiveness or functionality in one end, then you depressurize something else, and that is where your risk is going to come. So it is important that we look at this holistically.

And I will say, the CIO is certainly geared to describe that relationship as he is driving this as an enterprise to make sure that we are paying attention to every one of these parts.

To answer your second question about what do you think is the most difficult, I would answer "yes" to that question. There is nothing easy on this slide at all. And maybe to take a look at maybe increasing levels of difficulty, I will say that scale and scope of some of these are really daunting tasks. So I wouldn't want to pick any out in particular.

But I know the members are very familiar with 1647 and 1650, weapons systems and critical infrastructure. That is a pretty big lift in the Department.

Having to modernize our encryption, that is a very heavy lift that is extremely complicated that not only goes to the central repository of how that encryption is designed and disseminated but all the way to the tactical devices that we use on the battlefield. So it is a wide, very complex problem.

Position, navigation, and timing, again, would be another challenge.

Those things that appear to the right-hand side, that tactical edge, probably affect the force in volumes and ways that we are still getting our arms around.

I don't know if that is a satisfying answer, ma'am. But that is what I——

Ms. STEFANIK. It is helpful to outline a little bit the thinking behind this slide. I think the other members of the committee, we will share that with them.

My next question is for Mr. Deasy.

Can you provide this committee with specific updates and specific initiatives from the Joint AI Center—in particular, the national mission initiatives and also added component mission initiatives?

Mr. DEASY. So, as you know, we received towards the end of last year our initial funding to stand up JAIC. We now have our initial billets in from the services side as well as the civilian side.

We have identified two national mission initiatives right now. One of them is in the predictive maintenance space, and one is in the humanitarian space. So let me take you through each of those.

What we were looking for when we talk about a national mission initiative is something that touches all services, a common problem they are looking to solve for, and, most importantly when it comes to AI, access to data that is meaningfully available. Because if you think about AI, AI needs data. You are ingesting that data, and then you are running it through a machine-learning algorithm, and then you are coming out with, hopefully, an operational output.

Predictive maintenance was, if you think of the amount of money we spend inside the Department of Defense just on maintenance, we broke out maintenance and we said: Aircraft, significant amount.

We said, what is an asset that we are using that all services use that have common problems with maintenance? We looked at the Black Hawk, the UH–60 [medium utility helicopter]. And what we found was, if you look at engine wear in conditions where there is a great deal of sand out in desert conditions, that turns to glass. And so what if we could do a predictive analytics to go in, teach a machine to look at all that sensor data coming off of those vehicles, and be able to start to predict in advance of when the glass condition is occurring so you could actually repair it in advance?

So that is the one we are working on right now. That is the first NMI [national mission initiative] on the predictive maintenance side.

The second one, the humanitarian side, was we wanted to look at one that had a whole-of-government where we could take a leadership in. And we said there was two significant conditions that are occurring. One was if you look at the hurricanes we had this past year, and one was if you look at the wildfires that occurred out in California. So let's take each of those.

On the wildfire one, what is the problem you are trying to solve there? You are trying to solve for the fire line, where it exists. And what if you could take imagery instead of the human asset having to go out, visually look at the fire line, but actually use artificial intelligence to look at the fire line, determine where it is moving, and be able to overlay that onto a handheld device that a firefighter is using?

Hurricanes. The other example there is hurricanes cover a large, vast area. So can we use imagery over a large, vast area to determine where the flooding is occurring, how high the flood waters are, and whether there is human risk space or other types of assets in a risk space? So, once again, we are going to use the imagery data to be able to look at risk space.

Why are those both important to us? Because the algorithms that we will develop to intelligently learn fire lines are the algorithms we will develop to intelligently learn a better way of looking at flood, is we will be able to apply that to other mission sets inside the Department of Defense.

That is the value of JAIC. The value of JAIC is to take those algorithms that are developed for purpose A and then be able to reapply them elsewhere inside the Department of Defense. So we think we will be able to reapply those algorithms elsewhere.

Ms. STEFANIK. So just to follow up on the reapplication of those two national mission initiatives, you know, one of my greatest concerns when we think about emerging threats is China's investment in AI capabilities and China's investment in data, that this is a strategic priority.

My question is, do you believe that those two identified national mission initiatives will ensure that we not just keep pace with how China is investing in AI but we will be able to catapult how we are approaching AI not just from DOD but from a whole-of-government approach?

Because my concern is that, while those are two very important issues—predictive maintenance and humanitarian assistance—that scope is quite limited when you look at the scope of China's investment utilizing AI for part of its defense strategy.

Mr. DEASY. So, of course, those in themselves aren't going to solve for what you are bringing up. We are going to need a series of national mission initiatives.

As I pointed out, we just literally started this up in late December, and here we are now in February. I think the fact that we have been able to stand up an initial set of billets with two NMIs in approximately 60 days says volumes to just how smart and quickly we are working this.

But to your very point, we are going to need a number of national mission initiatives in different areas.

I think part of the thing that you are probably getting at is also vis-a-vis where China is; you know, do we have the ability to outpace them. I think Dr. Portis said it best in a testimony that I did with her recently. China may be at a level of investment where we compare to ourselves as quite significantly higher, but if you look at the vast talent, the U.S. still holds the majority of the talent when it comes to AI. And what we have to do is we have to learn how to quickly leverage and bring that talent in.

Which is why I am so passionate about the need that JAIC has to connect to the academia world and to the private-sector world. Because our success is going to require those partnerships to go well beyond two NMIs.

Ms. STEFANIK. And another question regarding the JAIC. In previous testimony, we have heard about the hundreds of AI initiatives with the DOD. How, specifically, are those individual AI missions or initiatives being integrated into the overall strategy from the JAIC?

Mr. DEASY. Right now, there is not a significant amount going on inside of JAIC to integrate those individual projects. Where that integration will take place—and it goes back to Mr. Waltz's question earlier—is going to be how do we stand up an enterprise cloud capability where all of those individual projects can benefit.

Cloud itself does not do a whole lot; it is what you put on top of it that matters. And what we need to put onto that cloud is data. And data is what is going to drive the success of a lot of our AI initiatives across the Department of Defense.

I have been asked many times what will slow us down, and what will always slow us down is our access to data, our ability to quickly integrate that data, and then to turn that data into something that we can then apply machine learning.

Ms. STEFANIK. Yeah. No, I understand, Mr. Deasy, the importance of cloud and the importance of data in terms of the fuel when it comes to AI. But my question—and I am going to continue asking these tough questions of the Department—is, when we are creating a Joint AI Center and we are failing to integrate the hundreds of other AI initiatives within the Department, that is of concern here, because it means that we are not looking at this from a whole-of-department approach.

Again, I understand the connection to moving to the cloud, to access to data, but we need to continue pushing the Department when it comes to how we are addressing AI, because I am fearful we are falling behind our adversaries in terms of how they are addressing this.

I want to ask a budget question as it relates to AI. We know that AI is a very shiny object. And if we label everything as AI, it is going to exponentially increase cost.

So how are you dealing with this initiative and identifying true AI capabilities that the Department will need, in terms of your fiscal year 2020 budget request?

Mr. DEASY. So we are working closely with the various components and the services on defining the categorization for AI.

I want to point out that we are not ignoring 300. We are learning how to quickly get a flywheel going of how to bring in and integrate these initiatives. And I cannot stress that our flywheel is about 60-some days old now and we are integrating at a rapid rate.

What we want to be able to do is to take all of those initiatives and define which of them are actually, truly NMIs and how can we better integrate those in the JAIC.

And then the real question is, where they are not national mission initiatives and they are actually individual components, we have set up a requirement that if they are of a certain dollar value they need to go through JAIC, they need to be validated by JAIC to ensure that they are being set up the right, successful way. So JAIC will intersect with CMIs that exist out in the services when they hit a certain dollar threshold.

Ms. STEFANIK. Okay. Thank you.

I yield back.

Mr. LANGEVIN. I thank the ranking member.

So just a last couple of questions, if I could.

Going back to the discussion on cloud, Mr. Deasy, I just wanted to say, so a fit-for-purpose cloud obviously can only be pursued with an exception from the CIO's office. Do you have an estimate of how many exceptions you are going to issue?

Mr. DEASY. Earlier, there was a question asked about the ongoing 300-plus cloud initiatives, and I pointed out that one of the things we need to do is to go through and take a determination of how many of those are more general purpose versus what will be truly fit-for-purpose. That is something we still have to do.

Right now, obviously, our focus is to make sure we know what the architecture is going to look like for our general purpose, which will help inform us on things that will stay fit-for-purpose or move over. So it would be really inappropriate for me—I would be surely guessing as to a certain percentage or a number of those 300 that will be migrated onto general versus fit-for-purpose until we understand the overall architecture.

Mr. LANGEVIN. Okay.

And the last question I had for you, Mr. Deasy and for the panel: After CES phase two is unveiled and implemented, will there be a petition process for DOD components to participate in CES, such as the case of Ms. Hershman and the data scientist?

Mr. DEASY. I think I understand the nature of your question as taking Cyber Excepted Service and how do we expand it to beyond. So I will tell you right now, we are already using those authorities on how we are approaching AI. We are going to need to use those authorities, clearly, when it comes to things like data scientists.

So one of my asks back to Congress is to continue to help us on how we take the great work we have done with CES and think

about other technologies that we are going to be confronted with and we are going to want to leverage inside the Department and be able to use the goodness of CES beyond its original cyber intended purposes.

Mr. LANGEVIN. Okay. But there will be a petition process within——

Mr. DEASY. Yeah.

Mr. LANGEVIN. Okay. Very good.

That is all I had at this point. Anything from the ranking member?

Okay.

So, in closing, let me just say, if I could, Mr. Deasy—and I appreciate the work that you and all of you are doing on these important topics.

If I could just mention, I think that the approval request for resources, if they can move quickly to implement the Cyber Excepted Services, those requests, they are approved quickly—it doesn't seem like a large number of people we are talking about—that would be helpful to move things along more effectively. But I leave that to you to work out, and we will be following up with this closely.

I really do thank all of you for your testimony and for the work you are doing. I look forward to following up further at either hearings or briefings.

But, with that, if there are no further questions, the committee stands adjourned.

[Whereupon, at 4:21 p.m., the subcommittee was adjourned.]

A P P E N D I X

FEBRUARY 26, 2019

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

FEBRUARY 26, 2019

Opening Statement
Chairman James R. Langevin
Intelligence and Emerging Threats and Capabilities Subcommittee
Department of Defense Information Technology, Cybersecurity, and Information Assurance

February 26, 2019

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 status, its modernization efforts, and its strategic direction for the foreseeable future. Our witnesses today are Ms. Lisa Hershman, the Acting Chief Management Officer (CMO), Mr. Dana Deasy, the Department's Chief Information Officer, and Brigadier General Dennis Crall, the Deputy Principal Cyber Advisor (PCA).

The Defense Department's IT architecture is as important to the mission as the weapons platforms that our service members employ. We cannot expect the services to maintain combat superiority if the technology that we rely on is deficient, outdated, insecure, or inoperable.

IT should never be considered a back-office function, as it may have been in previous eras. The challenge of managing the Department's IT is highlighted best by the sheer number of topics we will be hearing about today including cybersecurity, business systems, Artificial Intelligence, data management, JEDI, and the Cyber Excepted Service.

IT reform and modernization require appropriate stewardship by the Department's leaders, many of whom are seated here today. Over the past several years, Congress has endeavored to ensure that the Department is structured in a way that gives senior leaders the authorities they need to carry out their responsibilities.

For example, Congress created and elevated the position of CMO and gave that individual the responsibility for business systems. Additionally, Congress provided new standard setting and budget authorities to the CIO that took effect at the beginning of the calendar year. All of this was done with an understanding that the PCA also has a critical role to play with respect to cybersecurity of such systems.

Given how dynamic the IT space is, it's reasonable for this subcommittee to continually take stock of how the Department is implementing statutory changes and whether the outcomes match Congressional intent.

For this reason, I am eager to hear from the witnesses how the new roles, responsibilities, and authorities are being implemented and whether any of the changes made in recent years ought to be modified further. This includes

discussion of the resources dedicated to the office of the PCA and coordination mechanisms.

In addition to organizational changes, the Department is taking positive steps towards embracing new technologies. Initiatives such as the Joint Artificial Intelligence Center and the Joint Enterprise Defense Infrastructure cloud initiative seek to capitalize on emergent technologies with significant potential benefits for the Department. This subcommittee is invested in the success of these efforts, if managed correctly, and with an understanding of how these high dollar investments at the OSD level coincide with efforts by the services and agencies, such as the other 300-plus cloud computing initiatives.

Success for the Defense Department in the IT space is predicated not only on the software and hardware that we buy and maintain, but equally on the workforce that we employ. The Pentagon cannot succeed in this new era if we are not recruiting and retaining the best workforce.

I am pleased that the workforce is consistently raised as a priority issue and flagged as a one of the premier lines of effort in the DoD Cyber Strategy. The competition for talent in this space is fierce, which is one of the reasons Congress created the Cyber Excepted Service (CES), a personnel system built specifically to attract top tier talent with competitive salaries. The DoD CIO was designated as the Department's lead in crafting this new personnel model.

To date, CES has only been implemented at U.S. Cyber Command, Joint Forces Headquarters DoD Information Networks, and DoD CIO Cybersecurity. Today provides us an opportunity to ensure the appropriate resources are dedicated to swift implementation across the Department.

Finally, I remain concerned about cybersecurity across the Department. While we have made significant progress in securing the DoDIN, particularly as U.S. Cyber Command matures, the theft of DoD data from contractors and the security of weapons systems themselves are both challenges we must address. Congress has taken steps in recent years to evaluate the risk posed by our DIB supply chain, but I will be interested to hear more how the CIO's office is leveraging its position and expertise to take more steps to mitigate this risk.

I look forward to hearing from our witnesses how they are posturing the Department for success.

I'd like to now turn to Ranking Member Elise Stefanik for any opening comments she'd like to make.

Statement of Hon. Elise Stefanik, Ranking Member,
Subcommittee on Intelligence and Emerging Threats and Capabilities
Hearing on
Department of Defense Information Technology, Cybersecurity,
and Information Assurance

February 26, 2019

Thank you Chairman Langevin. And welcome to our witnesses here today. Since this is our first open hearing of the 116th Congress, I would like to take a moment to congratulate my friend and colleague Jim Langevin on his Chairmanship of this important subcommittee. As many of you know, IETC has a strong bi-partisan tradition and I look forward to working again alongside Jim.

During the last Congress, we explored how emerging technologies are changing the nature of warfare and we legislated aggressively in the areas of Artificial Intelligence, quantum sciences, and other related technologies.

So – I am pleased that this year we are starting with an open hearing on Information Technology, cybersecurity and information assurance – all of which are of the same continuum towards enabling the military and forming the backbone of the battlefield of the future.

I have said in the past that too often the Pentagon has treated information and communication technologies as a support tool, secondary to platforms, weapons, training and operations within the Department. But anyone who has seen our forces operate over the past 25 years understands that our military advantage comes from networked and secure systems proving Intelligence, precision-strike, information fusion, and advanced warning capabilities that our warfighters have come to rely on.

This military advantage, however, is at risk of eroding – and some would argue has already eroded – when we consider advances that have been made most notably by Russia and China.

All DOD missions and systems remain at risk from adversarial cyber operations. The Department continues to discover mission-critical vulnerabilities in acquisition programs, and uncover massive breaches of cleared defense contractors. Indeed, across the Department we still struggle with incorporating agile software-enabled systems that remain relevant, and keep pace with the hyperconnected, digital world of today.

Considering this, our hearing today in a larger sense is about continuing to build the foundation for the future of warfare, where information and data are a strategic resource to be protected, preserved and fully enabled.

IT modernization, cybersecurity and information assurances are primary prerequisites for this future, and the Department must achieve fluency in these areas as we consider evolutionary – and indeed revolutionary – leaps towards other enabling technologies such as AI, 5G, high performance computing and even quantum computing.

Given the challenges I just mentioned, I fear that we are not on strong footing; and one need also only consider the fits and starts with the Department's evolution to a modern Cloud computing environment. The Department's legacy approach to Cloud computing has been fractured and uneven; and as DOD considers a more strategic and holistic strategy – one that I fully agree with – the trajectory is mired by legal disputes that all but guarantee further delays.

These are delays we cannot afford given the rapid pace of technological advancements – as well as adversarial advancements, since China and others continue to transform their militaries, increasingly surveil their own citizens, and advance authoritarian and undemocratic objectives.

Make no mistake: In the areas of IT reform and digital modernization, I support the vision and direction being outlined by the CIO, Mr. Dana Deasy who is with us today. Nonetheless, we continue to have tough questions regarding Cloud computing and the JEDI project that still dominates the headlines. So, I look forward to discussing today exactly how the Department's move to commercial Cloud fits in with IT reform and digital modernization.

Each of our witnesses plays a central role and forms an important partnership in ensuring that DOD has modern information and communications technologies, as well as the policies and standards needed to support the Department's many missions.

I am pleased to see that Lisa Hershman, the Acting Chief Management Officer of the Department, is with us here today. When we consider IT reform and the importance of delivering optimized enterprise-wide business management solutions for the Department, we quickly gain an appreciation of the trusted partnership that must exist between the Chief Management Officer and the CIO. I look forward to hearing about this partnership, and how both the CMO and CIO are collaborating with the Department's new Chief Data Officer, to manage the complexities of data management, and provide a Common Enterprise for Data across the Department.

Lastly, the importance of the Principal Cyber Advisor cannot be overlooked, and I am pleased to welcome back Brigadier General Dennis Crall, the Deputy PCA, before our subcommittee. The PCA's roll in synchronizing, coordinating, and overseeing the implementation of the Department's Cyber Strategy is renewed again since DOD recently released an updated Cyber Strategy in September of 2018, and completed a comprehensive Cyber Posture Review directed by this committee. With action being taken on DOD's "top 10 cyber priorities" and "first four" efforts, I look forward to hearing more today about the important progress being made.

So, thank you again to each of our witnesses.

UNCLASSIFIED

Embargoed until release by the

House Armed Services Committee

Testimony

Before the

House Armed Services
Committee, Intelligence,
Emerging Threats and
Capabilities Subcommittee

Department of Defense
Information Technology,
Cybersecurity, and Information
Assurance

By

Ms. Lisa W. Hershman

Acting Chief Management

Officer

Department of Defense

February 26, 2019

Testimony of Ms. Lisa W. Hershman, on Department of Defense Information Technology, Cybersecurity, and Information Assurance to the House Armed Services Committee, February 26, 2019

Thank you Chairman Langevin, Ranking Member Stefanik, and other members of this subcommittee for the opportunity to testify today on the Department's information technology (IT), cybersecurity, and information assurance. I am Lisa Hershman, the Acting Chief Management Officer (CMO) of the Department of Defense (DoD). I would like to begin today's hearing by outlining my roles, responsibilities and priorities, the Department's aggressive work to reform and modernize business operations through IT and business systems change, and the monumental changes in our management of data throughout the enterprise.

As the Acting CMO, it is my responsibility to deliver optimized business operations and shared services to assure the success of the National Defense Strategy (NDS). This responsibility is only made possible by the elevation of the CMO as the third in the Department and the critical authorities granted by you and your colleagues in the National Defense Authorization Act (NDAA) of Fiscal Year (FY) 2017. This law provided the CMO authority to direct the Principal Staff Assistants, Military Services, Combatant Commands, and remainder of the Defense Agencies and DoD Field Activities with regard to business operations.

My goal as Acting CMO aligns directly with the intent of the NDAA: efficiency for lethality. Efficiency for lethality is defined as reforming the Department's business processes, systems, and policies to gain increased effectiveness, higher performance, and reprioritized resources. Integrity and consistency of every measure is a cornerstone of our approach. I appreciate the work of the Office of Under Secretary of Defense for Comptroller (USD(C)) and the Military Departments for actively partnering to define standards for reform in execution and validate our efforts in the budget. Because of this effort, the Department has realized a total of $4.702 billion in programmed savings in FY17 and FY18, indicative of the success in reform efforts executed to date. However, reforming the business operations of the Department must not only be focused on financial savings, but also creating a sustainable, cultural impact. Through reform I aim to establish a culture of continuous improvement focused on results and accountability.

The Department's priorities of reform are based upon the framework defined by the FY19 NDAA, the President's Management Agenda, the senior leader Reform Management Group (RMG), and the first DoD-wide financial audit. While our reform efforts continue in the areas of civilian resource management, acquisition management, real estate management, logistics and supply chain management, contract management, and healthcare management, the President's Management Agenda, the RMG and the audit and identified business operations, IT infrastructure,

business systems, and data management as the most significant opportunity for improvement.

Our current IT and business systems environment is extremely complex. The Department currently maintains hundreds of business systems with ad hoc interconnectivity, thousands of data centers, hundreds of cloud efforts, and dozens of thousands of applications, with an IT and cyberspace budget of nearly $42 billion in FY18. These systems and infrastructures are managed by 65 Chief Information Officers (CIOs) throughout the Department with varying goals and performance metrics. This type of disparate management and duplication makes it extremely difficult for us to deliver an effective, innovative, or secure IT environment.

As the CIO for defense business systems in accordance with the FY18 NDAA, I consider it my responsibility to reverse this environment. I am developing the defense business systems strategy to ensure the development of integrated business processes through the Defense Business Enterprise Architecture. It is imperative to ensure the execution and enterprise management of business reform and associated business IT, and I am actively executing this in close coordination with Mr. Dana Deasy, the CIO.

We are executing IT reform efforts through several initiatives in four major areas. We are converging networks, service desks, and operation centers into a consolidated, secure, and effective environment capable of addressing current and future mission objectives. We are transitioning the Department to a cloud-enabled future, while standardizing IT commodity applications through commercial industry capabilities to deliver modernized services. We are unifying the Department's collaboration capabilities into a commercial cloud-enabled service. We are also modernizing coalition information sharing capabilities used by the Department and allied mission partners supporting global operations.

I would like to call your attention to the necessity of conducting business operations and systems reform. Despite the best efforts of software manufacturers, business systems represent a significant vector of cybersecurity vulnerabilities, from the business systems themselves to the supporting middle ware and operating systems. The number of vulnerabilities is a direct result of the sheer variety of software vendors, packages, releases, updates, patches, and configuration parameters which is then multiplied by the volume of software instances in use. The Department's sprawling portfolio of more than 1,800 business systems represents an uncomfortable level of exposure to cyber vulnerabilities.

In addition to these vulnerabilities, the Department historically under-invests in the modern tools and techniques for IT configuration management and IT asset

management, which are well proven as cybersecurity best practices in the commercial sector. These same business systems produce data that is of lower quality - less complete, less correct, less current, and less consistent - than what is ideal. In industry, high quality data is well established as a leading measure of high quality business systems, cybersecurity maturity, and business performance.

At a minimum, the Department's business systems should be operating at the same level as the commercial sector, if not higher. It is therefore imperative that we reform our business systems.

We are executing business systems reform by eliminating redundant systems, maximizing shared service delivery, and streamlining business operations. Through our initiatives we have made progress toward simplifying the IT landscape, reducing operational costs, through greater use of industry-proven enterprise services, and enabling business process integration.

As an example of our efforts in business operations and system reform, I would like to call attention to our Defense Civilian Human Resource Management System (DCHRMS) initiative. Through this initiative, we are aggressively driving change in how we manage the employee records of our civilians. Civilian job transfers within the Department occur roughly 40,000 times per year, with new employee records created each time an employee transfers. These records have been managed

by six separate systems that independently maintained the personnel records of our civilians. Through this reform initiative, the Department has rationalized policy and business processes to enable the consolidation of the six systems into one, cloud-based, software-as-a-service Human Capital Management capability. DCHRMS will be the first, single, authoritative, employee record system for all of our 900,000 civilians. DCHRMS will eliminate the unnecessary steps taken by human resource employees to create new employee records during transfers, and free up our human resource employees to focus on critical business deliverables, such as reducing time to hire. Most importantly, this consolidation will ensure a single, secure personnel record with one authoritative data source for all actions, removing hundreds of local copies of data yielding a material improvement in our cyber posture.

This initiative and others like it may seem commonplace when compared to the Department's operational missions, but are key enablers as we reduce duplication and inefficiency within the headquarters operations to achieve greater lethality and readiness.

As we execute these reforms, we remain ever mindful that the goal is delivery of secure, relevant, clean data to support both warfighting and business decisions, while IT infrastructures and business systems act as mere vehicles by which data travels.

The Department's historic operating environment poses many challenges to success in achieving this goal. The Department has traditionally been faced with a data analytics talent shortage, poor data quality, little to no data analytics policy, immature data analytics infrastructure, a complex data security environment, and outdated technology architectures for data analytics.

These challenges have not gone unrecognized by the members of the Armed Services Committees, and I want to personally thank you for supporting the data needs of the Department through the FY18 NDAA. This law provided the CMO with the framework to establish common enterprise data and data management and analytics as a shared service. To ensure data management had the full dedication it requires, I hired the Department's first Chief Data Officer (CDO), Mr. Michael Conlin.

The goal of establishing a CDO for the Department was not only to implement common enterprise data and data management and analytics as a shared service, but to create a lasting data-driven ecosystem. As outlined in my "Implementation Plan for Common Enterprise Data," this will require investments in people, processes, technology, and governance, and it will occur in four phases.

In the first phase of implementing common enterprise data, we began to understand the maturity of the Department's current data environment though pilot programs.

These pilot programs have allowed us to develop a repeatable business insight approach, implement proof of concept for the enterprise data analytics technical architecture, deploy a repository for common enterprise data, and define the data governance system.

To deploy a repository for common enterprise data, the CDO worked in conjunction with the Office of the USD(C) to develop the Defense Repository of Common Enterprise Data (DRCED) to be the shared-service platform for all common enterprise data. The DRCED is organized by a domain-oriented approach to include data management, audit findings, financial management, cost management, performance management, and readiness insights.

To define the data governance structure, the CDO established the Data Management and Analytics Steering Committee as the principal data governance body. This governance body is comprised of the chief management and financial officers of the Office of the Secretary of Defense, Military Departments, the Office of the Director of Cost Assessment and Program Evaluation, the Office of the CIO, the Office of the Principal Deputy Assistant Secretary of Defense for Readiness, and the Joint Staff J8 for Force Structure, Resources and Assessment.

We are now in the second phase of structuring and institutionalizing the Department's enterprise data governance and enterprise shared service analytics

capabilities. This includes developing a data science analytics training and career ladder, developing processes to maintain an enterprise data catalog and inventory, deploy artificial intelligence and machine learning, and developing the Department's Enterprise Data Strategy.

In the third phase, we plan to resolve organizational conflicts and eliminate differences in data approaches, leading to higher levels of constructive collaboration toward Department-wide goals. This norming phase includes establishing processes for integrated enterprise performance, cost, and budget reviews, completing automated cross domain security solutions, implementing data quality improvements, and accelerating the hiring of data scientists.

The fourth phase of this implementation will demonstrate the Department's ability to continually improve through a data-driven performance culture embedded in the business and mission processes. The Department will develop a performance evaluation assessment for the execution of the Department's Enterprise Data Strategy, and establish interoperability standards across lines of business.

In sum, the implementation of common enterprise data will provide the Department improved data management practices, improved data security, an established analytics infrastructure to acquire, store, and analyze data, and enhanced enterprise decision-making throughout the Department. Through these efforts the end state of

our data environment will be a Department that makes decisions based on accurate, timely business data as opposed to internal boundaries and past experiences. This is a monumental shift in the way the Department conducts its business operations, and I am committed to ensuring the priority of data management in my role.

As Acting CMO and CIO of defense business systems, I am committed to leading business operations for the Department through innovative processes and services, data driven solution, and mission focused funding. It is imperative to our mission that we increase cybersecurity, modernize and standardize business processes, and decrease duplication of IT services throughout the Department. While I maintain this responsibility for data and business systems, I rely on my counterparts here with me today to be accountable. I entrust Mr. Dana Deasy as CIO to continually decrease duplication of IT services, and Brigadier General Dennis Crall as Deputy Principal Cyber Advisor to increase cybersecurity as an advocate for the implementation of the Department's Cyber Strategy.

Thank you for the opportunity to outline my roles, responsibilities, and priorities, and provide details of our work in reforming the Department's IT, business systems, and data management. I welcome your questions.

Lisa W. Hershman
Acting Chief Management Officer
Department of Defense

Ms. Lisa W. Hershman is currently acting Chief Management Officer of the Department of Defense. Ms. Hershman has been serving as the Deputy Chief Management Officer of the Department of Defense.

Ms. Hershman is a recognized thought leader in business transformation who brings extensive private sector expertise to her service in the Department of Defense. She is the principal management officer for the Secretary and Deputy Secretary of Defense responsible for delivering optimized enterprise business operations to assure the success of the National Defense Strategy.

Ms. Hershman is responsible for ensuring that business transformation policies and programs are designed and managed to improve performance standards, efficiencies and effectiveness among the Office of the Secretary of Defense (OSD), the Services, Combatant Commands, and Defense Agencies and Field Activities. Additionally, she oversees the collection and management of common, enterprise-wide data sets to drive best decision-making throughout the Department.

Ms. Hershman is a charter member of the Office of Management and Budget's (OMB) Performance Improvement Council, and serves as the Performance Improvement Officer for the Department of Defense. She also serves as the Cross-Agency Priority goal leader for Category Management and Workforce of the 21st Century in support of the President's Management Agenda.

Prior to her service to the Department of Defense, Ms. Hershman was Founder and CEO of The DeNovo Group, a business transformation and process management consultancy. She is the former CEO of Hammer and Company, serving as the successor to the late Dr. Michael Hammer; the MIT icon, best-selling author and founder of the field of business process reengineering. Ms. Hershman is co-author of the internationally acclaimed business book, Faster Cheaper Better, with Dr. Hammer and has been featured in BusinessWeek, Forbes, Fox Business News, and Investors Business Daily.

In addition, Ms. Hershman served as Senior Vice President of Operational Excellence at Avnet, a global distributor of electronic components and technology systems. As the executive in charge of transformation and customer experience in 72 countries, her work was honored with the Avnet Corporate Chairman's Award. Ms. Hershman began her career with General Electric, where she managed a portion of the Seawolf submarine program.

Her civic engagement includes serving as the 2017 Chairwoman of the Scrum Alliance, Vice Chair of the Indiana Commission for Higher Education, and as a member of Ball State University's Miller School of Business Entrepreneurial Education Advisory Council.

Ms. Hershman earned her engineering and industrial distribution degree from Clarkson University and has studied innovation with MIT and IMD and finance with Cornell.

STATEMENT BY

DANA DEASY

DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON INTELLIGENCE AND

EMERGING THREATS AND CAPABILITIES

ON

"DEPARTMENT OF DEFENSE INFORMATION TECHNOLOGY, CYBERSECURITY,

AND INFORMATION ASSURANCE"

FEBRUARY 26, 2019

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 Dana Deasy, the Department of Defense (DoD) Chief Information Officer (CIO). I am 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 nuclear command, control, and communications (NC3) matters. These latter responsibilities are clearly unique to the DoD, and my imperative as the CIO in managing this broad and diverse set of functions, is to ensure that the Department has the information and communications technology capabilities needed to support the broad set of Department missions. This includes supporting our deployed forces, cyber mission forces, as well as those providing mission and business support functions.

Today, I would like to highlight key areas of the Department's digital modernization and IT reform efforts now underway. First, I will provide a general overview of the Department's cloud strategy, including the Joint Enterprise Defense Infrastructure (JEDI). Then I will provide an overview of our artificial intelligence (AI) strategy, including the standup of the Joint Artificial Intelligence Center (JAIC). Regarding command, control, and communications (C3), I will briefly highlight the important work underway regarding 5G and spectrum management. I will touch upon several key elements in the area of cybersecurity, which directly impact each of the key areas of digital modernization. Finally, I will focus in on some details of our IT reform efforts.

Cloud

Earlier this month, the Department submitted its cloud report and strategy, in accordance with Congressional requirements. As stated in that submission, DoD will remain a multi-cloud environment with both general purpose clouds and fit-for-purpose clouds as part of the long-term cloud strategy. DoD's scale and complexity of missions require multiple clouds from multiple vendors. This initiative is part of a larger effort to modernize information technology across the DoD enterprise. A modern digital infrastructure is critical to defending against cyber-attacks as well as enabling machine learning and artificial intelligence. As outlined in the cloud strategy, moving the Department to a cloud environment will enable greater computing power at greater speed and allow for the flexibility required to meet warfighter requirements at the tactical edge.

The Joint Enterprise Defense Infrastructure (JEDI) is one of the multiple cloud efforts the DoD is pursuing to enhance lethality and strategic readiness, while enabling the warfighter to respond at the speed of operations. As I have discussed with some of you previously, it is a pathfinder, general purpose, enterprise-wide cloud. JEDI will enable DoD to learn how to implement an enterprise cloud solution, take advantage of economies of scale, and enhance data-driven decision making. JEDI will be the foundational for leveraging artificial intelligence and machine learning and contribute directly to the modernization of command, control, and communication (C3) systems.

Another key component of our cloud strategy are fit-for-purpose clouds. In situations where a general purpose cloud solution is not capable of supporting mission needs, the Department may use a fit-for-purpose commercial solution. As further described in the Cloud Strategy, these situations are specific, narrowly focused cloud initiatives that address requirements that cannot be supported by a general purpose cloud. When mission needs cannot be supported by a general

purpose cloud, a mission owner will be required to submit for approval an exception brief to the DoD CIO describing the capability and why the general purpose cloud service does not support their mission. Fit-for-purpose clouds, where approved and allowed, will always enhance the DoD cloud environment and not be a detriment to it.

Artificial Intelligence (AI)

The National Defense Strategy makes clear that the character of warfare is changing. Competitors, like Russia and China, are investing heavily in modernization and artificial intelligence to redefine the future of warfare. To maintain and increase our competitive military advantage, DoD must do the same. Last June, the Department delivered its classified AI strategy to Congress. Two weeks ago, shortly after the President signed the Executive Order on AI, we released our unclassified summary of the classified DoD strategy. The DoD AI strategy contains four key points: 1) it emphasizes the need to increase the speed and agility with which we deliver and adopt AI-enabled capabilities; 2) the value of establishing a common foundation to enable decentralized development and experimentation; 3) the importance of evolving our partnerships with industry and academia; and 4) the Department's commitment to be a global leader in the safe, lawful, and ethical use of AI technologies. The Department's strategic approach emphasizes the rapid, iterative delivery of AI and importance of using lessons learned to create repeatable processes and systems that will improve effectiveness and efficiency across the enterprise. DoD will work with partners from across the Interagency, Industry, Academia, and the international community on AI missions that support DoD's ability to ensure our nation's security.

The Joint Artificial Intelligence Center (JAIC) is the focal point for carrying out the DoD AI strategy. JAIC will accelerate DoD's delivery and adoption of AI to achieve our global mission, while attracting and cultivating a world-class AI team. It was established last June under the office of the DoD CIO to provide a common vision, mission, and focus to drive Department-wide AI capability delivery. JAIC is charged with the task of accelerating and scaling the use of AI across the DoD, with emphasis on near-term execution. The ultimate goal is to use AI to solve large and complex problem sets that span across multiple services, relying on an enterprise cloud-enabled common foundation to provide shared data repositories, reusable tools, frameworks and standards, and cloud and edge services.

The AI efforts of the JAIC and the Office of the Undersecretary of Defense for Research and Engineering (OUSD(R&E)) will complement each other. OUSD(R&E) will provide foundational AI research and technologies that JAIC can transition to the operational environment. In turn, the JAIC will provide operational AI insights and user results to inform OUSD(R&E) focus areas. The AI Strategy refers to National Mission Initiatives, or NMIs, and Component Mission Initiatives, or CMIs. NMIs are broad, joint, cross-cutting AI challenges that the JAIC will orchestrate using a cross-functional team approach. CMIs are specific to individual components, who seek AI solutions to a particular problem. The components will run those projects, but the JAIC will support them in a number of ways, from funding, data management, common foundation, and integration into programs of record.

Command, Control, and Communications (C3)

The emergence of digital technologies has introduced new challenges to the traditional C3 landscape. In order to take advantage of new digital capabilities and to protect our warfighters from corresponding weaknesses, we must modify and modernize our C3 systems.

C3 must enable the right communications, at the right time, to protect and enable the warfighter.

All U.S. military services, in one form or another, are beginning to transition to the concept of multi-domain operations, which requires the seamless integration across land, air, sea, space and cyber. The ability of our C3 systems and forces to exchange information and communicate effectively gives our warfighters the best capabilities to deliver the fight tonight. With new approaches, and emergence of digital technologies, victory in future conflict will in part be determined by Joint and Coalition forces' ability to rapidly share information across domains and platforms.

In order to facilitate economic growth while providing national security, DoD CIO, working closely with USD(R&E), the Federal Communications Commission (FCC) and the Department of Commerce (DoC), will play a key role in the Department's efforts in the implementation of 5G telecommunications. As the primary federal user of spectrum, we must help guide effective implementation of the "Presidential Memorandum for Developing a Sustainable Spectrum Strategy for America's Future." DoD must become a key innovator in spectrum sharing technology and policy, while leveraging mutually dependent C3, cloud, cyber and AI technologies, to gain and maintain an advantage over our competitors. DoD CIO has been working closely with Federal partners and Industry through the Wireless Innovation Forum to share spectrum, and accommodate both broadband and naval radar operations in the 3550-3650 MHz band. The Department has been a key participant in shaping this innovative spectrum sharing framework.

Cybersecurity

DoD released the 2018 Cyber Strategy this past September. As aligned with the National Cyber Strategy, the Department of Defense Cyber Strategy articulates how DoD implements the National Defense Strategy in cyberspace, describes how the Department aims to compete, deter, and win alongside allies and partners in cyberspace, and directs DoD to defend forward, shape the day-to-day competition, and prepare for war.

As I testified before the Senate Armed Services Committee, Subcommittee on Cybersecurity last month, the DoD CIO, working closely with the Defense Information Systems Agency (DISA) and the Principal Cyber Advisor (PCA), implements the DoD Cyber Strategy in close coordination with the Military Departments and other DoD Component CIOs. DoD CIO and PCA co-lead bi-weekly meetings focused on cyber issues with the Deputy Secretary of Defense and all of the Military Departments and Office of the Secretary of Defense (OSD) Principals present. These meetings ensure that the Deputy Secretary of Defense is kept abreast of progress on cyber initiatives and that all Department leaders are present to receive direction and share challenges. Additionally, DoD CIO also works closely with the Protecting Critical Technology Task Force to identify technical solutions to enhance protections of the Defense Industrial Base (DIB).

The Department has created the "Cyber Top Ten", which helps us to prioritize where and how we apply resources and innovation to execute our Cyber Strategy. The "Cyber Top Ten" focuses on remediation strategies for a complex cyber landscape, whose components range from information and networks, to our cyber workforce and supply chain risk management, and beyond.

For the first time, DoD CIO is reviewing, commenting on, and certifying all of the IT budgets, which include cyber, across the Department. DoD CIO's Congressionally mandated

responsibility to certify the Military Departments' cybersecurity investments and efforts enables me to ensure the Department is pursuing enterprise cybersecurity solutions that are lethal, flexible, and resilient. DoD CIO now has the authority to set and enforce IT standards across the Department. Standards are not limited to the technical standards developed by the commercial sector and organizations like the International Standards Organization. Standards include setting the bar for cybersecurity requirements, such as endpoint security standards and standards for architecture, and DoDIN standards.

The Department's cyber workforce is critical to our mission success. The authorities provided by Congress have allowed the Department to adjust existing personnel policies and to implement new policies that account for this dynamic need in an increasingly important mission area. One key authority being the establishment of the Cyber Excepted Service (CES). By fostering a culture based upon mission requirements and employee capabilities, CES will enhance the effectiveness of the Department's cyber defensive and offensive mission. This will provide DoD with the needed agility and flexibility for the recruitment, retention and development of high quality cyber professionals.

Information Technology (IT) Reform

DoD CIO is working closely with the Chief Management Officer (CMO) to achieve a modernized and effective force through DoD-wide IT reform activities. These activities are being established to implement, consolidate, and streamline capability delivery to support an evolving mission environment.

Establishing a consolidated and converged IT infrastructure drives efficiencies across the Department, and provides opportunities for reductions in acquisition overhead, an increase in combined purchasing power, and the utilization of shared expertise across the DoD environment. Refocusing IT manpower initiatives towards an increase in experience and skillsets, coupled with automation improvements, provides a reduction in labor resources that can be aligned to support emerging mission areas. Standardizing and modernizing the IT environment eliminates unnecessary systems, and allows the DoD to focus finite cyber resources across fewer areas, ultimately shrinking the Department's cyber threat attack surface.

Several key reform efforts are underway. First, Network and Service Optimization Reform will converge DoD networks, service desks and network/service operation centers into a consolidated, secure, and effective environment capable of addressing current and future mission objectives. Second, Cloud & Data Center Optimization Reform transitions the DoD to a cloud-enabled future. Enterprise Collaboration/IT Tools Reform converges and transitions the DoD collaboration capabilities into a unified commercial cloud-enabled enterprise service. Finally, License Consolidation Reform negotiates improved terms and conditions with commercial vendors, prioritizes IT spend across the department, and standardizes purchasing processes.

Conclusion

I want to emphasize the importance of our partnerships with Congress in all areas, but with a particular focus on digital modernization and IT reform. The increased authorities that have been granted to the DoD CIO with each National Defense Authorization Act are one key example of this partnership. Continued support for a flexible approach to cloud, AI, C3, and cyber resourcing, budgeting, acquisition, and personnel will help enable success against an ever-

changing dynamic threat environment. I look forward to continuing to work with Congress in these critical areas. Thank you for the opportunity to testify this afternoon, and I look forward to your questions.

Dana Deasy
Chief Information Officer
Department of Defense

Mr. Dana Deasy is the Department of Defense Chief Information Officer (DoD CIO). He is the primary advisor to the Secretary of Defense for matters of information management, information technology, and information assurance, as well as non-intelligence space systems, critical satellite communications, navigation and timing programs, spectrum, and telecommunications.

Mr. Deasy previously held several private sector senior leadership positions, most recently as Global Chief Information Officer (CIO) of JPMorgan Chase. There, he was responsible for the firm's technology systems and infrastructure across all of the firm's businesses worldwide. Mr. Deasy managed a budget of more than $9 billion and over 40,000 technologists supporting JPMorgan Chase's Retail, Wholesale and Asset Management businesses. He has more than 35 years of experience leading and delivering large scale IT strategies and projects, to include Chief Information Officer and Group Vice President at BP.

Earlier in his career, Mr. Deasy served as CIO for General Motors North America, Tyco International, and Siemens Americas. He also held several senior leadership positions at Rockwell Space Systems Division, including as Director of Information Management for Rockwell's space shuttle program.

He was inducted into the CIO Hall of Fame in 2012 and the International Association of Outsourcing Professionals Hall of Fame in 2013 and also named Transformational CIO in 2017.

STATEMENT BY

BRIGADIER GENERAL DENNIS A. CRALL
U.S. MARINE CORPS
SENIOR MILITARY ADVISOR FOR CYBER POLICY
DEPUTY PRINCIPAL CYBER ADVISOR

ON BEHALF OF THE DEPARTMENT OF DEFENSE

TESTIMONY BEFORE THE
HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON
INTELLIGENCE, EMERGING THREATS, AND
CAPABILITIES

ON

"DEPARTMENT OF DEFENSE INFORMATION TECHNOLOGY, CYBERSECURITY, AND INFORMATION ASSURANCE"

FEBRUARY 26, 2019

NOT FOR PUBLICATION UNTIL
RELEASED BY THE HOUSE ARMED SERVICES COMMITTEE

Good afternoon Chairman Langevin, Ranking Member Stefanik, and Members of the Intelligence, Emerging Threats, and Capabilities Subcommittee. Thank you for the opportunity to testify before the Subcommittee regarding our combined partnership in achieving the Department's information technology (IT), cybersecurity, and information assurance efforts. I appear before you today in my roles as the Senior Military Advisor for Cyber Policy and the Deputy Principal Cyber Advisor to the Secretary of Defense.

As provided in Section 932 of the National Defense Authorization Act for Fiscal Year (FY) 2014, the Principal Cyber Advisor (PCA) serves as the civilian Department of Defense (DoD) official who acts as the principal advisor to the Secretary of Defense on the Department's military and civilian cyber forces and activities. The Office of the PCA (OPCA) synchronizes, coordinates, and oversees the implementation of the Department's Cyber Strategy and other relevant policy and planning documents to achieve DoD's cyber missions, goals, and objectives. At the core of the OPCA is the Cross Functional Team (CFT) of detailees from the Military Departments, Services, and Defense Agencies. The CFT provides an objective and broad perspective needed to ensure that outcomes match short- and long-term approved, strategic visions. To meet increasing demands outlined in the DoD Cyber Strategy Lines of Effort (LOE) and the DoD Cyber Posture Review's gap analysis, the Deputy Secretary of Defense has made a substantial investment in the OPCA, adding permanent billets including an OPCA Deputy for long-term continuity.

The OPCA executes the DoD Cyber Strategy, including by addressing the gaps identified in the DoD Cyber Posture Review, through the LOE implementation process. The LOE implementation process allows the Department to take a system-wide view of the environment,

address disparate approaches, and eliminate friction points across the Department. Although the LOE end-states, articulated in the Cyber Strategy, are enduring, the intermediate objectives are more dynamic to allow the Department to re-evaluate and adjust as needed to the operating environment. OPCA activities are rooted in strategy and prioritized by risk; they are warfighter-focused with the aim of increasing the lethality of the U.S. Armed Forces. To that end, we are leading a Department-wide effort to translate the Cyber Strategy LOEs into specific objectives, tasks, and sub-tasks that are focused on outcomes. Integral to this effort is the ability to measure results clearly and objectively to be able to gauge return on investment.

The DoD's "Top 10 Cyber Priorities" are nested under the Cyber Strategy LOEs to ensure consistency and completeness of execution. Through implementing the "First Four (a sub-set of the Top 10)," the OPCA is focused on outcomes to improve end-point security, identification and access management, development security operations, and cyber workforce management. The FY 2019 objectives are aggressive and include end-point detection and automated reporting of devices with an operating system; the development and deployment of a DoD Enterprise Identity Service; establishment of a developer's toolkit; and roll-out of Cyber Excepted Service Phase II. A DoD re-programming request is pending to enable these mission critical activities.

Together, the DoD Chief Information Officer (CIO) and the OPCA work together directly to implement the DoD Cyber Strategy in close coordination with the other DoD Component CIOs. The DoD CIO and PCA co-lead weekly meetings focused on cyber issues with the Deputy Secretary of Defense and with all of the Military Departments' and Office of the Secretary of Defense (OSD) Principals present. These meetings ensure that the Deputy Secretary of Defense is kept abreast of progress on cyber initiatives and that all Department leaders are present to

receive direction, share challenges, leverage opportunities--all with the purpose of achieving timely and measurable outcomes.

The Department has an ongoing commitment to information technology, cybersecurity, and information assurance as articulated in our Cyber Strategy. To that end, I will continue to partner across the Department as an advocate to integrate and oversee the development of cyberspace capabilities, activities, and policies, within cyber-related initiatives. The OPCA with its cross-functional team has proven to be a valuable component in translating plans to actions. Partnerships with the DoD CIO, the Military Departments, the Services, and other DoD Components could not be stronger and are key to continued success.

I am grateful for Congress's strong support of the Department of Defense's efforts to build the correct partnerships needed to operate in cyberspace to increase the lethality of our Armed forces. I thank the Subcommittee for its interest in these issues and look forward to your questions.

BGen Dennis Crall, USMC
Deputy Principal Cyber Advisor, Office of the Secretary of Defense

Brigadier General Crall assumed the duties of Deputy Principal Cyber Advisor within OSD in February 2018. A native of South Carolina, he graduated from the University of South Carolina and was commissioned in 1987.

Brigadier General Crall is a career Aviation Command and Control Officer who has commanded at the Squadron and Group levels. He deployed as the Direct Air Support Center (Airborne), Officer-In-Charge in support of Operation Iraqi Freedom, conducting thirty-four combat missions spanning over three hundred fifty flight hours. He has also served as the Joint Liaison Officer to the 7th Air Force, 607th Air Support Operations Group in Osan, Korea.

Brigadier General Crall's joint assignments include Chief, Joint Cyberspace Center, US Central Command (CENTCOM); Executive Officer to the Deputy Commander, CENTCOM; Division Chief, Information Operations, CENTCOM; Division Chief, Developments and Concepts, CENTCOM; and Branch Chief, Strategic Plans, Information Operations, US Special Operations Command (SOCOM).

Brigadier General Crall's supporting assignments were with Marine Corps Recruiting Command, serving as the Operations Officer, Recruiting Station Albuquerque, NM; and Contact Team Officer, 6th Marine Corps District, Parris Island, SC.

Brigadier General Crall is a graduate of the Marine Corps Command and Control Systems Course; a distinguished graduate of the US Air Force Air Command and Staff College where he earned a M.S. in Military Operational Art and Science; and a distinguished graduate of the National War College where he earned a M.S. in National Security Strategy. He has also completed the Harvard Kennedy School Cybersecurity Executive Program.

WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING

FEBRUARY 26, 2019

RESPONSE TO QUESTION SUBMITTED BY MR. LANGEVIN

General CRALL. A modern digital infrastructure is critical to defending against cyber-attacks as well as enabling machine learning and artificial intelligence. The DOD cloud initiative is part of a larger effort to modernize information technology across the DOD enterprise. Consolidating currently disparate efforts at the enterprise level will enable the Department of Defense to provide greater security and ensure greater reliability of the department's digital infrastructure. The DOD Cloud Initiative includes multiple cloud efforts, including JEDI Cloud. JEDI will allow DOD to take advantage of economies of scale, ensure superiority through data aggregation and analysis, and lay the foundational technology for artificial intelligence and machine learning. [See page 21.]

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

FEBRUARY 26, 2019

QUESTIONS SUBMITTED BY MS. STEFANIK

Ms. STEFANIK. In your testimony, you claimed $4.702 billion in programmed savings in FY17 and FY18. Can I get a list of these savings and where you found them?

Ms. HERSHMAN. The Department has saved $4.702B through reform efforts in FYs 2017 and 2018 combined, and is on track to save more than $6B in FY 2019. This achievement is a collective effort by key stakeholders in the Department. The CMO, Military Departments, and the USD(C) identified, validated, and presented savings formally in the FY 2020 budget that were reinvested in priorities identified in the NDS. The Department was successful in meeting or exceeding many of its priority initiatives, including those related to achieving efficiencies, effectiveness and cost savings, audit readiness, and improving the quality of the Department's business operations. The list below includes some areas in which the Department has found found savings:

- Management Headquarters Reductions
- Services Requirements Review Board and Contractor Courts
- IT Circuit Optimization
- Enterprise Licensing Agreements
- Data Center infrastructure
- Military Health IT Optimization
- Defense Travel Modernization
- Defense Agencies and DOD Field Activities Civilian Personnel Reductions
- Defense Media Activity Business Process and Systems Review

Ms. STEFANIK. What is your savings goal for the next five years?

Ms. HERSHMAN. Over the next five years the Department is projecting a $44.9B savings in ongoing reform initiatives. These reform savings will be garnered from business process improvements, business systems improvements, policy reforms, weapons systems acquisition reform, divestments, and better alignment of resources to the National Defense Strategy. Additionally, studies are underway to further streamline or consolidate 4th Estate functions, with the intent on a more efficient structure.

Ms. STEFANIK. How are you re-investing the $4.702 billion?

Ms. HERSHMAN. DOD is actively institutionalizing reform and is committed to reinvesting the savings in the Military Departments in support of readiness and lethality priorities. The FY 2020 budget request builds on our success with the FY 2018 and FY 2019 budgets to repair damaged readiness and marks a key shift in preparing to deter or defeat great power adversaries well into the future.

QUESTIONS SUBMITTED BY MR. CONAWAY

Mr. CONAWAY. Are any of the witnesses concerned about the investments China is making in Chinese companies to pursue Artificial Intelligence and Machines Learning capabilities? If so, how important is it for the United States to have a robust technology industrial base?

Ms. HERSHMAN. CMO will defer to DOD CIO's response to this question.

Mr. CONAWAY. How does a winner take all cloud competition help bolster that robust industrial base?

Ms. HERSHMAN. CMO will defer to DOD CIO's response to this question.

Mr. CONAWAY. What are the cyber risks of placing too much of our national security sensitive data within the infrastructure of one cloud provider?

Ms. HERSHMAN. CMO will defer to DOD CIO's response to this question.

Mr. CONAWAY. Are you aware of any assessments underway at DOD or DNI to assess the implications of a vulnerability in a cloud providers infrastructure and how that vulnerability could impact data held across the national security enterprise?

Ms. HERSHMAN. CMO will defer to DOD CIO's response to this question.

Mr. CONAWAY. What are security benefits of cloud diversity?

Ms. HERSHMAN. CMO will defer to DOD CIO's response to this question.

Mr. CONAWAY. Are any of the witnesses concerned about the investments China is making in Chinese companies to pursue Artificial Intelligence and Machines

Learning capabilities? If so, how important is it for the United States to have a robust technology industrial base?

Mr. DEASY. There are three reasons to be concerned about the investments China is making in AI and Machine Learning.

First, the significant scale and strategic focus demonstrated by Chinese Artificial Intelligence (AI) investments and their stated goal to dominate the global AI technology landscape. As stated in the recent Executive Order 13859 of February 11, 2019 "Continued American leadership in AI is of paramount importance to maintaining the economic and national security of the United States and to shaping the global evolution of AI in a manner consistent with our Nation's values, policies, and priorities."

Second, the Department of Defense is concerned about the powerful tools available to the Chinese government to coerce commercial Chinese companies to support Chinese military AI development.

Finally, the Department is concerned that Chinese military leaders have explicitly stated that their investments in AI are aimed at closing the gap in military power between China and the United States. China seeks to use AI as a tool to "leapfrog" the United States' current global leadership position in military technology. Given the progress in AI demonstrated by China over the past few years, that is not something the U.S. should take lightly.

The strength of the U.S. technology industrial base and the commercial AI ecosystem is a critical source of U.S. competitive advantage. Just as commercial spending on computers and other information technology has historically far outpaced DOD spending, so too does commercial investment in AI. DOD should seek to effectively partner with American companies and draw upon the innovativeness of American AI experts. This partnership must, however, remain consistent with American values.

Mr. CONAWAY. How does a winner take all cloud competition help bolster that robust industrial base?

Mr. DEASY. The Department will implement a commercial General-Purpose enterprise-wide cloud solution, Joint Enterprise Defense Infrastructure (JEDI), for the majority of systems and applications. However, the DOD's Cloud Strategy defines the need for additional fit for purpose clouds to meet specific needs and gaps. DOD expects that cloud technology and offerings will continue to become more interoperable and seamlessly integrated, enabling lower transaction costs and better intercloud security features across multiple providers. DOD is best served by a robust, competitive, and innovative technology industrial base.

Further, maximizing competition is critical to a robust and comprehensive enterprise-wide environment for all cloud-related contracting actions and not limited to any one particular contract. Cloud-related contracting actions go beyond just contracts for hosting environments (whether the environment is JEDI, milCloud 2.0, DEOS, or other fit for purpose needs). More critically, the engineering and migration support necessary to develop and deploy systems and applications are often suited to companies with more agile and nimble capabilities, which often may be appropriate for smaller specialized business entities.

Mr. CONAWAY. What are the cyber risks of placing too much of our national security sensitive data within the infrastructure of one cloud provider?

Mr. DEASY. Applications and data within a single cloud environment are able to maximize the native security features of cloud technology, which includes robust and automated failover and redundancy features. The risks are managed according to the sensitivity of the data by adding controls at the specified security level. It is also important to note that a single cloud environment does not mean that all data and applications are hosted in a single physical environment where everything is vulnerable to a single attack. Rather, the provider will have varying levels of logical and physical isolation available, based the sensitivity of the data, which will work in concert with the Department's existing cyber security tool sets. Leveraging a single versus multiple cloud provider environment reduces the number of potential vulnerabilities, since with each provider comes additional connection points and accreditations, resulting in the possible increase in both vulnerabilities and time and cost.

Mr. CONAWAY. Are you aware of any assessments underway at DOD or DNI to assess the implications of a vulnerability in a cloud providers infrastructure and how that vulnerability could impact data held across the national security enterprise?

Mr. DEASY. The Department continues to perform an ongoing comprehensive risk assessment of cloud security risks. The risks are managed according to the sensitivity of the data by adding controls at the specified security level. This assessment is not limited to a particular current or future program, but rather is a holistic as-

sessment across the Department's cloud portfolio. The Department's assessment is ongoing, continuously analyzing and understanding how to characterize risks and effectively mitigate them. The Department has also been looking closely at the work being done by groups outside of the government.

Mr. CONAWAY. What are security benefits of cloud diversity?

Mr. DEASY. The benefits of cloud diversity include more variety of choices in services, to include cyber security services, partnerships and unique solutions along with the increased availability of hosting locations, which provides physical diversity. Cloud diversity is beneficial, which is why DOD's Cloud Strategy is to remain a multiple cloud environment.

However, technical complexity increases, based on the number of cloud providers and available offerings. The risk associated with deploying wide-reaching cloud diversity entails understanding how to deploy and secure workloads properly in any cloud environment while also understanding and utilizing all of the services available to help secure workloads across multiple cloud environments, when necessary.

Mr. CONAWAY. Are any of the witnesses concerned about the investments China is making in Chinese companies to pursue Artificial Intelligence and Machines Learning capabilities? If so, how important is it for the United States to have a robust technology industrial base?

General CRALL. China's 2017 national AI strategic plan calls for Chinese technology to be on par with that of the United States by 2020 and for China to become the world leader in AI by 2030. In 2019, China's aggressive pursuit of and investment in AI has significantly closed the technology gap with the United States. China now ranks first in the quantity and citations of AI research papers, holds more AI patents than the US and Japan, and exports armed autonomous platforms and surveillance AI. However, China's January 2018 "White Paper on Artificial Intelligence Standardization" points out that the China's AI ecosystem lags in several key areas: top talent, technical standards, software platforms, and semiconductors. These are strengths in our technology industrial base that the United States must capitalize on to maintain a leading edge in AI development.

Mr. CONAWAY. How does a winner take all cloud competition help bolster that robust industrial base?

General CRALL. I agree with DOD(CIO) as the Department will implement a commercial General-Purpose enterprise-wide cloud solution, Joint Enterprise Defense Infrastructure (JEDI), for the majority of systems and applications. However, the DOD's Cloud Strategy defines the need for additional fit for purpose clouds to meet specific needs and gaps. DOD expects that cloud technology and offerings will continue to become more interoperable and seamlessly integrated, enabling lower transaction costs and better inter-cloud security features across multiple providers. DOD is best served by a robust, competitive, and innovative technology industrial base.

Further, maximizing competition is critical to a robust and comprehensive enterprise-wide environment for all cloud-related contracting actions and not limited to any one particular contract. Cloud-related contracting actions go beyond just contracts for hosting environments (whether the environment is JEDI, milCloud 2.0, DEOS, or other fit for purpose needs). More critically, the engineering and migration support necessary to develop and deploy systems and applications are often suited to companies with more agile and nimble capabilities, which often may be appropriate for smaller specialized business entities.

Mr. CONAWAY. What are the cyber risks of placing too much of our national security sensitive data within the infrastructure of one cloud provider?

General CRALL. I agree with DOD(CIO) as applications and data within a single cloud environment are able to maximize the native security features of cloud technology, which includes robust and automated failover and redundancy features. The risks are managed according to the sensitivity of the data by adding controls at the specified security level. It is also important to note that a single cloud environment does not mean that all data and applications are hosted in a single physical environment where everything is vulnerable to a single attack. Rather, the provider will have varying levels of logical and physical isolation available, based the sensitivity of the data, which will work in concert with the Department's existing cyber security tool sets. Leveraging a single versus multiple cloud provider environment reduces the number of potential vulnerabilities, since with each provider comes additional connection points and accreditations, resulting in the possible increase in both vulnerabilities and time and cost.

Mr. CONAWAY. Are you aware of any assessments underway at DOD or DNI to assess the implications of a vulnerability in a cloud providers infrastructure and how that vulnerability could impact data held across the national security enterprise?

General CRALL. As the DOD(CIO) has emphasized, the Department continues to perform an ongoing comprehensive risk assessment of cloud security risks. The risks are managed according to the sensitivity of the data by adding controls at the specified security level. This assessment is not limited to a particular current or future program, but rather is a holistic assessment across the Department's cloud portfolio. The Department's assessment is ongoing, continuously analyzing and understanding how to characterize risks and effectively mitigate them. The Department has also been looking closely at the work being done by groups outside of the government.

Mr. CONAWAY. What are security benefits of cloud diversity?

General CRALL. As stated by the DOD(CIO), the benefits of cloud diversity include more variety of choices in services, to include cyber security services, partnerships and unique solutions along with the increased availability of hosting locations, which provides physical diversity. Cloud diversity is beneficial, which is why DOD's Cloud Strategy is to remain a multiple cloud environment.

However, technical complexity increases, based on the number of cloud providers and available offerings. The risk associated with deploying wide-reaching cloud diversity entails understanding how to deploy and secure workloads properly in any cloud environment while also understanding and utilizing all of the services available to help secure workloads across multiple cloud environments, when necessary.

QUESTIONS SUBMITTED BY MR. BROWN

Mr. BROWN. In June 2017 the administration issued EO 13800 to "Strengthen the Cybersecurity of Federal Networks and Critical Infrastructure." Yet, after the first defense-wide audit was completed in November 2018, Deputy Secretary of Defense Patrick Shanahan stated "We failed the audit. But we never expected to pass it." The subsequent report stated that the IT systems have "systemic shortfalls in implementing cybersecurity measures to guard the data protection environment" and "issues exist in policy compliance with cybersecurity measures, oversight, and accountability." How are these two efforts—the EO and the audit—informing each other? What explains the significant noncompliance with cybersecurity standards almost two years after the EO was issued?

Mr. DEASY. The DOD follow-on activities to EO 13800 and DOD actions to remediate FM Audit Notice of Findings and Recommendations (NFR) have important intersections. Following analysis of the FM Audit NFRs, DOD developed a prioritization approach that seeks to prioritize addressing those findings with a nexus to both cybersecurity and material weakness. These analyses and prioritization efforts pointed to the need for enterprise capabilities in support of Identify, Credential and Access Management (ICAM). Following DOD efforts to respond to EO 13800, DOD developed its top 10 Cyber Priorities. Among areas identified as the "first four," were strategic initiatives associated with ICAM. These efforts are in alignment with ongoing Cyber Hygiene Scorecard efforts, which identified and tracked needed improvements associated with credential management, privileged users, and access control.

QUESTIONS SUBMITTED BY MR. KIM

Mr. KIM. As you are well aware, the overwhelming majority of internet traffic travels via undersea cables. Importantly, there are three major cable landing points in my home State of New Jersey. These cables and accompanying infrastructure are vital to economic and national security. What efforts are currently underway either internal to government or in partnership with the private sector to keep telecommunications infrastructure secure and accessible to the Defense Department?

Mr. DEASY. The DOD partners with the Department of Homeland Security, Intelligence Community, other government agencies, and Industry on a routine basis to ensure the security and resiliency of undersea cables, landing sites and associated infrastructure. Specifically the DOD CIO, partners with Joint Staff, United States Strategic Command, Defense Information Systems Agency, and Defense Threat Reduction Agency to secure cable landing points by funding and remediating physical and cyber vulnerabilities found.

○