AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

[H.A.S.C. No. 115–122]

DEPARTMENT OF DEFENSE'S ARTIFICIAL INTELLIGENCE STRUCTURE, INVESTMENTS, AND APPLICATIONS

HEARING

BEFORE THE

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

HEARING HELD
DECEMBER 11, 2018

U.S. GOVERNMENT PUBLISHING OFFICE
34–978 WASHINGTON : 2019

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

ELISE M. STEFANIK, New York, *Chairwoman*

BILL SHUSTER, Pennsylvania
RALPH LEE ABRAHAM, Louisiana
LIZ CHENEY, Wyoming, *Vice Chair*
JOE WILSON, South Carolina
FRANK A. LOBIONDO, New Jersey
DOUG LAMBORN, Colorado
AUSTIN SCOTT, Georgia
JODY B. HICE, Georgia
(Vacancy)

JAMES R. LANGEVIN, Rhode Island
RICK LARSEN, Washington
JIM COOPER, Tennessee
JACKIE SPEIER, California
MARC A. VEASEY, Texas
TULSI GABBARD, Hawaii
BETO O'ROURKE, Texas
STEPHANIE N. MURPHY, Florida

ERIC SNELGROVE, *Professional Staff Member*
LINDSAY KAVANAUGH, *Professional Staff Member*
JAMIE JACKSON, *Deputy General Counsel*
NEVE SCHADLER, *Clerk*

CONTENTS

Page

STATEMENTS PRESENTED BY MEMBERS OF CONGRESS

Langevin, Hon. James R., a Representative from Rhode Island, Ranking Member, Subcommittee on Emerging Threats and Capabilities 2
Stefanik, Hon. Elise M., a Representative from New York, Chairwoman, Subcommittee on Emerging Threats and Capabilities 1

WITNESSES

Deasy, Dana, Chief Information Officer, Department of Defense 5
Porter, Dr. Lisa, Deputy Under Secretary of Defense for Research and Engineering, Department of Defense 4

APPENDIX

PREPARED STATEMENTS:
Deasy, Dana 32
Porter, Dr. Lisa 27
Stefanik, Hon. Elise M. 25

DOCUMENTS SUBMITTED FOR THE RECORD:
[There were no Documents submitted.]

WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING:
[There were no Questions submitted during the hearing.]

QUESTIONS SUBMITTED BY MEMBERS POST HEARING:
Mr. Larsen 43

DEPARTMENT OF DEFENSE'S ARTIFICIAL INTELLIGENCE STRUCTURE, INVESTMENTS, AND APPLICATIONS

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES,
Washington, DC, Tuesday, December 11, 2018.

The subcommittee met, pursuant to call, at 3:30 p.m., in room 2118, Rayburn House Office Building, Hon. Elise M. Stefanik (chairwoman of the subcommittee) presiding.

OPENING STATEMENT OF HON. ELISE M. STEFANIK, A REPRESENTATIVE FROM NEW YORK, CHAIRWOMAN, SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

Ms. STEFANIK. Thank you for your patience. The subcommittee will now come to order.

Welcome, everyone, to this open hearing of the House Armed Services Subcommittee on Emerging Threats and Capabilities. Today we will examine the DOD's [Department of Defense's] efforts to transform the delivery of artificial intelligence-enabled [AI] capabilities to the warfighter.

AI and machine learning are topics of priority and deep interest among the members of this subcommittee as we build a blueprint for the battlefield of the future. Over the last year, we have explored these technology issues closely and heard from numerous outside subject matter experts on the emerging opportunities, challenges, and implications of adopting commercial artificial intelligence solutions into the defense enterprise.

We have also closely examined our adversaries' investments in AI and related technologies, including China's whole-of-society approach, which threatens our competitive advantage. In response, this committee has taken deliberate bipartisan actions to better organize the Department of Defense to oversee, accelerate, and integrate artificial intelligence and machine learning technologies.

The John S. McCain National Defense Authorization Act for Fiscal Year [FY] 2019 directed the Secretary of Defense to conduct a comprehensive national review of advances in AI relevant to the needs of the military services.

Section 238 further directed the Secretary to craft a strategic plan to develop, mature, adopt, and transition artificial intelligence technologies into operational use.

Additionally, section 1051 established the National Security Commission on AI, an independent entity inside the executive branch, to take a holistic view of the competitiveness of U.S. efforts

and elevate the national conversation surrounding the national security implications of AI.

Today, we will continue this conversation and hear about the DOD's efforts to reorganize and more effectively oversee the execution of AI programs across the military services. We will also examine the Department's investments in basic research to generate groundbreaking AI capabilities for future conflict.

The transformation and prioritization of AI inside the Department today will shape the efficiency of DOD's business functions, and most importantly, the effectiveness of our forces in future battle.

Let me welcome our witnesses here today: Dr. Lisa Porter, Deputy Under Secretary of Defense for Research and Engineering at the DOD, and Mr. Dana Deasy, Chief Information Officer at the DOD.

We look forward to your testimony.

And finally, I want to take this time to recognize and express this subcommittee's gratitude to two staff members who will be departing the committee this month, Neve Schadler and Mark Pepple. Thank you so much for all of your work this past year and years prior. Your contributions to this committee are appreciated from both sides of the aisle, and we wish you best of luck in your next endeavors.

Let me now turn to Ranking Member Jim Langevin for his opening comments.

[The prepared statement of Ms. Stefanik can be found in the Appendix on page 25.]

STATEMENT OF HON. JAMES R. LANGEVIN, A REPRESENTATIVE FROM RHODE ISLAND, RANKING MEMBER, SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

Mr. LANGEVIN. Thank you, Madam Chair, and I want to thank and welcome our witnesses here today.

This year the Emerging Threats and Capabilities Subcommittee has placed a significant emphasis on how artificial intelligence, machine learning, and associated technologies can be used to advance U.S. warfighting and deterrence capabilities and bring efficiencies to business processes and systems in the Department.

In June, the subcommittee held an industry roundtable where we focused largely on the implementation of AI in the defense innovation system and how the Department of Defense can best leverage in-house and commercial capabilities to support military functions.

During the roundtable discussion I expressed serious concerns about what I perceived as a disjointed, ad hoc approach by DOD in developing Department-wide AI policies, strategies, and programs. Since then, I am pleased to see that the Department has made some strides toward refining and refocusing its AI programs and initiatives.

Most notably, the Department launched the Joint Artificial Intelligence Center [JAIC]. I look forward to better understanding how this center, located under the Chief Information Officer, will bring synergy to Department-wide efforts.

More specifically, I hope to hear today about the center's structure, mission, roles and responsibilities, coordination with the mili-

tary services, and plans for delivering and scaling critical AI capabilities.

Finally, I would like to better understand how the center fits into the Department's cloud initiative.

Now, many claim that data is the new oil. Access to data, data integrity, and data labelling are key issues facing the Department.

In addition to hearing about the Joint AI Center, I look forward to hearing from Mr. Deasy about how he is setting standards and issuing other guidance to the services, agencies, and other entities pertaining to these issues.

In August, through Chairwoman Stefanik's leadership, we successfully authorized the National Security Commission on Artificial Intelligence. I commend the Chair for her work. I was proud to join her in that effort.

The commission has been tasked with comprehensively examining U.S. advances in AI with regard to investments in basic and advanced research, efforts to recruit top-notch talent, ethical and safety considerations for military applications, and strengthening our global competitive advantage in the field.

I appreciate the DOD's partnership in standing up the commission and look forward to hearing more about its plans to prioritize funding and resources for the commission during today's hearing.

I also look forward to hearing more about the division of roles and responsibilities for the AI portfolio between the Department's Under Secretary of Defense for Research and Engineering and the Chief Information Officer, as well as efforts to synthesize AI strategies and plans with the services.

There is enormous momentum around AI, and it is exciting, and it is critical that the U.S. capitalize on this momentum in order to maintain its technological edge. As a matter of national security, I strongly encourage the Department to continue to strengthen its partnerships with academia and the private sector, better leverage Federal labs, invest in cutting-edge research, and continue to explore applications of AI with the interagency to ensure that we remain at the forefront of AI innovation.

Before I yield back, I, too, want to join Chairwoman Stefanik in recognizing Dr. Mark Pepple, and Neve Schadler, clerk, for their service to the committee as well as they depart at the end of the year. I want to thank them for their work. They have made great contributions to our work here on the committee, and we are grateful for their service.

So thank you. And I yield back.

Ms. STEFANIK. Thank you, Ranking Member Langevin.

I also want to welcome the chairman of the full committee, Chairman Thornberry, who is here with us today. And this issue is of deep interest to him, as reflective of the interest of committee members beyond this subcommittee.

Without objection, the witnesses' prepared statements will be made part of the record. I ask that you please keep your opening remarks to no more than 5 minutes.

And Dr. Porter, we will begin with you.

STATEMENT OF DR. LISA PORTER, DEPUTY UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING, DEPARTMENT OF DEFENSE

Dr. PORTER. Good afternoon, Chairwoman Stefanik, Ranking Member Langevin, and distinguished members of the subcommittee. Thank you for inviting me to appear before you today to discuss artificial intelligence, particularly as it relates to national security applications.

As this subcommittee knows, artificial intelligence, or AI, is not a new thing. As long as there have been computers, there have been engineers who have dreamed of enabling machines to think the way humans do. In fact, DARPA [Defense Advanced Research Projects Agency] funded much of the early work in AI decades ago.

Today we are experiencing an explosion of interest in a subfield of AI called machine learning, where algorithms have become remarkably good at classification and prediction tasks when they can be trained on very large amounts of data.

There are numerous examples of successful applications of machine learning techniques. Some of the obvious ones include facial recognition in photographs and voice recognition on smartphones.

However, there has also been a significant amount of hype and confusion regarding the current state of the art. It is the USD (R&E) [Under Secretary of Defense for Research and Engineering] position that we must not abandon the tenets of scientific rigor and discipline as we pursue the opportunities that AI presents.

Today's AI capabilities offer potential solutions to many defense-specific problems. Examples include object identification in drone video or satellite imagery and detection of cyber threats on networks. However, there are several issues that must be addressed in order to effectively apply AI to national security mission problems.

First, objective evaluation of performance requires the use of quantitative metrics that are relevant to the specific use case. In other words, AI systems that have been optimized for commercial applications may not yield effective outcomes in military applications.

Second, current AI systems require enormous amounts of training data, and the preparation of that data in a format that the algorithms can use, in turn, requires an enormous amount of human labor.

Furthermore, AI systems that have been trained on one type of data typically do not perform well on data that are different from the training data. For example, algorithms that are trained on internet images will generally underperform when used on drone or satellite imagery.

Another well-known limitation of current systems is that they cannot explain what they do, making them hard to trust.

Furthermore, current systems require robust processing power.

And finally, current systems are susceptible to various forms of spoofing, known as adversarial AI.

We are working to address these challenges and vulnerabilities through multiple efforts, most of which will lever the complementary roles of the Joint Artificial Intelligence Center, the JAIC, and the USD(R&E) enterprise.

The JAIC will offer a means to rapidly determine the appropriate metrics for operational impact for a variety of applications, as well as the operational performance limitations of current tools. And these insights will help inform algorithm and system development across multiple USD(R&E) efforts.

Furthermore, the JAIC's focus on scaling and integration will drive innovation and data-curation techniques, while DARPA will pursue algorithms that can be robustly trained with much less data.

In order to address AI's trust issue, DARPA's Explainable AI program aims to create machine learning techniques that produce more explainable models while maintaining a high level of performance. The High Performance Computing Modernization Program is designing new systems that will provide ample processing power for AI applications on the battlefield. Finally, countering adversarial AI is one of the key focus areas of DARPA's AI Next campaign.

Ultimately, as we look to the future, we anticipate a focus on developing AI systems that have the ability to reason as humans do, at least to some extent. Such a capability would greatly amplify the utility of AI, enabling AI systems to become true partners with their human counterparts in problem solving.

It is important that we continue to pursue cutting-edge research in AI, especially given the significant investments our adversaries are making. We are therefore grateful for the leadership and support that the members of the subcommittee have shown regarding AI.

We also appreciate the establishment of the National Security Commission on AI, whose charter is appropriately focused on key areas that must be assessed objectively to assure that the U.S. maintains a leadership position in AI-enabled technologies and systems.

Thank you for your interest in this important topic, and I look forward to answering your questions.

[The prepared statement of Dr. Porter can be found in the Appendix on page 27.]

Ms. STEFANIK. Thank you.

Mr. Deasy.

STATEMENT OF DANA DEASY, CHIEF INFORMATION OFFICER, DEPARTMENT OF DEFENSE

Mr. DEASY. Good afternoon, Ms. Chairwoman, Ranking Member, and distinguished members of the subcommittee. I thank you for this opportunity to testify on the Department's progress in AI adoption and the establishment of the Joint Artificial Intelligence Center.

I am Dana Deasy, the Department of Defense Chief Information Officer. I am the principal adviser to the Secretary of Defense for a set of responsibilities that integrate together to ensure that DOD has the information and communications technology capabilities needed to enable the broad set of missions we perform as a joint force.

The application of AI is rapidly changing a wide range of businesses and industries. The 2018 National Defense Strategy [NDS]

foresees that ongoing advances in AI will change society and, ultimately, the character of war.

In June, Deputy Secretary Shanahan directed my office to establish the Joint Artificial Intelligence Center as a focal point for that endeavor. In parallel, DOD submitted its first AI Strategy to Congress, an annex to the NDS. JAIC's formation also dovetailed section 238 of the latest NDAA.

Going forward, JAIC will benefit from and help bring into reality recommendations of the National Security Commission on AI.

In talking about the Joint Artificial Intelligence Center, I would like to highlight three themes today.

The first is delivering AI-enabled capabilities at speed. JAIC is collaborating now with teams across DOD to systematically identify, prioritize, and select mission needs, and then rapidly execute a sequence of cross-functional use cases that demonstrate value and spur momentum.

Projects fall into two main categories: National Mission Initiatives [NMI] and Component Mission Initiatives [CMI]. NMIs are driven and executed by JAIC, whereas CMIs are component-led and are able to make use of JAIC's common tools, libraries, best practices, and more.

I will note that our new emphasis on rapid, iterative delivery of AI complements the Department's ongoing work at the other end of the AI spectrum and fundamental research, as Dr. Porter shared with you today.

Two examples of early projects. First, predictive maintenance. The NMI helps address Secretary Mattis' direction to the services to improve their maintenance readiness rates and offers well-defined return on investment criteria.

A second example, humanitarian assistance and disaster relief. This NMI is an open mission to apply AI to saving lives and livelihood. We are applying lessons learned and reusable tools from the DOD's AI pathfinder, Project Maven, to field AI capabilities in support of such events as hurricanes and wildfires.

The second theme is all about scale. JAIC's early projects serve a dual purpose: to deliver new capabilities to end-users, as well as to incrementally develop the common foundation that is essential for scaling AI's impact across the DOD. This means shared data, reusable tools, libraries, standards, and AI cloud and edge services that help jump-start new projects.

We will put this in place, this foundation, in a manner that aligns with the DOD enterprise cloud adoption. Let me underscore that point. Our enterprise approach for AI and enterprise cloud adoption via the DOD-wide cloud strategy are mutually reinforcing, mutually dependent undertakings.

The third theme is we build the initial JAIC team. It is all about talent. And this will be represented across all the services and all components.

Today we have assembled a force of nearly 30 individuals. Going forward, it is essential that JAIC attract and cultivate a select group of mission-driven, world-class AI talent, including pulling these experts into service from industry.

In closing, 2 weeks ago, in front of 380 companies and academic institutions at DOD's AI Industry Day, I announced we had

achieved a significant milestone: JAIC is now up and running and open for business.

I look forward to continuing to work with Congress in this critical area in an ongoing dialogue on our progress in AI adoption and the ways in which JAIC is being used to accelerate that progress.

Thank you for this opportunity to testify this afternoon, and I look forward to your questions.

[The prepared statement of Mr. Deasy can be found in the Appendix on page 32.]

Ms. STEFANIK. Thank you for those opening statements.

I want to ask a broad question to begin. I am deeply concerned, as I read headline after headline announcing the U.S.'s looming defeat when it comes to the global race for AI dominance. It seems like every week there is a new headline.

I want to quote a recent article, of the fall of this year, in Foreign Policy:

"There will not be one exclusively military AI arms race. There will instead be many AI arms races as countries (and, sometimes, violent nonstate actors) develop new algorithms or apply private sector algorithms to help them accomplish particular tasks.

"In North America, the private sector invested some $15 billion to $23 billion in AI in 2016. That is more than 10 times what the U.S. Government spent on unclassified AI programs that same year.

"China says it already holds more than 20 percent of patents in the field and plans to build its AI sector to be worth $150 billion by 2030."

My broad question is, are we falling behind already? If so, how far behind? And how do we jump-start it to make sure that we do not lose our technological edge when it comes to AI?

Dr. Porter, I will start with you.

Dr. PORTER. So I would say we are not behind. Right now we are actually ahead. However, we are in danger of losing that leadership position. So your concern is certainly valid.

Ms. STEFANIK. And let me, I am going to jump in there. How are we ahead? How do we measure that?

Dr. PORTER. Absolutely. So there are a lot of ways to assess that, but if you look in terms of our talent, particularly in our academic base, the United States, along with our partners in the U.K. [United Kingdom] and Canada in particular, are seen, even by the Chinese, as having quite a lead.

And I will tell you the reason for that—and this is an important point to make, and I alluded to it in my opening—DARPA, in particular, and also the NSF [National Science Foundation], have been funding this field for decades. So we have built an extremely robust and deep bench in the disciplines that are required to advance this field.

Even when you hear about AI winters in the past and so forth, the United States continued to invest robustly in this domain for decades. And then we have this vibrant private sector that is able to turn around and take that research and rapidly convert it to commercial products and create new markets.

So we have a lot going for us, and I believe China has, unfortunately—or fortunately if you are from China, I guess—they have

figured out that that is one of the key ingredients to our success, that we have a multitiered approach in this country to ensuring that we continue to stay on the cutting edge. We invest heavily in academia, we invest heavily in our labs, and then we figure out how to convert those investments quickly and rapidly into products and creating new markets.

They recognize that, and that is why you are seeing a tremendous increase in their investments, particularly in academic as well as startup community, which I think you were alluding to.

Ms. STEFANIK. What about the race for data? You talked about some of the challenges that we face. Obviously, data is the fuel for AI. So when we talk about an AI arms race, part of that is a race for data and being able to analyze data in a comprehensive way. Can you comment on that, Dr. Porter? Beyond the challenges, what are our solutions to ensure that we have the fuel to help propel our AI research?

Dr. PORTER. Yes. So data is a very key element. I have commented on this and so has The New York Times. Probably you saw the article a couple weeks ago highlighting how China has created these places where people are sitting there and essentially labelling data, right, for their needs.

So one of the things we have to do is we have to be smarter about how we understand how these algorithms are working, and that is why DARPA always looks at a problem and says: Okay, how do we do this better? Our industrial sector also recognizes these challenges, so they are going to look at how do we do this better.

So it is not going to be just about how do we get a lot of data; it is going to be about how do we develop algorithms that don't need as much data; how do we develop algorithms that we trust as they are using the data and they are evolving the data.

And this is where the JAIC comes in. I think this is why the powerful connection between R&E and JAIC is so important, because we have an opportunity now, as we want to test out new ideas, we get to a point where we use something like DIU [Defense Innovation Unit], that says, hey, what is going on in the private sector; how are they trying out new things; let's try to prototype; and then get them out into the operational place more quickly and say, how is that actually working?

So this can be a very powerful way for us to accelerate the experimentation that is going to be continual to stay ahead of the game, because it can't just be about labelling data. It has got to be about being smarter using the data that you have got.

Ms. STEFANIK. Thank you, Dr. Porter.

Mr. Langevin.

Mr. LANGEVIN. Thank you, Madam Chair.

And thank you again to both of our witnesses for your testimony today.

Dr. Porter, I would like to start by asking you to expand on what you talked about in terms of the DARPA project and using less data to get better outcomes, if you want to talk a little bit more about that.

Dr. PORTER. Sure. That is just one of the many areas that DARPA has been focusing on. I think some of you are aware of their AI Next campaign, which they have announced publicly, and

they are trying to address all of these weaknesses that—or several of the weaknesses, I should say, that I outlined, and one of them has to do with this reality of the big data problem.

Folks on the cutting edge are now talking about how we can't just be using traditional machine learning. What is the next step? How do we combine other elements to get after this?

And if I can brag about something that DARPA has done recently, because I think it will give you some hope when I say I think the United States has ways to stay ahead. They recently started something called AI Exploration, and this is a way that they very rapidly get money out, particularly into academia, and the labs, and the small businesses, to say, all right, by the time I announce my concept I want you guys to go after, within 90 days I am going to get you the money. Not from the time I tell you, you are selected, but from the time I post it till you get the money.

They have already done this once and within 90 days they had 16 awards out, each about a million dollars or so. And the problem they are tackling is, can we bring some physics into machine learning so that we don't need as much data and we don't have to worry so much about these fragile and brittle things that I was talking about.

So I am telling you this story because I think you have got a lot of innovation going on within the DOD enterprise to say: How do we get to speed, as well as scale? And this is what Dana and I are going to continually try to work together on, is how do we move faster, because AI is all about speed. It really is. This is one of those domains where things are just going very, very quickly.

Mr. LANGEVIN. Thank you, Dr. Porter.

Mr. Deasy, as I mentioned in my opening statement, data is the fuel that powers AI and machine learning. So what efforts are you undertaking to promote policies and practices that ensure DOD owns data collected under its authorities?

Mr. DEASY. So it is interesting, when I joined the Department and we kicked off the JAIC, sir, one of the earliest questions I got asked was: What are going to be some of the earliest stumbling blocks you are going to face in the successful standup of JAIC? And I said: I can almost predict now that as we roll out the first two, three, four applications, the thing that will be hitting us over and over again will be data.

And what do I mean by that? It will be: Where is the single source of the truth coming from? How do you ingest it? What are its formats? Do we have duplicate data? And how do we bring it together.

Part of the reason why you heard me comment in my opening remarks about the integration of cloud: cloud provides us the physical capacity to take this enormous amount of data and bring it together.

True, it will still continue to sit in different formats. But what we will do in development of JAIC is we will start to define with different problem sets and different algorithms what is the expectation in terms of the data standards that need to be deployed.

So if we are looking at audio versus we are looking at image data, or if we are looking at textual or good old-fashioned tables, one of the things that the JAIC will need to do is—two things—

technically describe what it is we need to do to ingest the data and what are the tools; and then two is what are the policies and standards that need to be put in place on the correct formats of data as people develop new systems going forward.

Mr. LANGEVIN. Yeah, but you didn't answer my question about what are we doing to ensure that DOD owns the data collected under its authorities. I need that. But I also need to ask you, how are you incorporating publicly available data sets into your efforts, and have you had challenges accessing data sets owned by other entities? So those two.

Mr. DEASY. Yeah. Too early from the standpoint of JAIC, as JAIC is just stood up. So we haven't had a program right now where we are actually accessing public data. DARPA may be in a position to describe what they have done on that standpoint. But, indeed, there will be programs eventually where we will need to incorporate that, and we will have to be very clear on the ownership of that data.

If the data is truly being created, whether it be from an intel [intelligence] community, a mission partner, very clear rules of the roads will have to be established early on as to the ownership of that data.

Part of our job in standing up JAIC—and I need to stress this throughout today—is that this is going to be an iterative learning cycle. We are going to take something in, we are going to learn what are the issues.

One of the issues, the one you probably bring up here, who owns the data? Where is the legal authorities for that data? And we are going to have to actually take these on a case-by-case basis, then develop ongoing policy that can be applied for more missions as we go forward.

Mr. LANGEVIN. Okay. I am glad we are thinking about these things now for sure.

I know my time is expired. I have other questions. If we get to a second round, I will ask those then. If not, I will submit them for the record. But thank you, and I yield back.

Ms. STEFANIK. Thanks.

Dr. Abraham.

Dr. ABRAHAM. [Inaudible—off mic] but certainly on other sides of this globe. I refer to even gene editing here. Of late we have seen that go awry on the eastern part of the globe. So I worry about the scientific discipline that will be involved with our data.

To follow up on Jim's question a little bit, Mr. Deasy, the algorithms that are constructed by, I am assuming, commercial industry, they own that data. Am I correct there, the way the law stands as of now?

Mr. DEASY. Yes. So in the case of some solutions that we built, for example, in Maven, where we have used partners, part of that case will be commercial available solutions and algorithms that they will own.

Dr. ABRAHAM. And you said JAIC wants to incorporate people from industry to be part of the total family.

Mr. DEASY. Absolutely.

Dr. ABRAHAM. Is that a correct statement?

Mr. DEASY. It will be a combination of those solutions that will be developed by our own organization, JAIC, and those that will be developed through partners. So there will be no single solution where we will probably come from either all commercial, internally, but we will be using a combination of both.

Dr. ABRAHAM. But I just go back to a few years ago where the VA [Department of Veterans Affairs] had a physician develop a drug that was used, and who owned that particular patent was a big mess.

So I just implore—and I am sure you are ahead of the curve here—but if we have the rules of the roads in place before those algorithms are developed and then we have to get into this debate, I think it is prudent to do that.

Madam Chair, I yield back. Thank you.

Ms. STEFANIK. Thank you, Dr. Abraham.

Mr. Larsen.

Mr. LARSEN. Thank you very much. Thanks for coming today.

So one of the criticisms or, I guess, concerns when we compare ourselves to our competitors, especially China, is they can take a top-down approach, sort of drive everything through state-owned enterprises, through what they consider public financing, where we have to have a more of a bottom-up approach because we have such a very active private sector innovative economy.

And so how are you trying to balance that? How are you trying to drive the innovation so that it creates options for the DOD to pick from? Because we are probably not going to drive it to any one solution, but a set of solutions, and then you can choose partners as you move forward. Who might be best to answer that?

Mr. DEASY. Well, I will talk about it from an operational production.

Mr. LARSEN. Yeah, sure.

Mr. DEASY. We will let Dr. Porter discuss it more from a research and science.

Mr. LARSEN. Yeah.

Mr. DEASY. So the way that JAIC is being established is going to be very much a hub-and-spoke model. There will be a physical entity that we are creating in the Washington, DC, area. But we recognize that we are going to need talents that are going to exist, for example, outside in the academia environment.

So part of our spoke model is we will be establishing locations next to academic environments, we are actually in the process of selecting those right now, where they will have certain skill sets. And so what we are actually doing is going through an inventory process of identifying what are the problems we believe are most in need to solve for and what institutions.

Between that and the fact in our AI Day that we ran recently, the reason we ran that day was we are now getting in white papers that are coming in from the commercial sector, as well as the academic sector, starting to describe what are their solutions against the problem sets we are trying to solve. We are right now in the case of actually building out an inventory of these solution sets.

Mr. LARSEN. Interesting. And Dr. Porter.

Dr. PORTER. So one of the things that when Dana and I talk about this—and this may be a helpful thing if you can visualize

it—we think about near, mid, and long term. And in the near term, of course, that is where JAIC resides.

And in the mid term gets to kind of your question. This is where DIU, for example, says: All right, what is going on in the private sector? Because those problems that I articulated that we have to address, the private sector has to address as well.

So if an algorithm isn't very robust, my recommender system doesn't tell you that the movie that I am recommending to you makes any sense to you, you are not going to use my system either, and that is going to cause revenue problems. So I have got to solve that problem.

So the DIU, in places like that, they look and say: Well, what are they coming up with in the near term or the mid term that we can fold back in and test.

And so DIU has a very effective way of basically doing proof of principle and projects at a lower level and say: Okay, JAIC, I think we have got this; we want you to scale it up and really test it, and wring it out, and tell us where we are missing things and continue to iterate. So that is kind of a unique capability.

Now, if you go a little further out, to your point, some of these problems the commercial sector are not going to solve, because they are hard or they are not relevant to their markets. That is why we need a DARPA. That is why we need our national labs. That is why we need our underpinning across that entire spectrum of our academic experts who can guide us in the near, mid, and far term to think about what can we solve now and where do we need to have long-term strategic investment.

And, again, the willingness as a nation to continue to invest in the hard problems even as some of those are going to lead to missteps and we are going to have to try again, right? That is that high-risk, high-payoff realm. So we have to cover that entire spectrum. If we do that, we can optimize on benefitting from the private sector, as well as pushing to solve the problems we care about most that are hard.

I am sorry, I went over the time.

Mr. LARSEN. No, that is fine. I have a little less than a minute.

So the Center for Strategic and International Studies just published a report late last month on AI and national security, and the argument they made was the need for robust supporting capabilities or an ecosystem around AI, especially within DOD.

And I don't know if your folks have evaluated that. But it might be—it is not an easy read for people like me, but it is a good read for folks like you to use it maybe as a marker standard to compare yourself against. There are other folks writing about this as well. But I would commend that to you.

And they outline a variety of areas: trust and security of AI, the people part of it, the digital capability, and the policy. Which you have already outlined some of those concerns and the things you are trying to focus on. I would just lay that out there if you are thinking about how to compare yourself to where maybe you ought to be versus where you are today.

And I will wait for a second round. Thanks.

Ms. STEFANIK. Mr. Hice.

Mr. HICE. Thank you, Madam Chair.

China has identified AI as a strategic technology for them, and they plan to develop an AI industry worth over $21 billion by 2020.

As we all know here in this room, China also has a strong history of both government and industrial espionage, and this just creates a great deal of concern personally.

So what are we doing to protect ourselves, specifically from China, but really from anyone, from hackers? What are we doing to make sure our AI program remains ours?

Mr. DEASY. Okay, I will start.

So I would say a couple things on that. Interestingly enough, we are actually going to apply AI to help us address this problem.

So I mentioned earlier we have two types of initiatives, National Mission Initiatives and Component Mission Initiatives. We are actually doing some work right now to start to evaluate with U.S. Cyber Command, how is it we can apply AI in pattern recognition in signatures, where are you looking for anomalies that are going on in your network, and how can you use AI to quickly assess that there has been a change to what is a normal pattern.

If you think about how hackers actually try to penetrate, they will go to the point of least resistance, and once they are in, they will go laterally. And then what you are looking for is exfiltration.

And so we believe actually AI will be a very good machine use case for looking at how we look at signatures and patterns of data across our network and actually use that to help ensure that we don't have exfiltration occurring from folks like the Chinese.

Mr. HICE. Dr. Porter, would you like to add anything to that?

Dr. PORTER. Sure. I think you are highlighting an extremely important point. I think there are specific technical approaches that we are going to be working. And that example is a good one, because we are not going to get it all right, and it is going to be iterative, and DARPA, in fact, is also looking at this from their perspective.

But I would want to emphasize the broader point you are making. I think we have to be vigilant and aware of this problem. I actually spent time at In-Q-Tel and I have spent time in the intel community. And I know this committee was briefed, I think back in June, about the Thousand Talents Program that China has, and I know you guys were told at that time exactly your point: They have a goal of facilitating both legal and illicit transfer of U.S. technology, intellectual property, and know-how, and we have to be cognizant of that in the community.

So across our research domain and spectrum we are thinking about that. It isn't just about protecting against hacking, although that is certainly a big part of it, it is all of those ways that they have to try to capture that intellectual property, which I think is what you were alluding to.

Mr. HICE. Absolutely it is. And I know some of this probably would be best served in another environment than this.

Dr. PORTER. Right.

Mr. HICE. But I would like to dive deeper into this issue if we can in another setting.

But going back to what Mr. Larsen said, I want to just get a little more clarity. How do you plan to recruit talented data engineers and scientists? Specifically in the near term, I guess.

Mr. DEASY. Right. So right now, we have approximately 30 people inside. It is a combination of civilians, which are DOD employees, as well as military.

The philosophy is over time we are going to need to actually build out an internal capability that will include people inside the military.

So what we have done recently is we brought in 10 very highly talented, skilled individuals from the various services into JAIC. We are going to team them with data scientists, "been there, done it" people that we are recruiting. And the idea is to use this pairing system so people can leave JAIC, go back into the services, and then use that to increase the flywheel.

How we are recruiting people is a combination of commercial contacts, academia contacts, think tank contacts. We have quite a list of people that we are currently identifying.

We expect at some point we may have to put something in place like the Cyber Excepted Service, which is going to allow us to recruit in a way that has a lot of additional speed. It is going to have to handle compensation differently. And it is going to handle how we onboard them in a much better fashion than you would normally onboard into government.

Mr. HICE. Okay. Thank you very much. I yield back.

Ms. STEFANIK. Mr. Veasey.

Mr. VEASEY. Thank you, Madam Chair.

I wanted to ask Dr. Porter or Mr. Deasy about the $2 billion that DARPA has announced as a multiyear investment for AI Next.

Can you explain to me exactly what the $2 billion is going to be used for? Is it just to sort of develop a kind of a basic groundwork on how we should move forward? Or is it going to advance specific technologies?

Dr. PORTER. So it is kind of both, because that is what DARPA does. Now, to be clear, the $2 billion is over 5 years, so it is roughly $400 million a year. And they have several thrust areas that target these problems that I was talking about.

So one I already told you about, this Exploration program, and this is that really rapid getting stuff out there and getting really great ideas funded. So we do exactly what you just said and provide that foundation for larger efforts.

There is also a lot of focus on what I mentioned, adversarial AI. This is where it has been proven, and if you read the popular press there are these examples that people are publishing almost daily now, where they can spoof AI systems pretty easily.

One of the ones that is notable, because in the self-driving car community they really took note of this, is there is a team at Berkeley, at the school out in California, they put tape on stop signs. And when you put the tape on the stop signs, the AI system thought the stop sign was a speed limit sign for 45 miles an hour. So you can imagine that is a little bit of a problem, right?

And there are countless examples of this now. It is almost a game now where people are showing all the ways they can spoof these systems.

So, obviously, if we are going to trust this and we are going to apply it to things where there are high stakes, i.e., the DOD mission, we have got to do much better at understanding how we en-

sure that people can't spoof our systems. There is a lot of research to be done there, and that is one of the key thrust areas in the AI Next program.

Mr. VEASEY. As we try to gain a better understanding, is the $400 million, is that like a good starting number? Or where does the number ideally need to be in order for us to sort of stay on track?

And right now, I think you had mentioned earlier that when it comes to China and other competitors, that we actually are ahead. But financially, like where do we need to be to make sure that we stay ahead and that we can continue to work on things like making this AI more smarter, to where tape can't throw it off?

Dr. PORTER. You have got it.

I think it is a reasonable investment level. And one of the things DARPA likes to emphasize, which I fully agree with, is it is not just the amount of money you invest in, it is how you do it.

So DARPA has a model, right, where they try things that a lot of people won't try because it is risky and it may not pay off. And if it doesn't work, no harm, no foul, we will try something else, because we are trying to pursue the really hard things.

That whole model that DARPA has is pretty unique, and, in fact, when you couple that with a robust funding effort, as the $2 billion over 5 years is, you can actually get significant jump-aheads. And that is really what I am trying to emphasize here. That is one of our unique secret sauce ingredients in the United States.

Mr. VEASEY. Thank you very much.

Madam Chair, I yield back.

Ms. STEFANIK. Mr. Bacon.

Mr. BACON. Thank you both for being here. I am grateful for your expertise and sharing it.

It seems to me that until a few years back, or maybe even a decade ago, DOD would drive a lot of the technology. The private sectors would then leverage that. And then we saw a period of time where there was probably a lot of even synergy.

But in my visits recently to the private sector and some of the larger companies, it seems to me they are producing technology faster than DOD can install it, or with the requirements process, testing, by the time we do field it, it is already 2 to 3 years out of date, if not more.

Are we positioning ourselves right in the AI to stay abreast and not fall behind?

Dr. PORTER. So I will start, and then I will, because I think this is a joint answer.

I think you highlighted the problem we are very much interested, the two of us, in trying to address. If we do nothing else, we are going to still have this problem, because even if DARPA gets us ahead of the game and the private sector takes off with those ideas and goes their own way and creates these great products, we have got to have a way to more rapidly transition that innovation back in, learn from it, and continue the cycle.

And both Dana and I have talked multiple times about the speed challenge, and this is why we are really trying very hard to figure out, how do we coordinate that cycle, so that spin cycle, if you will,

so that we get multiple spins very quickly, rather than three, four, five multiple-year cycles just to insert something.

It is not solved, but I think what you are seeing here is a real serious attempt by the DOD to say, let's line this up so that we can improve this.

Would you not agree?

Mr. DEASY. Yeah. As someone who spent the majority of my career in the private sector, I am often asked when I arrive, what is it I have noticed most, and I say clock speed. How fast we can embrace, either decide to work with something, get rid of it and move on.

And one of the reasons we created the relationship we created was you need two things in AI to be successful. You need a maniacal focus on the here and now of operationalize and getting things up and running, and that is that flywheel I talk about. But you also need an intense focus on where the future is going, where the science is going.

And you need a place to take that science. In this case, what DARPA develops. Bring it in, rapidly decide whether or not it can work or not work. If it doesn't work, move on. Tell DARPA that is the case. Or if it is working and it just needs tweaking, then let's do that.

This is why we think this model we have put in place is actually going to help to address the very problem you raise on how do we get the flywheel of innovation moving at a lot faster clock speed.

Mr. BACON. Are we confident DARPA is abreast of all of what the various private sector companies are doing? I mean, do they have their fingers on the pulse of a lot of different companies? Are we confident of that?

Dr. PORTER. So we are confident, but that is why we also have DIU in our quiver. Because, as you know, DIU sits out in Silicon Valley, but also sits in Austin, Texas, sits in Boston, and it is keeping its finger on the pulse.

And, again, where they are going to really see the innovation is a little bit nearer term, but it is that nice bridge between where DARPA may be looking a little further out, DIU is going to see where opportunities are in the next 12 to 24 months, which is much shorter than where DARPA typically looks.

So we try to cover that landscape appropriately——

Mr. BACON. Right

Dr. PORTER [continuing]. So that we are seeing everything we should be seeing.

Mr. BACON. Two follow-on questions. Do we need to make any revisions to our acquisition rules processes to help you out, one.

Two, when I was recently visiting a company this past week, they would say they come up with new technology, but because the DOD didn't have a requirement for it, they didn't want to really look at it. However, later on, they would say, yeah, basically the requirements were shortsighted because they didn't realize what the technology—what could be executed or applied.

So my question, two of them, do we need to make any revisions to our acquisition system? And two, do your requirements keep up with some of the far-ranging technologies that you are seeing in AI?

Thanks.

Mr. DEASY. So I will start with the first half of that, the acquisition.

What I tell people often is, one of the things that we struggle with at the DOD and government is what I call a startup mentality. How you start AI is a very iterative process. And many times the acquisition cycles are asking you to define 30, 60, 90, 2, 3, 1 year, 2 years out, what the end state will look like.

I am just trying to get the end state identified for the next 90 days, 120 days, and then allow us to create this, what I will call this iterative approach for how we are going to build out. We are going to try a solution, we may acquire a product. We will say that product didn't quite meet the needs, and then we are going to need to go back out in a very rapid cycle.

So, yes, I do believe there will need changes, and I believe it is going to be, how do we move to a more startup mentality when looking at technologies like AI?

Ms. STEFANIK. We will now move to the second round of questions and get through as many as we can before they call votes.

My second question has to do with a previous testimony before this committee. I believe it was Deputy Secretary Shanahan talked about the fact that there are hundreds of AI projects and programs within the DOD.

Can you speak, Mr. Deasy, to how we plan on integrating those programs into the JAIC and how that process is going? And can you also highlight one of the best examples of an AI program that was started within the DOD that we can learn from?

Mr. DEASY. Yeah. So clearly what the Deputy was referring to is there are a lot of programs that are using data learning, machine learning, cognitive. You have to be quite thoughtful when describing what is the universe of AI. I would argue that some of those programs, when you really kind of dig under the covers, are more business analytics, as they are as to true, what I will call, machine learning.

With that said, there is no doubt that one of the biggest benefits that JAIC will bring is trying to reduce the replication and the duplication of tools, processes, and, frankly, methodologies that are being used.

A good example of this—and it actually brings DIU into it—is you think about the predictive maintenance. So this is an area where how do you look at helicopters, planes, ships, anything where there is a need to reduce the waste and the cycle time of readiness. This is an example where DIU went out and did some work, found some solutions in the marketplace. They are now bringing that to us.

One of our first initiatives is predictive maintenance, and we are actually going to use the learnings from DIU and the commercial offerings as a way we are going to jump-start the predictive maintenance.

Ms. STEFANIK. Thank you.

Mr. Langevin.

Mr. LANGEVIN. Thank you.

So for Mr. Deasy, our military force projection capabilities are developed and tested almost entirely within the continental United

States, but the nature of warfighting is largely expeditionary. That is, the great majority of warfighting is going to occur far away from the wide infrastructure and domestic regulatory constraints of the U.S., requiring flexible access to maneuver within a different electromagnetic environment.

What role do you see for AI in overcoming this challenge? And how would it potentially apply to other domains like space and cyber?

Mr. DEASY. So interesting enough, I just came back from a Five Eyes† meeting over in the U.K. in which we discussed with our mission partners what is the role that AI can play in a lot of spaces. You mentioned the one, electromagnetic spectrum. I mean, the nature of electronic warfare is such that trying to degrade, spoof, and change the nature of spectrum is such that clearly AI can play a role in being able to quickly assess where spectrum has been compromised and how do you then change the nature of the use of that spectrum.

Another example is, if you think about mission partner networks and how we need to share data in a classified or confidential manner, we see that AI will be able to use, much to my earlier comment, patterns and changes of behavior as we are sharing data across our mission partner networks. And so we have had conversations recently with our partners on what is it that we should be doing more joined up in the matter of these AI initiatives.

Mr. LANGEVIN. Okay. Thank you. That is encouraging.

Also, getting back to data, what efforts are you taking to set standards and guidance for data integrity? And finally, what efforts are being taken to provide for a common lexicon for AI and machine learning?

Mr. DEASY. So on the data front, one of the things that we are doing, for example, is we are working now with the CMO [Chief Management Officer] office. They have actually hired a Chief Data Officer. And on the reform side, we are doing some early work, because I have been quite a proponent of saying that we are going to have to solve for do we really understand where the sources of our data come from, what I like to refer to as the single source of the truth.

So we are partnering with the CMO and the Chief Data Management Officer to start to identify what are those going to be, those problematic data sets, where we are going to have to get clearer standards, especially in the back office area of reform. That is the area we are focusing on right now in the Chief Data Management Officer.

Mr. LANGEVIN. Dr. Porter, do you have anything to add to on that?

Dr. PORTER. Regarding the data integrity issue I think——

Mr. LANGEVIN. Press your mic [microphone].

Dr. PORTER. Oops. I am sorry about that. Regarding data integrity there is also a research component to that as well. And, again, it gets back to, as people recognize how important your data is to training your algorithms, they are going to try to mess with your data, right?

†Australia, Canada, New Zealand, United Kingdom, and United States intelligence alliance.

And so there is both the how do you ensure you are thinking about AI not in an isolated way, but as was raised earlier in the context of cybersecurity and other elements in your system that have to work together.

And so one of the things I like to emphasize, which I think you were touching on when you asked questions about space and so forth, AI doesn't really mean anything until you think about it in the context of the larger system that you are using it in.

So how does it apply to your mission usually means it has to be part of a larger system. How does it get integrated in a way that you don't open up vulnerabilities because you have forgotten that, wow, if my data is really easy to get into someone is going to mess with it, so that I am training on the wrong thing, as an example.

So there are research elements of this, because we have to take a system-level approach, as we do with all technology, when we think about integrating it into operations.

Mr. LANGEVIN. So the last question I had is, to what extent are the Department's challenges based on development of AI technology—e.g., data processing and neural network algorithms—versus a lack of infrastructure, such as big data repositories, compute power, and cloud capabilities?

Mr. DEASY. [Indaudible]

Mr. LANGEVIN. Microphone.

Mr. DEASY. Thank you, sir. I will start with that.

So I mentioned earlier the cloud. If you kind of step back for a second and say, what has happened that has allowed AI to suddenly be on the forefront of all conversations? And I would argue there is the data science behind this, and I would say we have entered an era now where there is unlimited compute power. AI needs a massive amount of computer power, a massive amount of storage, and, of course, you need the algorithms behind it.

The reason why I have been so vocal and energized about wanting to get to an enterprise cloud capability is I want to provide the Department of Defense with a way to handle that unlimited compute capacity, unlimited storage, on demand, as needed, with high integrity.

And this is why I have been such a strong advocate about pushing the need for an enterprise cloud solution, because the enterprise cloud is going to become the foundation for which all the data and all that compute power will reside on top of and those algorithms will use.

And understand that when I talk about cloud, I am not talking about a centralized, single repository. I am talking about a world where we need to work in a decentralized world. If you are out at the warfighter, tactical edge, and we need to be able to work in what I will call a compromised, degraded mode. So it is clouds that can handle the edge, all the way that clouds can handle the central.

Mr. LANGEVIN. Thank you. My time has expired, so I yield back. Thanks.

Ms. STEFANIK. Thank you very much to our witnesses.

Votes have been called. For other members who we didn't get to your second round of questions, please submit your questions for the record.

And thank you, Dr. Porter and Mr. Deasy, for the testimony today. We look forward to discussing this in the next Congress. And I know I look forward to working with Mr. Langevin on it. Thanks.

Mr. DEASY. Thank you.

Ms. STEFANIK. The hearing is adjourned.

[Whereupon, at 4:30 p.m., the subcommittee was adjourned.]

A P P E N D I X

DECEMBER 11, 2018

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

DECEMBER 11, 2018

Opening Statement
Chairwoman Elise M. Stefanik
Emerging Threats and Capabilities Subcommittee
Hearing on

Department of Defense's Artificial Intelligence Structure, Investments, and Applications

December 11, 2018

The subcommittee will come to order.

Welcome, everyone, to this open hearing of the House Armed Services Subcommittee on Emerging Threats and Capabilities. Today we will examine the Department of Defense's efforts to transform the delivery of Artificial Intelligence-enabled capabilities to the warfighter. AI and Machine Learning are topics of regular conversation and deep interest among the members of this subcommittee as we build a blueprint for the battlefield of the future. Over the last year, we have explored these technology issues closely and heard from numerous outside subject matter experts on the emerging opportunities, challenges, and implications of adopting commercial Artificial Intelligence solutions into the defense enterprise. We have also closely examined our adversary's investments in Artificial Intelligence and related technologies, including China's whole-of-society approach, which threaten our competitive advantage.

In response, this committee has taken deliberate, bipartisan actions to better organize the Department of Defense to oversee, accelerate, and integrate Artificial Intelligence and Machine Learning technologies. The John S. McCain National Defense Authorization Act for Fiscal Year 2019 directed the Secretary of Defense to conduct a comprehensive, national review of advances in AI relevant to the needs of the military services. Section 238 further directed the Secretary to craft a strategic plan to develop, mature, adopt, and transition Artificial Intelligence technologies into operational use. Additionally, Section 1051 established the National Security Commission on AI, an independent entity inside the executive branch to take a holistic view of the competitiveness of U.S. efforts and elevate the national conversation surrounding the national security implications of AI.

Today, we will continue the conversation and hear about the DoD's efforts to reorganize and more effectively oversee the execution of AI programs across the military services. We will also examine the Department's investments in basic research to generate groundbreaking AI capabilities for future conflict. The transformation and prioritization of AI inside the Department today will shape the efficiency of DOD's business functions, and most importantly, the effectiveness of our forces in future battle.

Let me welcome our witnesses today:

Dr. Lisa Porter
Deputy Undersecretary of Defense for Research and Engineering at the Department of Defense

And -

Mr. Dana Deasy
Chief Information Officer at the Department of Defense

We look forward to your testimony. Finally, I would like to recognize and express my gratitude to two staff who will be departing the committee this month, Neve Schadler and Mark Pepple. These hearings could not occur without your tireless efforts. Your contributions to the committee did not go unnoticed, and we wish you the best of luck in your future endeavors.

Let me also welcome Chairman Thornberry who has joined us here this morning. Welcome Mr. Chairman and we're glad you can be here.

Without objection, the witnesses' prepared statements will be made part of the record. I ask the witnesses please keep your remarks to no more than 5 minutes.

Dr. Porter, we will begin with you.

STATEMENT BY

DR. LISA PORTER
DEPUTY UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING

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

ON

"Department Of Defense's Artificial Intelligence Structures, Investments, And Applications"

December 11, 2018

NOT FOR PUBLICATION UNTIL
RELEASED BY THE HOUSE ARMED SERVICES COMMITTEE

Chairwoman Stefanik, Ranking Member Langevin, and distinguished Members of the Subcommittee – thank you for inviting me to appear before you today to discuss artificial intelligence, particularly as it relates to national security applications.

As this Subcommittee knows, artificial intelligence, or "AI," is not a new thing – as long as there have been computers, there have been engineers who have dreamed about enabling machines to think the way humans do. In fact, the Defense Advanced Research Program Agency (DARPA) funded much of the early work in AI decades ago. These efforts led to "expert systems," such as tax preparation software, that people take for granted today. But these early systems were limited to very narrow applications and could not generalize.

Today we are experiencing an explosion of interest in a sub-field of AI called "machine learning," where algorithms have become remarkably good at classification and prediction tasks when they can be trained on very large amounts of data. There are numerous examples of successful applications of machine learning techniques; some of the obvious ones include facial recognition in photographs and voice recognition on smart phones. However, there has also been a significant amount of hype and confusion about the current state of the art. It is the USD(R&E) position that we must not abandon the tenets of scientific rigor and discipline as we pursue the opportunities that AI presents.

Today's AI capabilities offer potential solutions to many defense-specific problems; examples include object identification in drone video or satellite imagery, and detection of cyber threats on networks. However, performance must be assessed rigorously against quantitative metrics that are directly tied to the specific mission problem. For example, most commercial search applications focus on precision – meaning that, if I ask for images of cats, every image that comes back to me has a cat. Such algorithms may not do as well with recall – in other words, I may not get all the images that have cats in them. A metric that emphasizes precision over recall may not be appropriate for a military application where I am looking for, say, missile launchers, and I may be willing to accept some false alarms (lower precision) as long as I do not miss any launchers (higher recall). If I do not optimize my algorithm against the proper metric, I will not get the performance I need.

A related challenge to proper metric selection is determining the performance level required for operational utility. Oftentimes, current systems and capabilities are not quantitatively benchmarked, making it difficult to know what level of performance to target, and therefore how to assess whether the expected outcome will justify the development and system integration expenditures.

One of the drawbacks of today's machine learning techniques is the amount of human labor required to properly prepare, or "curate," the training data. For example, the impressive advances

in object detection and classification in imagery during the past few years came about largely because of the arduous two-year data labeling campaign led by Dr. Fei-Fei Li, which employed over 50,000 workers ("Mechanical Turks") from 167 different countries to generate about 15 million curated images. But while the performance of algorithms trained on this extensive data set against similar imagery is quite impressive, their performance against different kinds of imagery, such as satellite imagery, is not. In other words, despite all of the successful examples of current machine learning systems, they are narrow in what they can do, they are brittle, and they cannot explain what they do – which makes them hard to trust. Furthermore, current systems require robust processing power. And finally, current systems are susceptible to various forms of spoofing, known as "adversarial AI."

We are working to address these challenges and vulnerabilities – metric selection, data curation, trust, processing power, and adversarial AI – through multiple efforts, most of which will leverage the complementary roles of the Joint Artificial Intelligence Center (JAIC) and the USD(R&E) enterprise. The JAIC will offer a means to rapidly determine the appropriate metrics for operational impact for a variety of applications, and these insights will help inform algorithm and system development across multiple USD(R&E) research efforts. Furthermore, the JAIC's focus on scaling and integration will drive innovation in data curation techniques. A specific example of the synergy that we plan to foster between our organizations is a recent partnership between the Defense Innovation Unit (DIU) and the JAIC focused on predictive maintenance, where DIU chose a successful commercial airline industry supplier to prototype a six-month pilot program for E-3 Sentry aircraft maintenance. DIU and the JAIC are now working together to scale this solution across multiple aircraft platforms, as well as the Army's Bradley Fighting Vehicle.

In order to address AI's "trust issue," DARPA's Explainable AI program aims to create machine learning techniques that produce more explainable models while maintaining a high level of performance, while USD(R&E), together with the Service Labs and our international partners, is pursuing methods, tools, and techniques to enable rapid verification, evaluation, and certification of autonomous and AI-based systems. The High Performance Computing Modernization Program is designing new systems that will provide ample processing power for AI and machine learning applications on the battlefield. Finally, countering adversarial AI is one of the key focus areas of DARPA's $2 billion AI Next campaign.

Ultimately, as we look to the future, we anticipate a focus on developing AI systems that have the ability to reason as humans do, at least to some extent. Such a capability would greatly amplify the utility of AI, enabling AI systems to become true partners with their human counterparts in problem solving. As an example, an AI system with sense-making capabilities could advise a warfighter in a time-sensitive situation on what action to pursue, enhancing the decision-making process by discounting the human's own biases. This goal is the quintessential

"DARPA-hard" problem, and we anticipate many false starts as we pursue it over the coming years. Nonetheless, it is important that we continue to pursue this cutting-edge research, given the significant investments our adversaries are making in AI. We are therefore grateful for the leadership and support that the Members of this Subcommittee have shown regarding AI. We also appreciate the establishment of the National Security Commission on AI, whose charter is appropriately focused on key areas that must be assessed objectively to ensure that the US maintains a leadership position in AI-enabled technologies and systems.

Thank you for your interest in this important topic, and I look forward to answering your questions.

Dr. Lisa J. Porter
Deputy Under Secretary of Defense for Research and Engineering

Dr. Lisa Porter is the Deputy Under Secretary of Defense for Research and Engineering (DUSD(R&E)), and with the USD(R&E), is responsible for the research, development, and prototyping activities across the DoD enterprise. In addition, the USD and DUSD oversee the activities of the Defense Advanced Research Projects Agency (DARPA), the Missile Defense Agency (MDA), the Strategic Capabilities Office (SCO), Defense Innovation Unit (DIU), the DoD Laboratory and Engineering Center enterprise, and the Under Secretariat staff focused on developing advanced technology and capability for the U.S. military.

Dr. Porter previously served as Executive Vice President of In-Q-Tel (IQT) and Director of IQT Labs. Prior to joining IQT, Dr. Porter was the President of Teledyne Scientific & Imaging. She was the first Director of the Intelligence Advanced Research Projects Activity (IARPA) in the Office of the Director of National Intelligence (ODNI), and also previously served as the Associate Administrator for the Aeronautics Research Mission Directorate at the National Aeronautics and Space Administration (NASA). Dr. Porter also served as a program manager and senior scientist at the Defense Advanced Research Projects Agency (DARPA).

Dr. Porter holds a bachelor's degree in nuclear engineering from the Massachusetts Institute of Technology and a doctorate in applied physics from Stanford University. She received the Office of the Secretary of Defense Medal for Exceptional Public Service in 2005, the NASA Outstanding Leadership Medal in 2008, the National Intelligence Distinguished Service Medal in 2012, and the Presidential Meritorious Rank Award in 2013.

STATEMENT BY

DANA DEASY
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER

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

ON

"Department of Defense's Artificial Intelligence Structure, Investments, and Applications"

December 11, 2018

NOT FOR PUBLICATION UNTIL
RELEASED BY THE HOUSE ARMED SERVICES COMMITTEE

Good afternoon Ms. Chairwoman, Ranking Member, and distinguished Members of the Subcommittee. I thank you for the opportunity to spend a few minutes on the establishment of our Joint Artificial Intelligence Center (JAIC), an effort that is of great importance to the Department of Defense and to our country, in a technology area that is profoundly significant to industry, academia, and society writ large.

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, and senior leadership and nuclear command, control, and communications (NC3) matters. I am also responsible for the success of the Department's new Joint AI Center. Several of these 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.

Artificial intelligence (AI) is rapidly changing a wide range of businesses and industries. It is also poised to change the character of the future battlefield and the pace of threats and capabilities we must face. The 2018 National Defense Strategy (NDS) foresees that ongoing advances in AI "will change society and, ultimately, the character of war." Structurally, we know AI has the potential to be an enabling layer across nearly everything -- that means countless applications in industry and everyday life, and it means the opportunity to positively transform every corner of the Department, from innovative concepts that change the way we fight, to improvements in the way we maintain our equipment, perceive our environment, train our men and women, defend our networks, operate our back office, provide humanitarian aid and respond to disasters, and more. The adoption of AI in defense enables us to better support and protect American servicemembers, safeguard our citizens, defend our allies, and improve the affordability, effectiveness, and speed of our operations.

Other nations, particularly China and Russia, are making significant investments in AI for military purposes. These investments threaten to erode our technological and operational advantages and destabilize the free and open international order. The Department of Defense, together with our allies and partners, must adopt AI to maintain its strategic position, prevail on future battlefields, and safeguard this order.

Under the NDS, the Department will accelerate the adoption of AI to expand our military advantages and create a force fit for our time. AI will enhance operational effectiveness, improve readiness, and increase efficiency in the general business practices of the Department. As we move out, we will make concerted effort to move AI technologies in a direction that improves our odds of security, peace, and stability in the long run by promoting vigorous dialogue and multilateral cooperation on the safe and ethical use of AI for national security and establishing new norms for responsible behavior, consistent with the law and our nation's values. This AI transformation will ensure that we maintain the ability to execute the Department's vital mission of protecting the security of our nation, deterring war, and preserving peace.

Last June, Deputy Secretary Shanahan directed my office to establish the Joint AI Center. This is a new unit whose goal is to accelerate the delivery of AI-enabled capabilities, scale the Department-wide impact of AI, and synchronize the Department's AI activities. In parallel, the Department submitted its first AI Strategy to Congress, an annex to the NDS that captures the integrated set of decisions we are making now to harness AI to advance our security and prosperity. The founding of JAIC also dovetailed Section 238 of the FY19 National Defense Authorization Act, which directed a joint approach to coordinate the efforts of the Department to develop, mature, and transition AI technologies into operational use. Today, I will provide you with an update on the establishment of JAIC. I will touch on how we are partnering with Research & Engineering (R&E), the role of the Military Services, the Department's initial focus areas for AI delivery, and how JAIC is supporting whole-of-government efforts in AI.

JAIC will operate across the full AI application lifecycle, emphasizing near-term execution, experimentation, and operational adoption to meet current needs. JAIC's work will complement the efforts of R&E, which are focused on foundational research, longer-term technology creation, and innovative concepts. You will hear JAIC communicate a clear and consistent message about transforming DoD through AI. This refers to the transformation that happens when you field technology on operationally-relevant timelines, enable men and women to experiment with it based on their own creativity, and ultimately generate new ways of working that solve our most critical challenges and expand our military strength. As we move to rapidly incorporate AI, those men and women in America's military will remain our enduring source of strength; we will use AI-enabled information, tools, and systems to empower, not replace, those who serve.

To derive maximum value from AI application throughout the Department, JAIC will operate across an end-to-end lifecycle of problem identification, prototyping, integration, scaling, and support. JAIC will partner with the Services and other components across the Joint Force to systematically identify, prioritize, and select new AI mission initiatives, and then stand up cross-functional teams to rapidly execute a sequence of use cases that demonstrate value and spur momentum. This includes engaging with leading commercial and academic partners for prototypes, fostering new forms of experimentation, and employing standardized processes with respect to areas such as data management, testing and evaluation, and cybersecurity. Our approach has been directly informed by the Department's AI pathfinder activity, Project Maven, which has been successful in identifying and beginning to address key challenges with integrating AI into operations and has put in place an initial set of data, tools, and infrastructure for AI delivery, as well as initial templates for acquisition, testing and evaluation, operational assessment, and more.

JAIC's early projects serve a dual purpose: to deliver new AI-enabled capabilities to end users as well as to help incrementally develop the common foundation that is essential for scaling AI's impact across DoD. This foundation includes shared data, reusable tools, frameworks, libraries, and standards, and AI cloud and edge services. JAIC will work with teams throughout the Department to ensure that they can leverage this foundation to accelerate their progress in a manner that aligns with DoD enterprise cloud adoption. Let me underscore that point: our enterprise approach for AI and enterprise cloud adoption via the DoD-wide Cloud Strategy are mutually reinforcing, mutually dependent undertakings. Finally, JAIC will provide ongoing

support to the efforts of the Services and other organizations to ensure continuous improvement, assessment, and sustainment of AI systems and solutions across the enterprise.

The AI capability delivery efforts that will go through this lifecycle will primarily fall into two categories: National Mission Initiatives (NMIs) and Component Mission Initiatives (CMIs). As outlined in the DoD AI Strategy, a National Mission Initiative (NMI) is a pressing operational or business reform joint challenge, typically identified from the National Defense Strategy's key operational problems or nominated by a mission owner, which can only be solved by multi-service innovation, coordination, and the parallel introduction of new technology and new operating concepts. NMIs are typically driven by JAIC and are executed by cross-functional teams that are comprised of both JAIC personnel as well as subject matter experts from across the Department on a rotational basis. Execution of these projects will be essential for putting in place our initial common foundation.

The second project category is a Component Mission Initiative (CMI), which is a component-level challenge that can be solved through AI. JAIC will work closely with individual components on CMIs to help identify, shape, and accelerate their component-specific AI deployments through usage of common foundational tools, libraries, cloud infrastructure, etc., application of best practices, partnerships with industry and academia, etc. The component will be responsible for identifying and implementing the organizational structure required to accomplish its project in coordination and partnership with JAIC.

We are already forming strong partnerships with the Services and key components: for example, the Army established a new AI Task Force that is working closely with JAIC on predictive maintenance, we are actively engaged in an effort to apply data-driven insights to equipment availability at U.S. Special Operations Command and in the U.S. Air Force in partnership with Defense Innovation Unit (DIU), and we are partnering with U.S. Cyber Command to shape a new mission initiative together. These early efforts each make use of common approaches to data, tools, libraries, architectures, development approaches, and more. Additionally, we are already seeing encouraging signs that the Services are increasing their levels of investment in AI-related capabilities; this is exactly what we want to see happen.

JAIC's focus on near-term AI implementation and adoption complements efforts within the Office of the Under Secretary of Defense for Research and Engineering (R&E), at places such as the Defense Advanced Research Projects Agency (DARPA) that are focused on the next wave of AI research and longer-term technology creation. When it comes to research for the future versus the ability to apply it now at scale, DoD needs the best of both, and they feed one another: R&E will feed JAIC with updates on leading-edge AI technologies and concepts, and JAIC will provide R&E insights from operational fielding, user feedback, and data. Dr. Griffin, Dr. Porter, and I have a shared vision on this enterprise approach. JAIC is already working with DIU, DARPA, and the Strategic Capabilities Office to improve integration and enhance unity of effort on current and future AI projects.

Last week, I gave the opening remarks at the DoD AI Industry Day, an event put together through a partnership among JAIC, Project Maven, and the Army Research Lab, with strong participation from several other DoD components as well as attendance from a few HASC staff

members. I shared with the nearly 400 companies in attendance that we had achieved a significant milestone: JAIC is now up and running, and open for business. Examples of early mission initiatives include the following:

- **Perception –** Improve the speed, completeness, and accuracy of Intelligence, Surveillance, Reconnaissance Processing, Exploitation, and Dissemination. Project Maven's efforts will be included here.

- **Predictive Maintenance (PMx)** – Provide computational tools to decision makers to help them better forecast, diagnose, and manage maintenance issues to increase availability, improve operational effectiveness, and ensure safety, at reduced cost.

- **Humanitarian Assistance/Disaster Relief (HA/DR)** – Reduce the time associated with search and discovery, resource allocation decisions, and executing rescue and relief operations to save lives and livelihood during disaster operations.

- **Cyber Sensemaking** – Detect and deter advanced adversarial cyber actors who infiltrate and operate within the DoD Information Network (DoDIN) to increase DoDIN security, safeguard sensitive information, and allow warfighters and engineers to focus on strategic analysis and response.

We picked these initiatives to deliver mission impact at speed, demonstrate the proof of concept for the JAIC operational model, enable rapid learning and iterative process refinement, and build out our library of reusable tools while validating our enterprise cloud architecture. As did Project Maven, these efforts will benefit us by growing more AI expertise that will return to the Services and components to help accelerate their own AI projects.

For the predictive/preventive maintenance NMI, we are starting with Army and Army Special Operations helicopters (H-60s). There is sufficient data available to train algorithms, there will be well-defined return on investment criteria, and this project helps address Secretary Mattis' direction to the Services to improve their maintenance readiness rates. We anticipate moving to other airframes and vehicles once the H-60 project is well underway, working closely with DIU to scale the promising results they have demonstrated using AI for predictive maintenance on other Air Force and Army platforms.

For the humanitarian assistance and disaster relief (HA/DR) NMI, we are already applying lessons learned and reusable tools from Project Maven to field AI capabilities in support of events such as hurricanes and wildfires, disasters in which DoD plays a supporting role. One of the most important benefits of this NMI is that it is an inspiring, societally-beneficial, life-saving mission that is not only whole-of-government but whole-of-society. It brings in interagency, state and local governments, non-governmental organizations, allied and partner nations, and more. It offers a unique opportunity to combine DoD efforts with industry and academia in a new type of public-private endeavor to operationalize AI to solve our most challenging problems. Doing this at scale to address disasters on an integrated basis creates the potential to both save lives and livelihood as well as advance common tools, lessons, and partnerships for the benefit of many DoD missions.

While its primary focus is delivery initiatives such as these, JAIC has an important role in synchronizing DoD AI activities. This avoids duplication and excess cost, fosters sharing of lessons, and establishes a new enterprise approach for translating AI into decisions and impact at scale across the Joint Force. Under my CIO authorities and as laid out in the JAIC establishment memo, JAIC will coordinate all DoD AI-related projects above $15 million. This does not mean that JAIC will control the execution of these projects or the funding for Service- and component-level AI initiatives. It does mean that we will start to ensure, for example, that they begin to leverage common tools and libraries, manage data using best practices, reflect a common governance framework, adhere to rigorous testing and evaluation methodologies, and comply with architectural principles and standards that enable scale. Over time, when properly resourced, JAIC will assume a greater role with regard to component AI programs.

JAIC will be a key resource for whole-of-government efforts in AI, particularly as we explore as a Nation the opportunities and challenges associated not merely with fundamental AI research, but also with translating the technology into decisions and impact in operations. To underscore our focus on ethics, humanitarian considerations, and both short-term and long-term AI safety, JAIC is working closely today with the Defense Innovation Board (DIB) to foster a broad dialogue and provide input into the development of AI principles for defense. We are offering our perspective on the crucial research and development associated with operationalizing AI today in our engagements with the important work of the National Science and Technology Council Select Committee on AI. And I want to emphasize the importance of our partnerships with Congress in all areas, but with a particular focus on AI. The establishment of the National Security Commission on Artificial Intelligence in the National Defense Authorization Act for Fiscal Year 2019 is one key example of this partnership and an encouraging step forward.

The ingredients for JAIC to ultimately be successful include: enterprise cloud adoption; world-class AI talent, particularly in areas that are scarce within DoD today such as data engineering, data science, machine learning, and product management; a workforce that is taking steps to become broadly AI-ready; strong partnerships with the Services, Combatant Commands, and other key components; a tight two-way integration with the critical work of R&E; and energetic, combined problem-solving enabled by bonds of trust with AI leaders in industry and academia. The final ingredient for success is culture: specifically, the need for a cultural shift to become a more data-centric, computer science-literate, experimentation-driven organization that is comfortable deriving advantage from risk. These are the table stakes in AI. Our legacy culture and processes are particularly apparent as we launch what can only be described as a startup within the Department of Defense. As we do so, we are incorporating lessons learned from other Department activities that resembled startups in how they responded to urgent, compelling requirements across the Department – such as the ISR Task Force, Joint Improvised Explosive Device Defeat Organization, and Project Maven.

The central challenge laid down by the NDS is preserving and expanding our military advantage. In the era of AI, our ability to do this depends on our ability to integrate the technology on operationally-relevant timelines and adapt new ways of working.

The Joint AI Center will play a critical role in this transformation through the activities I have described: Delivering capability at speed to address key missions; establishing a common foundation for scaling AI's impact across the Joint Force, including shared data, reusable tools, frameworks and standards, and cloud and edge services; facilitating AI plans, policies, and standards, including those that ensure we lead the world in the development of AI solutions that are robust, ethical, and secure; and attracting and cultivating expertise in the form of a world-class AI team and an AI-ready workforce. The speed and scale of the change required is daunting, but we must embrace it if we are to reap the benefits of continued security and prosperity for the future.

Thank you for the opportunity to testify this afternoon. I look forward to continuing to work with Congress in this critical area, in an ongoing dialogue on our progress in AI adoption and the ways in which JAIC is being used to accelerate that progress. 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.

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

DECEMBER 11, 2018

QUESTIONS SUBMITTED BY MR. LARSEN

Mr. LARSEN. How do you assess the ability of military recruits to work with AI? What recommendations would you make to improve K–12 and community college curricula in order to make sure military recruits have the necessary skills and are appropriately prepared to work with AI-related applications?

Mr. DEASY. While some people joining the military today may have skills suited for working with AI, overall we assess that the current state of the existing workforce and military recruitment pipeline is a critical shortfall for DOD. Although means of quantifying this shortfall are still emerging, directional industry benchmarks indicate DOD should build capacity of several thousand people with AI-specific skills, such as data scientists and data coders. National investments in skills training and high-quality K–12 and community college education would be a significant force multiplier for DOD. Classes in computational thinking as early as middle school and again in high school will help establish a foundation for AI skills that will pay dividends in the DOD workforce. Other recommendations to ensure military recruits have the necessary skills and are appropriately prepared to work with AI-related applications include the following:

1. Accelerate the use of digital content and "flipped classroom" pedagogy. There has been a renaissance in digital content such as massive open online courses (MOOC), ebooks, and YouTube videos. This content represents a new category of learning experience that presents several advantages for K–12 and community college—generally high quality, low cost, scalable, and adaptable to the needs of an individual or community. In-person teachers can complement the online content, resulting in faster and more enjoyable learning experiences ("flipped classroom pedagogy").

2. Evaluate guidelines, measurements, and incentives for AI education in K–12. To establish consistent, measurable standards for AI education and training, guidelines, measurements, and incentives should be established across the country for curricula or key skills. As an example of an external effort underway, the Association for the Advancement of Artificial Intelligence (AAAI) and the Computer Science Teachers Association (CSTA) are in the process of formulating guidelines that will define what students in each grade should know in AI.

3. Launch public-private partnerships, including open missions to use AI to solve problems of societal significance. The use of public-private partnerships can bring AI education to more K–12 classrooms throughout the country. One type of partnership involves bringing to K–12 and community colleges national security challenges and forming an open mission to produce innovative AI technology to address real-world problems. Such initiatives would enhance AI education, generate excitement about working with the government, and inform potential recruits of AI-related opportunities within the military. Similar cyberspace initiatives have been very successful.

4. Establish clear pathways between K–12 and AI-enabled roles in military service. Establishing a career track for computer scientists in the military services provides potential recruits a clear path to obtain sophisticated AI-related training and education. Designating AI-related career fields allows for recruiting incentives such as scholarships and bonuses.

5. Prioritize continued learning within military. The unique pace of technological change in AI means that relevant knowledge decays more rapidly than ever before. After entry, incentivizing continual learning within military is imperative to maintain an "AI ready" workforce. This should include expanding opportunities for internships, fellowships, and exchanges between DOD and leading commercial AI companies.

○