[H.A.S.C. No. 116–90]

INTERIM REVIEW OF THE NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE EFFORT AND RECOMMENDATIONS

HEARING

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

HEARING HELD
SEPTEMBER 17, 2020

U.S. GOVERNMENT PUBLISHING OFFICE
42–135 WASHINGTON : 2021

SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES

JAMES R. LANGEVIN, Rhode Island, *Chairman*

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

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

BESS DOPKEEN, *Professional Staff Member*
ERIC SNELGROVE, *Professional Staff Member*
CAROLINE KEHRLI, *Clerk*

CONTENTS

INTERIM REVIEW OF THE NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE EFFORT AND RECOMMENDATIONS

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON INTELLIGENCE AND
EMERGING THREATS AND CAPABILITIES,
Washington, DC, Thursday, September 17, 2020.

The subcommittee met, pursuant to call, at 1:00 p.m., in room 2118, Rayburn House Office Building, Hon. James Langevin (chairman of the subcommittee) presiding.

OPENING STATEMENT OF HON. JAMES R. LANGEVIN, A REPRESENTATIVE FROM RHODE ISLAND, CHAIRMAN, SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES

Mr. LANGEVIN. The subcommittee will come to order.

I want to welcome members participating in today's hearing and, for those remotely, members who are joining remotely must be visible on screen for the purposes of identity verification, establishing and maintaining a quorum, participating in the proceedings, and voting. Those members must continue to use the software platform's video function while in attendance, unless they experience connectivity issues or other technical problems that render them unable to participate on camera. If a member experiences technical difficulties, they should contact the committee staff for assistance.

A video of members' participation will be broadcast in the room and via the television's internet feeds. Members participating remotely must seek recognition verbally and they are asked to mute their microphones when they are not speaking. Members who are participating remotely are reminded to keep the software platform's video functions on the entire time they attend the proceeding.

Members may leave and rejoin the proceeding. If members depart for a short while, for reasons other than joining a different proceeding, they should leave the video function on. If members will be absent for a significant period or depart to join a different proceeding, they should exit the software platform entirely and then rejoin if they return.

Members may use the software platform's chat feature to communicate with staff regarding technical or logistical support issues only.

Finally, I designated a committee staff member to, if necessary, mute unrecognized members' microphones to cancel any inadvertent background noise that may disrupt the proceeding.

Before I go to my opening statement, I understand that there will be votes during the course of the hearing, very likely. So if that occurs, we are going to keep the hearing going is what has been worked out and, unless it becomes an issue, we will see members who will go and vote and they will return as soon as possible but the hearing will continue.

So with that, I am going to now give my opening statement. Let me say that I am pleased to welcome four commissioners from the National Security Commission on Artificial Intelligence, a commission created by this committee in the John S. McCain National Defense Authorization Act for Fiscal Year 2019, to consider the methods and means necessary to advance the development of artificial intelligence, machine learning, and associated technologies to comprehensively address the national security and defense needs of the United States.

Our intent with this Commission was to ensure a bipartisan whole-of-government effort focused on solving national security issues and we appreciate the leadership and the hard of work of our witnesses in supporting the Commission's efforts in that spirit.

Today, we welcome Dr. Eric Schmidt, chairman of the Commission, the Honorable Robert Work, vice chairman, the Honorable Mignon Clyburn, commissioner of the workforce and ethics lines of effort, and Dr. José-Marie Griffiths, commissioner on the ethics line of effort and the chair of the workforce team.

I want to thank you all, first of all, for your service, as well as your other commissioners and look forward to hearing your testimony today.

Our understanding of artificial intelligence started in the 1950s and 1960s through research funded through the Department of Defense's vital science and technology investments by the Defense Advanced Research Projects Agency, or DARPA, and the Office of Naval Research and was aided by the convening power of universities.

Now, more than half a century later, this Commission is working through the difficult issues requiring national investments in research and software development and new approaches on how to, among other things, apply AI [artificial intelligence] appropriately for national security missions, attract and hold onto the best talent, protect and build upon technical advances, best partner with our allies on AI and stay ahead of the threat posed by this technology in the hands of our adversaries, and implement ethical requirements for responsible American-built AI.

Indeed, last year, the Defense Innovation Board, which was also chaired, until recently, by Dr. Schmidt, helped the Department begin the necessary discussion on ethics in AI. Dr. Schmidt, I want to thank you for the 4 years that you led the Defense Innovation Board and I look forward to working with you to make sure that you continue to be able to serve, in some capacity, with the Defense Innovation Board. You are an invaluable resource and we can't lose you.

So I applaud the Commission for being forward-leaning by not only releasing an initial and annual report, as required by law, but also releasing quarterly recommendations. Ranking Member Stefanik and I, along with Chairman Smith and Ranking Member

Thornberry, were pleased to support a package of provisions in this year's House version of the fiscal year 2021 NDAA [National Defense Authorization Act] based on the Commission's first quarter's recommendations. The House version carried 11 provisions, with the majority deriving from the Commission's call to strengthen the AI workforce. We are pleased that both Commissioner Griffiths and Commissioner Clyburn are with us today to testify on the need for action on AI talent.

On that note, we must implement policies that promote a sound economic, political, and strategic environment on U.S. soil, where global collaboration, discovery, and innovation can all thrive. The open dialogue, in-depth resident in academia and the research community can be an anathema to the requirement for secrecy in the Department of Defense but we must recognize and embrace how our free society provides the comprehensive advantage that lets us innovate faster than our great power competitors. Our free society enables a dynamic innovation ecosystem and federally funded open basic research focused on discovery has allowed American universities to develop an innovation base that has effectively functioned as a talent acquisition program for the U.S. economy that is second to none. And that talent is required today, as much as ever, to solve our most pressing national security challenges.

Indeed, great power competition is also a race for talent.

With that, we are looking forward to hearing about your efforts, the observations and recommendations you have already developed, and your plan to continue, until you submit the Commission's final report in the spring.

With that, before turning to our witnesses, I will now turn to Ranking Member Stefanik for her remarks. She has been an outstanding leader on the issue of AI and I am proud to partner with her on this whole effort.

I would like to now recognize Ranking Member Stefanik for her comments.

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

STATEMENT OF HON. ELISE M. STEFANIK, A REPRESENTATIVE FROM NEW YORK, RANKING MEMBER, SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES

Ms. STEFANIK. Thank you, Chairman Langevin.

Welcome to our witnesses, Chairman Schmidt, Vice Chairman Work, and Commissioners Clyburn and Griffiths. It is great to have you before the subcommittee today. Thank you for all of your continued service on this Commission.

I would be remiss if I didn't also thank Yll [Yll Bajraktari] for his incredible work as staff director. I know we are working so closely with you with our subcommittee staff and your team.

On March 20th of 2018, I introduced legislation in the House of Representatives to establish a national commission to review the advances in artificial intelligence, the competitiveness of our efforts, and the implications to our national security. Just a year later, I had the honor of speaking at the AI Commission's first plenary session, meeting many of you and providing my thoughts on

the importance and direction of the Commission's work. And just a few short months ago, I had the privilege of sponsoring, alongside my friend and colleague, Chairman Langevin, 11 amendments to the NDAA that originated from the Commission's first quarter recommendations.

This is truly a remarkable achievement and demonstrates the value of your findings and recommendations to policymakers, and in particular, to this committee. This impressive commitment reflects upon your hard work, the dedication of the staff, and also a recognition of how important and timely this conversation on artificial intelligence is to our national discourse and national defense.

In my comments at the Commission's first session, I spoke about the need for artificial intelligence to be transformative. I had stressed that, if AI doesn't fundamentally change the way we operate, how we view our collective defense, adapt our workforce composition, shift our priorities, and invest our resources, then we are failing to embrace this new technology to its fullest. I am pleased that many of your initial recommendations addressed these issues and I look forward to hearing your comments on how we are doing in these regards.

Over the last several weeks, we have seen glimpses into the power of artificial intelligence. DARPA's AlphaDogfight demonstration, which pitted an experienced Air Force pilot in a virtual dogfight against an algorithm developed by a small woman- and minority-owned business in Maryland. It was a decisive victory for artificial intelligence and one that Secretary of Defense Esper accurately observed as a, quote, tectonic impact of machine learning on the future of warfighting.

In another noteworthy demonstration, we observed a hypervelocity weapon shoot down a cruise missile with the help of an advanced battle management system powered by powerful data analytics and AI capabilities. The head of Northern Command noted afterwards, quote, I am not a skeptic after watching today.

Equally important as these AI technical demonstrations is the formulation of policy governing how we use these capabilities. The development of standards, ethical principles, accountability, and appropriate level of human oversight will be critical to ensuring the American people trust its use. Your work, both on the Commission and in your personal and professional endeavors, is key to ensuring a strong and enduring partnership between the military, academia, and private sector; a partnership built on trust, democratic ideals, and mutual value.

Again, I look forward to discussing the Commission's recommendations and your priorities for the remainder of the Commission's work. Thank you so much for your service and the hundreds of hours you have dedicated to this effort.

I yield back.

Mr. LANGEVIN. Thank you, Ranking Member Stefanik.

Let me now introduce our witnesses. We are pleased to have with us today Dr. Eric Schmidt, chairman of the National Security Commission on AI. Dr. Schmidt is the technical advisor to the board of Alphabet, where he was formerly the executive chairman. His previous roles included the chairman of Google Inc. and CEO [chief executive officer] of Google. He has a distinguished record of

contributions to the national security technology community, including recently chairing the Defense Innovation Board.

Dr. Schmidt, as a commissioner on the Cyberspace Solarium Commission, I would like to begin by thanking you for your commitment to ensure the two Commissions work closely together and all that you have done to make the AI Commission so robust.

Next, we will hear from the Honorable Robert Work, vice chairman of the Commission. Secretary Work is familiar to many of us on the committee, as the former Deputy Secretary of Defense and the Under Secretary of the Navy before that. Secretary Work's commitment to innovative strategic thinking is well known with his related work on the Third Offset Strategy.

Thank you for being here, Commissioner Work.

Next, we will hear from the Honorable Mignon Clyburn. Commissioner Clyburn has spent 9 years on the Federal Communications Commission, where her commitment to closing the digital divide was well known. She has had a distinguished career, fighting for diversity in the communications sector.

Thank you for being here as well, Commissioner Clyburn.

And finally, we have Dr. José-Marie Griffiths. Dr. Griffiths is the president of South Dakota University.

Dr. Griffiths, first of all, I want to thank you, again, for hosting me and my fellow Solarium commissioners 2 weeks ago to release our white paper on the Federal Cybersecurity Workforce. As you and I both know, our institutions of higher education are vital resources in educating the digital natives that we need to help us meet the AI and cybersecurity challenges that we will face in the coming decades.

So with that, I again want to thank our witnesses for being here today and I will turn now to Chairman Schmidt to summarize your comments for 5 minutes.

Chairman Schmidt, the floor is now yours.

STATEMENT OF DR. ERIC SCHMIDT, CHAIRMAN, NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

Dr. SCHMIDT. Thank you so much. I cannot express how grateful I am for the leadership of Chairman Langevin, Ranking Member Stefanik, this Commission, and the things that I and our Commission care so deeply about. It has been a remarkable year working with you all to try to get these things going forward.

The progress we have made, in terms of improving the situation of AI, is a good indicator of what is possible if we continue to work very hard on this. I cannot say enough how important this is.

I think addressing AI, in the way that we are describing, is a unifying topic. It is a bipartisan priority. What is more important than our national security? And when I hear that, I say: What is more important than leadership in AI? I could go on, and on, and on, to the point of boredom, I suspect, of how AI is so exciting. I imagine, if I were a graduate student today, the kind of amazing technologies and solutions I would be able to provide using these new AI techniques that did not exist when I was a computer scientist, as a younger scientist, in particular, the application to biology, and to medicine, and to health, and to the things that we all care and deal with so much in our society.

There is a term in history called the Cambrian explosion and it is the point in history where everything came together to form modern life, and everything aligned at that point, and we are in a similar position now with AI. These AI applications will be the basis for the solution to the COVID pandemic. I believe that, for example, the vaccines, essentially all the ones I have looked at, have had AI as a core part of their research enterprise.

I could just go on and on. Maybe it will help us plan how to allocate the horrible fires and the resources. There are so many areas where we struggle, where these new techniques can make us more effective and efficient.

We have to understand, however, that there are darker sides of this technology and, in particular, I will give you an example of something I am hearing a lot about. AI systems are trained from human behavior; humans have biases. And we don't—we are Americans. We don't believe in prejudice and bias and so we have to work on that. And, indeed, this is a large area of research. Face recognition, for example, is full of biases that are incompatible, today anyway, with the sort of rules of America.

But I am also concerned, and I want to hit this very hard, that the AI systems can be used in ways that really are counter to how you want our country to evolve. It can supercharge adversaries' disinformation campaigns. Most of the disinformation campaigns that I have looked at have been done by large groups of presumably poorly paid and badly managed Russians. Imagine when the same technology is used in scalable machine learning at a scale that is much more pervasive.

It is very clear, and Bob Work is an expert in this, that AI could lead to forms of autonomous warfare. He will say, if you talk to him, that it is fine to make the weapons more effective but that you fundamentally don't want automatic weapon systems that fire without human intervention. And indeed, our military has a rule of human in the loop for that reason.

We already know that authoritarian regimes, very incompatible with our democracy, are using AI technologies to try to consolidate power and homogenize thought; and homogenizing thought gives you an army of sycophants and the rest is history. And certainly, the technologies that are being broadly distributed now could distribute this to terrorists, and the future Osama bin Ladens, and sort of groups that we just don't want access to this.

The other thing that is happening, and in my work with the military I learned from them that they now view a very strong strategic competition with China is on our plate. And I would argue that China is no longer a near peer; they are a peer in this area. They are close enough. And the Commission has spent a lot of time discussing this—how close is it—but from my perspective, within a year or two is close enough to be a serious issue. And there is no question that if the Chinese become leaders in AI, which, in most cases, they are not today—perhaps in TikTok's algorithm but not otherwise—they are going to use it in ways that are inimical to our country's interest. So, we have got to take this really seriously.

So we are going to basically make and continue to make strong recommendations to make AI for good but I want to say right now

that my approach, and I think the Commission's approach, is very straightforward. We want America to win. Right? It is really easy to articulate that way. We need to do whatever it takes with respect to AI to be leadership.

One of you mentioned: Why don't we just set a goal of leading and winning sooner? I completely agree. And part of the reason that we talked about ethics was because we want to win in a way that is compatible with American values, which you all know and you all embrace.

So we have got a series of principles, which I will highlight briefly. We have got to be global leaders in AI. It is not okay if another country, specifically China but there could be others, where they are the innovators ahead of us. Why is this so important? And we can explore this, if you are interested in it, because AI is a new knowledge and reasoning system, it is at the beginning of every new area of inquiry. So every new aspect of science, every new aspect of thought, every new aspect of—every new thing now will start with AI as a contributing accelerator with new data, new insights, and so forth. That is why it is a pervasive technology. It is not like a missile that just gets smarter. Everything gets smarter. It has enormous systems implications to what we are doing and probably, eventually, to society as a whole.

By the way, the government is important here. When I was a graduate student, I was funded by DARPA and the National Science Foundation. I wouldn't have been able to do it without that funding. I didn't have the money. The remarkable relationship that collectively you all established between universities, the private sector, and the Federal Government, primarily, some State governments, is at the root of American exceptionalism in this area and I want to keep it. So, I cannot express the importance of Federal funding in research and these sorts of things. And we have talked about this before in this committee and subcommittee, and I think everyone understands, that the Federal Government funds the research that nobody else can because it is not in their business interest. So, there is a key role for Federal funding research.

Adopting AI for national security, as Congresswoman Stefanik mentioned, is central. She used some examples that are recent but there are example, after example, after example in national security. The most obvious ones involve the intelligence committees—community because they spend a great deal of time with data and AI is very good at sorting through data. I would much rather get heads-up from a computer system that is constantly looking for threats and then have a human say: Oh, that is interesting; I hadn't thought about that. Right, that is what AI can do. That will keep us safe.

We have got to find ways, and we have some proposals, where private sector individuals are flowing into and out of the government and vice versa. The fact that that talent and knowledge is in the private sector; we need it in the Federal Government and we need the Federal Government people in the private sector. We need to make that as easy as possible and we have some recommendations there.

We are going to talk a lot about talent today. The majority of the subsections of our recommendations, so far, have been talent. After

a while, when you work on this, you discover that you can write as many papers as you want, but the fact of the matter is that without the people who understand, this stuff is hard. To be very honest, a lot of it is really hard. I have Ph.D. in this area and it is hard for me. I can imagine what somebody who is trying to struggle through all the complexities. We need a next generation of talent and they need to be in the government working for the Secretary of this, and the Secretary of that, and the DOD [Department of Defense], and the intelligence community, and working for you all on your staffs, and so forth. You need that.

We are going to talk a lot about this and, indeed, Mignon and José-Marie will go into it in some detail.

We really want to emphasize that we want to do this in an American way—free inquiry, free enterprise, and the free flow of ideas, right? The Chinese model is different; it is not compatible with the way we work. There are other models. Let's do this the American way.

And you guys, by the way, did a really good job in terms of counterintelligence threat in research, taking action to protect fields like microelectronics, which we are also very worried about.

So, again, the government is beginning to understand this and beginning to act correctly. What we need to do is we need—we need to get the ethics stuff in agreement. I was part of a team that did a DOD ethics group. I was also part of a team at Google that did some ethics work. There is an emerging consensus of what AI ethics looks like and we include that as part of our report.

And then finally, I think, we need to win all of the tech competitions, not just the AI ones. We have never had a challenger at the level of depth and sophistication that China represents in terms of their innovative capability. We need to take it seriously, in terms of scale.

And I think, frankly, we should publish such a list. If you were to ask me today, I would tell you the list of things that are important are AI, obviously; biotechnology, the basis for a gazillion dollars' worth of industry; quantum computing, something which is hard to understand but incredibly important for national security; semiconductors, huge fight over that; 5G, very important; and advanced manufacturing, a huge basis for industry in our country.

But maybe there are others on that list and I think one of the things that we all should collectively discuss is what that list should be. And again, let me just emphasize, this has to be all around, built around American values.

And I will finish up by saying that we have been working hard with you and your staffs to translate these into specific recommendations. What I have learned in this process is there are all sorts of rules that govern how pieces of the government work. You all knew this. And if we can adjust those rules to be a little bit more focused on getting excellent AI techniques, technologies, getting leadership, getting everybody talking to each other, and all of that, the American model will not just succeed but really thrive.

So, I want to thank you so much for letting me speak.

[The joint prepared statement of Dr. Schmidt, Secretary Work, Ms. Clyburn, and Dr. Griffiths can be found in the Appendix on page 38.]

Mr. LANGEVIN. Thank you very much, Chairman Schmidt, for your leadership and all the work you have done to lead this Commission and give us a lot to think about.

With that, the chair now recognizes the vice chair of the Commission, the Honorable Robert Work. Secretary, you are invited to summarize your remarks for 5 minutes and, without objection, your written testimony will be submitted for the record.

Secretary Work, you may have to unmute your line.

STATEMENT OF HON. ROBERT O. WORK, VICE CHAIRMAN, NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

Secretary WORK. Sorry about that, sir.

Chairman Langevin, Ranking Member Stefanik, and members of the committee, thanks for the opportunity to testify today.

I would like to discuss the importance of capitalizing on AI for our Nation's defense and intelligence capabilities, and then discuss the Commission's view on this year's National Defense Authorization Act in the current House and Senate versions.

The Commission has found, in important ways and as Eric has laid out, AI is going to change how we defend the American homeland, how our intelligence agencies make sense of the world, and how our military deters adversaries and fights on future battlefields.

In the context of homeland security, we see promise in applying AI to border protection, cyber defense, critical infrastructure protection, counterterrorism, and counterintelligence investigations. It will also be central to countering malign information operations designed to create or deepen fissures in our society and undermine confidence in the electoral process.

In the intelligence realm, AI algorithms can sift through vast amounts of data, define patterns, and identify correlations, while automating imagery analysis, and other labor-intensive analytical tasks.

For our military, AI-enabled autonomous systems open up a vast new realm of possibilities for operational concepts and command decision making that will give us advantages in any fight. AI is going to enable new forms of what we call human-machine collaboration, using machines to help humans make better decisions, and human-machine combat teaming, both of which will improve combat effectiveness. If employed responsibly, we believe AI-enabled military systems can also help reduce risk to U.S. service members in the field and protect innocent lives abroad.

In addition, AI will make business functions of the Department of Defense, the entire Federal workforce, for that matter, and sector far more efficient and cost-effective.

The Commission is preparing recommendations in all of these areas. We have moved with an urgency that is commensurate with the opportunity and the national security threat presented by AI. As you know, sir, we have released our interim report last November that articulated a series of initial judgments of all of the Commissioners and we have published over 80 recommendations since. We will publish more next month.

We will deliver our final report to Congress and the President in March 2021. These are going to cover five key areas: research and development, national security applications, talent and workforce, promotion and protection of critical technologies, international partnerships and ethics.

We are encouraged to see several of the Commission's early recommendations reflected in both the House and Senate versions of this year's NDAA and I want to comment on the importance of the legislative action in five key areas.

The current bill encouraging actions to bolster government investment in AI research and development, improve public-private coordination, and establish technical standards. The Commission shares these priorities and endorses them and applauds them.

We want to emphasize the importance of creating a national AI research resource. Right now, we have AI research haves and have-nots. The haves are generally in the private sector and the have-nots are in academia. We are very encouraged in the new recent White House-led investments to establish seven national AI institutes but we believe that the AI research resource would complement and support these efforts.

In terms of defense, Department of Defense organization reform, we have made several recommendations to make sure that DOD puts the proper emphasis on AI and shepherds and monitors the way it is transforming the force.

Microelectronics, we need to preserve our leadership in this and we have put forth several recommendations to lay the groundwork for long-term access to resilient, trusted, and assured microelectronics.

The fourth area is ethical and responsible use. We have spent a lot of time on this and Eric has talked about that, so I won't dwell on it anymore.

And the fifth area is the Federal Government's AI workforce. I am going to leave that up to José-Marie and Mignon to discuss in detail.

So let me just stress we must grasp the inevitability of AI and out-innovate, out-invest, out-strategize, and outwit our competitors.

I thank this committee so much for devoting so much attention to including AI in developing this year's NDAA. We are extremely encouraged to see this process and we look forward to working with the committee in the future.

Thank you.

Mr. LANGEVIN. Very good. Secretary Work, thank you very much for your testimony.

I understand the commissioners have worked out among themselves that Dr. José-Marie Griffiths will go next. So, Dr. Griffiths, the floor is now yours to summarize your testimony for 5 minutes and, without objection, your written testimony will be submitted for the record.

STATEMENT OF DR. JOSÉ–MARIE GRIFFITHS, COMMISSIONER, NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

Dr. GRIFFITHS. Thank you very much. Chairman Langevin, and Ranking Member Stefanik, and members of the committee, thank you for the opportunity to testify before you today.

Within our Commission, I chaired our efforts to develop an AI-ready Federal workforce and to improve the AI talent pool in the United States more broadly. Over the last year and a half, our workforce line of effort has held 11 working groups and interviewed more than 150 AI and human capital experts from the government, private sector, and academia. Through this process, three broad themes have emerged about the government's workforce.

First, building an AI-capable workforce doesn't lend itself to neat and tidy solutions. We need to tackle the problem from multiple angles. Second, it is difficult for agencies to implement their own major workforce reforms. Anything other than incremental change requires congressional leadership. And third, every opportunity my colleagues have mentioned and every challenge we describe in our report is, at its core, a workforce issue.

When organizations fail to adopt AI, and it is almost always because of their lack of qualified engineers and lack of senior leaders with the right education and experience to establish priorities and cut through red tape; when organizations can't purchase the software and hardware they need, it is often due to a problem with the limited knowledge and understanding on the part of their acquisition and contracting personnel. When organizations struggle to collect and manage data, it often suggests a lack of training and education geared towards these complex tasks.

To better understand the composition of the workforce the government needs, we partnered with the Defense Innovation Board and the Joint AI Center to create an AI workforce model, which you can find in our interim report.

In broad strokes, we believe the government should focus on five things: (1) build a technical workforce with tiered levels of skill and educational requirements; (2) educate senior leaders, who can better define strategic and enterprise objectives; (3) train junior leaders, who will manage the deployment and use of AI-enabled technologies and capabilities; (4) train the end users of AI-enabled technologies, who will be responsible for collecting and managing data; and (5) train and educate people in critical support roles, including human resource, acquisition, contracting, and legal professionals.

Our early recommendations are meant to help set a foundation for Federal workforce improvements and we are encouraged to see so many of them reflected in this year's NDAA. I would like to highlight several provisions in particular that we strongly support. They include AI training courses for HR [human resources] professionals, the creation of unclassified workspaces, a pilot program for using electronic portfolios to evaluate applicants for technical positions, a program to track and reward the completion of AI training, a mechanism to hire university faculty on a part-time basis in government laboratories, expanding talent exchange programs between DOD and technology companies, and an adjustment to the

aptitude test that the armed services use so that it tests for computational thinking skills.

In combination, these reforms would mark a significant step forward and I urge Congress to ensure they are included as part of this year's defense authorization.

Thank you, again, for the opportunity to appear here today and I look forward to your questions.

Mr. LANGEVIN. Thank you very much, Dr. Griffiths.

The chair now recognizes Commissioner Clyburn for your testimony for 5 minutes and, without objection, your written testimony will be submitted for the record.

STATEMENT OF HON. MIGNON CLYBURN, COMMISSIONER, NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

Ms. CLYBURN. No objection. Thank you very much.

Chairman Langevin, Ranking Member Stefanik, and members of the committee, thank you for the opportunity to testify today.

I would like to use my time to continue the theme that my colleague, Dr. Griffiths, has just discussed, the state of the Federal Government's AI workforce. In my time on the Commission, it has become clear to me that talent is the centerpiece of any winning AI strategy. We have examined the government's current shortcomings and have found that, in addition to the series of reforms Dr. Griffiths mentioned, we need to take bolder action. Existing programs will not bring enough digital talent into the public service workforce to meet serious shortages. The current scholarship and service programs are limited in scale and will not create a common set of ideas, shared experiences, professional culture, or a common mission to improve the government's digital talent. So, we must fundamentally reimagine the way the U.S. Government recruits and builds its digital workforce.

The Commission has put forward two significant proposals and I will take these few minutes that I have left to briefly describe them. First, we propose building a United States Digital Service Academy. This academy will produce technically educated graduates who would have a service obligation as civil servants into Federal Government. The academy will be an independent entity within the government. It would be advised by an interagency board, which would be assisted by a Federal advisory committee composed of commercial and academic leaders in emerging technology. The academy would be a partnership between public and private sectors, working together toward a common goal of developing a modern digitally proficient workforce.

We should consider now, before legislative action takes place, how the private sector and academia can support an academy. We are eager to discuss what barriers, limitations, or other factors would prevent such cooperation, or work with legislators to ensure that language is written with this partnering in mind.

Second, we propose establishing a National Digital Reserve Corps. Many of the most talented technologists in the United States are eager to serve their country but are unlikely to become full-time government employees or military reservists. The government needs a mechanism to tap this talent reservoir. The govern-

ment should establish a National Reserve Digital Corps modeled after the military Reserves that allows individuals to work for government 38 days a year as advisors, instructors, and developers. We could incentivize participation with a training and education fund, and a scholarship program modeled after ROTC [Reserve Officers' Training Corps]. While short-term volunteers are not a substitute for full-time employees, they can help improve AI education for both technologists and non-technical leaders, perform data triage and acquisition, help guide projects and frame technical solutions, build bridges between the public and private sector, and other important tasks.

I urge Members of Congress to take both of these proposals into consideration and to develop the legislation that would be needed to turn bold ideas into real institutions and programs.

Thank you again for the opportunity to share our recommendations with you and I look forward to any questions you may have.

Mr. LANGEVIN. Very good. Thank you, Commissioner Clyburn.

I want to thank all of our witnesses here today for your extraordinary contributions to the National Security Commission on AI. We appreciate the testimony today and the written testimony that you have submitted.

And we will now turn to recognizing members for questions for 5 minutes. I will begin with myself.

Let me start with you, if I could, Chairman Schmidt. Given that China views talent as central to its technological advancement, U.S. policies that restrict foreign talent from studying and working in the U.S. seems to play right into China's hands. How do policies that restrict China's talent from studying and working in the U.S. impact our national security?

Dr. SCHMIDT. Well, thank you, Mr. Chairman.

I was quite surprised, when we looked at the quality of the top papers, how many Chinese graduate students were part of the top papers being produced in the United States. So in other words, if you were to get rid of them, if you were to say none of them are allowed in the U.S., U.S. research would suffer.

I don't know if it is appropriate or not, but I need to say that this Pathway Act that you guys are proposing is exactly a good answer to this because we need to identify the very tip-top people we need for national security from all countries, and we need to get them into America, and we need to keep them here, and we need to keep them here producing research wins, producing defense companies, producing high-tech companies, and so forth, and so on. Put another way, if those people are—using China as an example—if they are in China, they are going to start up a whole bunch of companies that are going to become a real pain in the ass, if it is okay to say that, for the Congress in a decade.

So in other words, I would much rather have them creating huge successes in America, for security and also for commercial reasons, than doing the same thing in China or another country, such as Russia, and then us having to deal with the consequences of that.

And just to make it clear, if you look at TikTok, the core achievement of TikTok, although it is a social phenomenon, is a different kind of AI recommendation algorithm where they are clearly ahead. The moment we started arguing with TikTok over their U.S.

operations, the Chinese Government banned the export of that algorithm. How important is that? I don't know but it is a good example of something that would have been available to U.S. researchers that is not available today. That is not a good thing.

Mr. LANGEVIN. Thank you. I share your concern. And the Pathways Act is a good remedy, again, arm the Secretary of Defense to designate critical study areas where we would want to keep that talent here. We would start out with 10 individuals but we would have liked to—very much like to rapidly expand it to a larger number from there.

The next question: What are any specific AI research areas in which you believe the United States is under- or over-invested and how would you propose rebalancing the U.S. science and technology investments?

Dr. SCHMIDT. So, my personal opinion—people can disagree over this—is that we are not over-invested in anything. It is clear that we are under-invested in the underlying infrastructure that is needed.

There is a proposal that is, I think, being discussed in the Congress called the National AI Research Resource. And the idea here, it is a good idea, it is basically to try to create an infrastructure that allows all of the creative people in the United States access to the systems where they can do the research. I can tell you that, if you work in a very large company, you have that. But what about all of the 10-person and 20-person companies, where they don't have the money, and the scale, and the time to get the kind of data, and data analysis, and computing platforms? What about the researchers, the three people in, you know, a little boat somewhere in their university, who don't have access but they have a brilliant idea?

One of the hallmarks of American creativity has been that the greatest things come from the weirdest corners. We want to make sure that those weird corners in the United States of sort of clever people, who are staying up all night drinking Diet Coke and eating hamburgers, whatever the stereotype you have is, they have the tools that they need to do global solutions very quickly.

Mr. LANGEVIN. Thank you. And understanding that many of your recommendations are focused on government-wide, what are the other committees that you are meeting with to help implement these provisions?

Dr. SCHMIDT. I am sorry. The committees of the Congress?

Mr. LANGEVIN. That is right. Yes, what other committees of the Congress are you meeting with to help implement these provisions?

Dr. SCHMIDT. In general, this area on our remit is controlled by the HASC [House Armed Services Committee] and the SASC [Senate Armed Services Committee].

Mr. LANGEVIN. Okay, all right.

Secretary WORK. Mr. Chairman?

Mr. LANGEVIN. Thank you very much.

Secretary WORK. Mr. Chairman, if I could add.

Mr. LANGEVIN. Of course.

Secretary WORK. We have worked very closely with the intelligence committees on several of the recommendations. [audio malfunction] and any of the areas that have to do with workforce, we

try to reach out to as many committees that oversee the government workforce, for example.

So I know Yll Bajraktari, we can take that as a question for the record, sir, and bring it back to you but we are talking with many of the committees.

[The information referred to can be found in the Appendix on page 59.]

Mr. LANGEVIN. Very good. Thank you very much.

I have additional questions but I am going to stop here. And I will now yield to Ranking Member Stefanik for her questions.

Ms. STEFANIK. Thank you, Jim.

I wanted to follow up on Eric's comments regarding the infrastructure side. So the Commission referenced many times the importance of accessible robust data sets for the development of machine learning and AI. However, we often hear and we have worked through many of these impediments within DOD, whether it be classified or controlled data sets from the government side or concerns that exist over intellectual property and data rights from the side of private industry that, of course, partners with DOD.

How, specifically, would the Commission suggest AI stakeholders alleviate these concerns and reduce those impediments? Because I view that as a form of the infrastructure. The data sets are the fuel for AI and this is a really tough challenge for us to work through.

Dr. SCHMIDT. Maybe Commissioner Work can also add to this.

When I look at this, what I would like to see is a broad research exemption that would allow the kind of data that is being collected to be used for research with appropriate safety safeguards and privacy concerns and so forth.

One of the key things to understand about AI is it needs data. It eats data. It is how it trains. It is how it learns. And the more data the better. There are a number of problems in AI which seem to only get better with more data. There is no limit to the amount of data you can feed them—language translation or language understanding is such an example.

And so the combination of the computing resource that I have highlighted, plus broader access to data under appropriate safeguards is key. Each of the groups that controls this has got to confront the fact that they have a lot of data that is in databases that are not connected together, that nobody knows how to get it out and so forth.

I believe, for a long time, that using intelligence as an example, in the intelligence community, if they could simply unify their databases, you would find an enormous number of new things because the data is over here and not there and the AI can see the pattern between the two that humans cannot.

Bob, could you add a little bit here?

Secretary WORK. I think I can start by adding a real-life anecdote, Congresswoman Stefanik. When we stood up Project Maven, which was designed to sort through all of the full-motion video and take analysts away from the screens, staring at the screens for hours upon hours, and having the computer work that data, Jack Shanahan, Lieutenant General Shanahan, who was, at that time, the head of the ISR, the Intelligence, Surveillance, and Reconnaissance Task Force, came to me and said: We can't do what you want

to do, Mr. Secretary, because the data that we need to train the algorithms is all classified Secret. And I said, so what do we have to do about it? And he said, all you have to do is declassify it. So I just asked: Okay, what would be the implications? And it turns out that it was very easy to do and it had absolutely no impact on security in the sense of us giving up any type of secrets.

So to your point, I believe that the JAIC [Joint Artificial Intelligence Center] and the new chief data officer need to have the authority to declassify data, when asked, to use for an AI algorithm. They are the ones that are in the position to determine whether or not declassification of the data would pose any risk to the Department and it would make it faster and easier to go after these AI algorithms.

Ms. STEFANIK. Thank you. I yield back.

Mr. LANGEVIN. Thank you, Elise.

Next, Mr. Larsen is recognized for 5 minutes.

Mr. LARSEN. Thank you, Mr. Chair. I appreciate that.

Chair Schmidt, earlier in your testimony and we were talking earlier, I had asked you whether or not we should make a similar declaration on AI policy that the Chinese Government has made, where they are going to be the global leader in AI by 2030. And I always thought, we will just say that we are going to be the global leader by 2029. We are just going to beat them to that. Why don't we and what would prevent us from doing that?

Dr. SCHMIDT. I think your question was very prescient, in my view, because the good news is I think we already are the global leader and we would need to maintain it.

So, I would recommend that the Congress come up with some mechanism to say where we must lead. There is a candidate list. Indeed, in one of the bills you have proposed, you have made a list, which is similar to—it is a biotechnology list, 5G, so forth, and so on. I would view these as a matter of national security, national priority. They are also at the basis for the economy of America. So the most valuable companies in the United States are all based on these technologies. We don't want to give up that either. So that even if you don't care about national security, you must care about our companies, and our economic growth, and the GDP [gross domestic product], and the wealth of our citizens.

So regardless of your point of view, I know you care about both, you are going to want a plan. And what I would recommend is that you ask us to produce the list and we will work with our colleagues and the other commissions and come back to you for your consideration.

Mr. LARSEN. And if we made that ask, could you still do that within the timeline of the Commission?

Dr. SCHMIDT. We have a team looking at this question. I am sure we could do a good first start. I would also say that these sorts of list are—they are one, they are controversial within the community because people are fighting for their own fiefdoms but there is also——

Mr. LARSEN. We don't have that here, so fine.

Mr. SCHMIDT [continuing]. But in the technical world, these battles occur.

But also, there is evidence that America's greatness is because of our ability to integrate these things quickly. So it is not only the areas but our ability and the flexible way in which we work as a society to create the companies, create the initiatives, create the resurgence, and create the health solutions, and so forth combining them.

So I would recommend that not only do we give you something that is interesting for your review but then you also ask, in some other forum, for a continual review of this. I think it is part of national security.

Mr. LARSEN. Okay. On Monday, the DOD released their AI education strategy, which was directed in section 256 of the fiscal year 2020 NDAA. It is really focused more on educating the women and men who wear the uniform in the DOD about the basics of AI and how it might apply in everything that they do.

Has the Commission evaluated that and would you evaluate it?

Dr. SCHMIDT. Let me ask Mignon and José-Marie.

Mr. LARSEN. Sure, I will ask Commissioner Clyburn.

Ms. CLYBURN. The short answer is yes, sir. We recognize that, without talent, without pathways inside and outside of the communities, that all will be troubled. I will just put it that way.

So, we have outlined, especially in our first quarter recommendations, a series of pathways, of opportunities, of synergies that should be realized and adopted across multiple platforms, including recognizing and affirming AI as a priority, no matter what your rank, no matter what your job description. So that holistic inclusive approach to learning and embracing AI as a way of life, as a way of your job, as a way of this mission as a national strategic priority, is definitely—you will see that all through this report, sir.

Mr. LARSEN. Thank you. Thank you. And I want to move to a final question.

Chair Schmidt, you know Kai-Fu Lee, I imagine.

Dr. SCHMIDT. I do, very well.

Mr. LARSEN. Yes. In his 2018 book on AI and superpowers, he made a distinction between the United States being better at innovation and with the Chinese system is better at application of AI.

Do you agree with that assessment? And, if you agree with that assessment, maybe, for the record, you could get back to us how we could be better in both.

Dr. SCHMIDT. So Kai-Fu and I have been colleagues and friends for a decade. And my view of his book was that it was the case for China. I think we don't really know if his claims are correct. But the argument that he made that is important to state right here and right on the record is that they have a massive investment in this area coming. And we know that there are areas where the application of this technology is a scale problem. In other words, we invent it and they apply it. And I am always worried that we are going to do something that will prevent us from having a global market.

Part of the genius of America is our companies are global companies. So, they have a huge market. And I want to make sure that that is a huge market and not taken over by China. So I am worried about what he says.

We can try to give you more clarity on some of the things that you can do. Many of them are more or broader than our mission. So, many of them involve essentially promoting entrepreneurship, trying to get more dynamism in the economy, trying to get more founders to found the great companies, more high-skills immigration, trade policy which promotes American exports. I suspect these are things that you would agree with but that is sort of the list.

Mr. LARSEN. Yes, all right. Thank you.

I apologize, Mr. Chairman. I yield back.

Mr. LANGEVIN. Thank you, Mr. Larsen.

Mr. Conaway is now recognized for 5 minutes.

Mr. LARSEN. I will just note, Mr. Chairman, Mr. Conaway is not present at this point.

Mr. LANGEVIN. Okay. Is Mr. Bacon there?

Mr. LARSEN. There are no Republicans present, at this point. So it would be the next in line, the Democrat next in line. Sorry, Mr. Chairman.

Mr. LANGEVIN. Okay, then we will take the Republicans when they come back.

Next will be Ms. Slotkin is recognized for 5 minutes.

Ms. SLOTKIN. Great. Thank you, Mr. Chairman. Great to see you both. Thank you for coming.

You know I was reading through the recommendations of the various quarters and I think there is nothing to contradict anything. You guys are the experts in this. But I think for former Deputy Secretary Work and for Mr. Schmidt, head of the Defense Innovation Board, we always have these commissions but the structure at the Department of Defense does not support an easy, efficient incorporation of new technology, not for any one person's fault but because of the incentive structure there.

And so, while I see a lot of suggestions, I am having trouble understanding how to incorporate this in a way that is practical.

So from each of your perches, one in the DIB [Defense Innovation Board] and one as DEPSECDEF [Deputy Secretary of Defense], can you talk about the structural change that, no kidding, no joke, would allow for this innovation to be incorporated and not just repeating the past of the services being able to do their own kind of decision making on this and only a notional kind of signoff at the top level that misses the real opportunities.

And I will turn to Mr. Schmidt first.

Dr. SCHMIDT. Actually, why don't we—with your permission——

Ms. SLOTKIN. Of course. Of course.

Mr. SCHMIDT [continuing]. Could we have Chairman Work speak first?

Ms. SLOTKIN. Of course.

Dr. SCHMIDT. I will follow him.

Secretary WORK. It is good to see you again, Representative Slotkin.

Ms. SLOTKIN. It is good to see you.

Secretary WORK. I could imagine you asking me this question in my office but you are exactly right.

On a transformation of the scale that the Commission believes is necessary, just how important artificial intelligence will be, not only to the business applications in the Department but, more im-

portantly, the operations and combat capability and effectiveness of the Department, you are going to have to have a strong top-down push. You are going to want to have the thousand flowers bloom within the services. That is going to be a very good thing to see and I actually think that is happening now. But without that strong top-down push, you are not going to get the broadest transformation that you are looking to.

The Commission talked about this a lot and came down with two things. One, I think you remember the old Advanced Capabilities and Deterrence Panel.

Ms. SLOTKIN. Yes.

Secretary WORK. And using that as an exemplar, we said we should have a steering group, a technological steering group, consisting of the Deputy Secretary, the Vice Chairman of the Joint Chiefs of Staff, the Principal Deputy Director of National Intelligence, the Under Secretary of Defense for Research and Engineering, and they would try to look at the forest, instead of the trees, and approach it the way that Eric talked about: How do you integrate all of these technologies for military advantage? And without someone doing that on a consistent basis, you are not going to have the transformation that you would otherwise have.

The second thing is we feel strongly now that the Secretary of Defense has come out and said that AI is, if not the top priority, one of the top three priorities and try [audio malfunction] underneath the Secretary of Defense, who could then delegate it to the Deputy, if he or she so desires.

The CIO [Chief Information Officer], we believe, should be responsible for the broader digital transformation of the Department. It makes sense to have things like the cloud, and the data strategy, and the infrastructure that Eric talked about. The CIO is natural for that job but we need to have a single organization that is focused on applications like a laser beam and, in our view, the CIO shouldn't lead that effort. It should come directly from the top, be top-down driven, and the executive agent for that should be the JAIC.

The combination of the technical steering group, which is looking at the forest rather than the trees, and then the JAIC, which is helping to plant and tend to the trees, is the way we think that you can have this be a sustained transformation.

Ms. SLOTKIN. Great. And Chairman Schmidt, in the last 30 seconds of my time?

Dr. SCHMIDT. I guess I should have realized that the military would be top-down and it is so top-down, everything that Bob just said is a requirement.

I would add one more thing. If I were advising the Secretary of Defense, I would just say I want everything faster. I want these prototypes faster. I want a design engineering mechanism where I get stuff faster.

These product cycles for weapon systems, which are 15 years, are crazy because the technology has already moved past what the spec was. It doesn't serve our Nation well. Let's get to a different model, where the stuff is happening very quickly, we are canceling and starting things, we are giving you all choices of things to approve, and so forth.

The proposal that Bob made is very consistent with that but I would tell you the metric I would apply, if I were Congress, is I want things faster.

Ms. SLOTKIN. Okay, thank you very much. I appreciate it.

Mr. LANGEVIN. Thank you, Ms. Slotkin.

Mr. Brown is now recognized for 5 minutes.

Mr. BROWN. Thank you, Mr. Chairman. I want to thank Chairman Schmidt and all of the commissioners for your work on this Commission in the area of artificial intelligence. Thank you for being here today.

I am enthusiastic about the opportunities, the potential for artificial intelligence, particularly how it is going to enhance not only the lethality but the survivability of our warfighters. I think about autonomous vehicles, air, land, and sea. I think about enhanced human decision making. I think about improved targeting, which is so important, particularly with the ever-increasing number of sensors in the various physical demands on the battlefield.

But I do have some concerns. I have some concerns that you have mentioned, Mr. Chairman, and that has been a topic of conversation, and that is biases in both the development and the deployment of AI, biases by culture, race, ethnicity, and even gender. And I am concerned particularly when we talk about AI for targeting, whether that targeting is done by the military or by law enforcement.

NIST [National Institute of Standards and Technology], in a study I think last year, found that African-American and Asian faces—we are talking about facial recognition in targeting, identifying—10 to 100 times more likely to be falsely identified than Caucasian.

Now, the second quarter recommendations did include the following: that R&D [research and development] is needed to advance capabilities of AI technologies to perceive and understand the meaning of human communication, including spoken speech, written text, and gestures. This research should account for varying languages and cultures, with special attention to diversity, given that AI typically performs worse in cases in gender and racial minorities.

So, there is a recognition of this. You probably know that of the $4.1 billion that the DOD invests in research and development at universities and colleges, less than 0.5 percent goes to historically black colleges and universities [HBCUs], and minority-serving institutions.

So I have a concern about the bias in the development and deployment and I have a concern about the lack of diversity and inclusion to address the bias. And nowhere in the first quarter interim report that you issued or the Commission issued did I hear much of anything about diversity inclusion.

So what are we doing to ensure that, as we are considering, and studying, and developing, and deploying AI in all of its many ways, that we are addressing biases? And in my opinion, you do that by making sure you have a diverse and inclusive team that is actually researching, and developing, and delivering this technology. What are we doing now? What should Congress do to move this along faster?

Dr. SCHMIDT. Speaking for the Commission, we completely agree with the framing that you just said on the issues and they are starkly correct.

Let me ask my fellow commissioners to comment on the solutions. I can tell you that this is a huge issue in the American research institutes, universities. Many, many people have ethics groups and concerns over bias. There may be algorithmic ways to change the algorithms, to eliminate this bias in such a way that we don't have to worry about it as much but right now, it is a very real issue.

Mignon and José-Marie?

Dr. GRIFFITHS. I am happy to start. There are really two answers to the question. One relates to how we build the AI algorithms to eliminate bias and how we make sure and test against all different scenarios that the bias doesn't exit. The other goes back to workforce again and to have a broadly diverse and inclusive workforce that represents the population of the Nation. That becomes very, very important as well.

I believe it was GM [General Motors] that first brought women in to design minivans for the soccer moms and the design of those vehicles suddenly became very different.

So I think two ends, one is the R&D and the actual algorithm development testing and evaluation and, on the other side, trying to ensure that we have the broadest possible representation coming into the workforce, which relates to actually some of the work that we are doing for our next report, which relates to looking not just at the universities and their production of graduates in AI and increasing those numbers, but actually reaching down into K–12 and also looking at alternative pathways into the workforce that go beyond the college degree.

So we are looking at those things at both levels.

And I think, Mignon, you may have something you wish to add here, too.

Ms. CLYBURN. Right. One of the reasons, Congressman, I mentioned the two proposals that would encourage and bolster a diverse—diverse sets of talent, including civilian talent, is when it comes to the development, when it comes to those teams, they have to be inclusive. They have to be diverse. When models are designed, there has to be an inclusive and expanded table. That is the problem.

One of the things—and I know I am running up on your minute—firsthand, a few years ago, I went in with this AI-enabled product and it didn't see my face at all. I was invisible in a room. So if I am invisible, that was a kind of passive invisibility but invisibility in terms of presence, in terms of you know being able to not only see but predict in a productive way, if that is not at the design phase, then we are going to have a perpetual problem at the implementation phase. So, it has to be inclusive. It has to be diverse and we have to be conscious and intentional about production and application.

Mr. BROWN. Mr. Chairman, in yielding back, if I could just comment that last year's NDAA we directed the Secretary of Defense to commission a study, the national study of defense research at HBCUs, in an effort to increase the research dollars, and the ca-

pacity, and capability. I would commend and request that this Commission take a look at that work—they are at the very early stages—and perhaps provide them guidance and input on how we can get more research dollars in those universities and colleges, where you have a high concentration of diverse candidates doing extraordinary things at the graduate and undergraduate level, and AI may very well be a part of that.

Thank you, Mr. Chairman. I yield back. Thank you for your indulgence.

Dr. SCHMIDT. And that is a yes.

Mr. LANGEVIN. Thank you, Mr. Brown. Thank you, Mr. Brown. It is certainly a very important topic to raise.

With that, Ms. Trahan is recognized for 5 minutes.

Mrs. TRAHAN. Thank you, Mr. Chairman, and I really appreciate the expertise represented in this Commission, and the depth of your recommendations laid out in the Q1 and Q2 reports.

I think my question is for Commissioners Griffiths and Clyburn. I am interested in just digging deeper into your line of effort on AI talent. There seems to be a severe lack of AI knowledge in DOD and other parts of government, where that AI requirements and capabilities get automatically bundled with cyber missions.

And so, one, it would be great if you could just explain why it is important to decouple our AI workforce from the cyber workforce. And then, also here, how you would recommend the government create a system for measuring and tracking its AI knowledge.

Dr. GRIFFITHS. I will jump in, if I may.

You are absolutely right. I think that decoupling cyber from AI is very important because cyber has a mission and it is very, very clear what the mission of cyber is. And while they may have common roots in fundamentals of computer science, they branch off after that and focus on different missions and confusing them confuses everyone.

From an academic perspective, academic programs are very different for producing graduates in those areas. So, I think decoupling is one and we have made recommendations not for eliminating one or crowding out a program in cyber, but actually adding to the vehicle or adding to the mechanism to ensure that AI receives appropriate attention, as well as cyber.

On the issue of the talent base within the government, you have no ways, at the moment, of knowing who has the talent and who doesn't have the talent. You don't even really know in the military who has capabilities of coding. And so a number of our recommendations are addressed to sort of testing for computational thinking, which now is the prevailing thought, the kind of capability and underlying fundamental skills, and the mindset that people have, the talent that they have that can then be developed into AI-related capabilities.

So, and the other area is, of course, a lot of educational training at different levels. And the workforce model that we developed jointly with the DIB and the JAIC I think really addressed all those different layers. We have three very technical work roles and four non-technical work roles, and all of them need to have some and different levels of understanding of AI, including ethical issues associated with the acquisition and application of AI.

Ms. CLYBURN. And I will just finish up by saying AI will continue to transform. It is not passive and nor should we—should it be passive, in terms of our intent, in terms of it being a single focal line of effort, if I may borrow our jargon, so to speak. And this general purpose technology has multiple applications that are significant with our focus when it comes to national security but it has a ripple effect throughout society.

So not targeting, not streamlining, not separating, so to speak, would be to our peril because of the expansive, the significance, and how much it is interwoven into our everyday lives.

Mrs. TRAHAN. I appreciate that. And, you know, if I have time for just one—I think I do have time to slip this last question in.

But, you know, we hear all the time that, you know, we are not recruiting enough technical talent and, certainly, we are not moving at the speed that we need to, and our onboarding authorities are often not able to meet the demand. You addressed some of these concerns in your quarter, I think it was the Q1, recommendations around strengthening the AI workforce and using a Cyber Excepted Service.

I am wondering if, you know, whenever we have folks in the private sector in front of us, we always love to, you know, borrow your best practices. In terms of specific recommendations the government should consider to be more competitive in recruiting this technical talent, knowing full well that some of the most competitive companies with the largest market share across the globe don't take the—you know, they don't necessarily pay the most, are there anecdotes that you can share with us on how we can think of novel ways of recruiting technical talent more quickly?

Dr. SCHMIDT. This is Eric. May I answer your question?

Mrs. TRAHAN. Please.

Dr. SCHMIDT. In my service to the DOD, for the 4 years I was the chairman of the DIB, I was struck by how many people want to volunteer to serve their Nation, and they are willing to do so at very low salaries, and under lots of difficult situations. The things that drive them crazy are things like it takes 3 months to get an offer out, or that they get classified in the wrong way, or they can't—they have 5 minutes per day to clean up their email because they only have a megabyte of email and their email system doesn't work.

So, they are willing to serve at a lower income level for the Nation but it has got to work operationally and there are many such simple things that the DOD and others could do, it is true of the Federal Government in general.

Mrs. TRAHAN. Thank you so much. Mr. Chairman, thanks for indulging me. I, obviously, yield back.

Mr. LANGEVIN. Thank you, Ms. Trahan.

The chair now recognizes Ms. Houlahan for 5 minutes.

Ms. HOULAHAN. Thank you, Mr. Chair, and thank you to all of the witnesses. And I just have some questions for any of you.

The Commission specified a belief that the JAIC should be elevated from its current position with the CIO to a direct report to the Secretary and it notes that the Secretary can delegate responsibility to the Deputy Secretary. The recommendation, however, does speak to your position that AI is an issue that has to be raised in

order to, and this is a quote from the report, provide the requisite level of senior oversight and support needed to preserve the Department's initial AI projects, enable their growth, and ensure that the Department can develop the capabilities needed to successfully adopt AI applications.

So the Secretary and the Deputy Secretary have the ability, right now, to take such a step today. However, they haven't acted on that recommendation to date, necessitating legislative involvement on the House's side in our most recent NDAA.

So my question is: Can you all help us understand, potentially, the reason that the Department has not accepted your recommendation and can you potentially reiterate for us the reasons why our colleagues on the Senate side should be interested in accepting the Commission's position that the JAIC should be placed under the Secretary's direct authority?

Dr. SCHMIDT. Bob, can you comment on that?

Secretary WORK. Yes, ma'am. The JAIC, I think right now, is starting to hit its stride. Dana Deasy, who is the current CIO, is an extraordinarily capable public servant and the JAIC has grown up under his supervision. And I think the Department of Defense is quite happy with the way things are progressing, as they should be.

What the Commission was thinking is that, over time, the CIO—you should split the responsibility, where the CIO focuses on the digital transformation of the Department, like getting the cloud set up and settled, doing the data strategy for the Department, and focused on all of the infrastructure, and having the JAIC focused, really like a laser beam, on AI applications.

At some point, someone is going to have to be designated kind of the system architect for large DOD programs and the system architect would say these are the AI applications that we think would have the broadest and the most consequential impact on the joint enterprise.

And so we think that having the JAIC doing that and having everybody in the services understanding that they are working under the direct supervision of either the Secretary or the Deputy Secretary, that that is the fastest way to get transformation. That I think is——

Ms. HOULAHAN. So, sir, what you said was you recommended that over time and then you ended by saying that is the fastest way. And so what is the timeline that your recommendation is or is it best to be immediately you know rip the Band-Aid and move forward? What is the recommendation, in terms of timeline and immediacy?

Secretary WORK. I think I can speak for the Commission, where we said the sooner you do this, the better—split the responsibilities, really start to run. As Eric said, we believe that urgency and scale is absolutely important. So the sooner you would do something like this, we think, the better.

Ms. HOULAHAN. Okay. So, urgency, the sooner the better. Do you all have anything else that you would like to contribute to that response?

Dr. SCHMIDT. So, we are celebrating the success of the JAIC today. Two or three years ago, there were people who didn't want

to do it at all and it took, again, top-down leadership from the Secretary of Defense at the time to really force it.

If you want to take a large bureaucracy and reform it in a way that is consistent with national security and modern principles, you have to force it from the top. This is a maneuver of that nature. There are probably others.

Ms. HOULAHAN. No, I appreciate that. I had the opportunity to visit the JAIC and I do understand how innovative it is and how impossible the lift is from an organization as big as the DOD to create something new and innovative.

I only have 24 seconds with my time, so I think I will yield back, Mr. Chair.

Mr. LANGEVIN. Thank you, Ms. Houlahan. And we are going to go to second round anyway, so if you want to ask another question, you will have another opportunity.

So I understand Elise has not returned yet but hopefully she will be back soon.

So I just had two additional questions. I just want to thank our witnesses again, as we go to a second round.

My first question is: What are the most significant gaps in current legislation that relate to artificial intelligence and national security and what do you believe are the Commission's most consequential recommendations that Congress has not yet acted upon?

Dr. SCHMIDT. Maybe each of the Commissioners could answer your question, Mr. Chairman.

My reaction is that the profound change that is needed is the workforce one, that without addressing the workforce one, the gains will be lost in the bureaucracy, et cetera.

Other commissioners?

Ms. CLYBURN. Investment, sir. This will not be a free endeavor but it is one that is a priority, it is one that it is critical. And so, honestly, right now I would say budgetary.

Dr. GRIFFITHS. If I may, Mr. Chairman, I believe that—I endorse what Eric said. I believe workforce is the core. As we have discussed at our various Commission meetings, workforce has an impact on every other line of effort and it needs to be done and incremental changes are not going to make a difference.

So, we do need to make sort of moves that generate and lift the scale up, so that we can get the workforce ready quickly to enable some of the innovations to move forward quickly.

Secretary WORK. I agree with my colleagues that workforce is number one. The National AI Research Resource I think would be a close second, along with the increases in investments, as Mignon has talked about.

The recommendations we have made on microelectronics and how we maintain our lead in that area I think are extraordinarily consequential. And then the recommendations we make as far as pursuing with our allies this together, since we see very clearly that this is a competition in values, as much as it is a competition in technology, and we want to involve all like-minded democratic nations so that AI reflects the values of democratic nations with respect for personal privacy, rule of law, et cetera.

So, I would put those four as very close together but with workforce on top.

Mr. LANGEVIN. Thank you, Secretary Work, and that leads—it is a good segue to my last question.

Obviously, as you pointed out, we are not developing AI in a vacuum. Other nations, who are competitors, or adversaries, enemies, are also developing AI technology and they may not be approaching it with the same type of safeguards that we are putting in place to make sure that AI is used ethically and responsibly.

What do we do about that? How do we protect ourselves against it? What is the way forward to pressure other countries to approach use of AI ethically and responsibly so we do have some safeguards in place?

Dr. SCHMIDT. Well, AI can be misused by countries that have different values than ours, the most obvious ones being the misuse of surveillance. And that, to me, is a political and nation-state issue. The technology is already in China. They are going to do whatever they are going to do with it. I don't know how to stop that technically.

I think it is very important that if a technology is invented in America that is dual-use and which could be used for very bad things, there would be a moment of reflection as to whether that should be broadly released or kept more close for that reason.

Mr. LANGEVIN. Thank you. Any other commissioner have a comment?

Ms. CLYBURN. I think the values need to be baked in. I believe, as was mentioned, those—the allies, the relationships, the norms need to be socialized, agreed, and expanded robustly. I believe to strengthen all of this, you know, would lie in our principles and those ethical standards, as we talk about efficiencies and all of the other benefits.

But the strength, to me, are the principles that the U.S. and its allies would, I believe, promote and amplify.

Secretary WORK. Sir, this is——

Mr. LANGEVIN. Have you done anything with respect to putting safeguards into play with the use of AI?

Ms. CLYBURN. There was a little bit—I heard. I don't think I——

Mr. LANGEVIN. I know Secretary Work was going to respond there.

Secretary WORK. Well, sir, on Monday, I just wanted to check on something because there was an extraordinary meeting, where 100 officials from 13 democratic countries met online Tuesday and Wednesday to discuss how their militaries could ethically use AI. It was the first summit of its kind. It follows on the heels of the AI ethical principles that Eric spoke to, which were the first published by any organization of the DOD, and it was hosted by the JAIC. And it has kicked off what JAIC is calling the AI Partnership for Defense. This is something that we haven't had an opportunity to talk about, as a commission, but I can state with certainty that we would endorse it and embrace it.

And central to this is talking about the limits, the moral, legal, and ethical limits that we want to establish for AI and national security applications. So, I really take this meeting as a very positive first step.

Mr. LANGEVIN. Agreed.

Do any of you know of any international efforts, including at the U.N. [United Nations], where this discussion and a framework for ethical use of AI is being undertaken with seriousness?

Secretary WORK. The primary place, right now, is looking at the ethical—the use of autonomous weapons and that is in the U.N., the United Nations' GGE, Group of Government Experts, as part of the CCW, the Convention on Certain Conventional Weapons. And that is very well attended by the Department of Defense and the Department of State and that is the primary place where the debate over how far and in what form AI-enabled autonomous weapons can be or should be used on the battlefield.

Mr. LANGEVIN. Very good. Thank you.

With that, let me go to Mr. Larsen for any questions he may have.

Mr. LARSEN. Thank you. I was wondering if any of the panelists have a view on your recommendation or your guiding principle 5, where you discuss principles of free inquiry, free enterprise, and free flow of ideas.

The last line of that section says: At the same time, we must not lose sight of enduring American principles and overly securitize basic research or the private sector.

I was wondering if you have some guidance for us on how to not overly securitize or to appropriately securitize basic research?

Dr. SCHMIDT. The Commission has spent a fair amount of time on this question of protection and it is an obvious one. An American firm, an American researcher invents something very important. What should we withhold, and what should we try to withhold, or maybe we will be not successful? And the consensus of the Commission seems to be that it is very difficult to withhold algorithms or even software because the algorithms are broadly known and they will be discovered by the competitor anyway, and the software is relatively reproducible. However, the insight from the Commission is that there are significant parts of the hardware value chain which are very specialized and that deserves very special attention.

Maybe the other commissioners may want to add something to add color to my statement.

Mr. LARSEN. Do any other commissioners have any views on that to add? If none—okay, thank you very much.

Dr. SCHMIDT. Thank you.

Mr. LARSEN. I yield back, Mr. Chairman.

Mr. LANGEVIN. Thank you, Mr. Larsen.

Ms. Houlahan, do you have additional questions?

Ms. HOULAHAN. I do. I do. I appreciate that.

My first question has to do with my interest in developing the U.S. Digital Service Academy which, of course, would create a pipeline of security-cleared Federal employees, and that was part of your proposal.

Can you highlight the components of that program and have you done any outreach to determine if there is an appetite for students for such a program?

Dr. SCHMIDT. There appears to be infinite appetite for this idea, if we can find the money.

Mignon, are you the best expert on this to comment on it?

Ms. CLYBURN. I will give it a try. Thank you very much.

One of the things, highlights that makes this particularly appealing, we believe, it is modeled after, you know, existing academies. We also know that existing academies, they are overflooded with applications. So, we think the interest would be there. We also think that the interest would be there for those who may not be able or might not have the interest in moving into military service or reservist service afterwards.

So the thing that is the most attractive, however, it is an incredibly targeted pipeline for all of the issues, when we talk about the lack of talent and having broad pathways for educational opportunities that are STEM [science, technology, engineering, and mathematics] or AI oriented. This would happen more robustly under this framework.

Dr. SCHMIDT. Can I add, Congresswoman?

Ms. HOULAHAN. Yes, please.

Dr. SCHMIDT. In our specific proposal, this is an independent entity under the Federal Government but it has a public sector-private sector board. In our formulation, it would be able to raise private money in addition to Federal money. In theory, it would offer—it would be able to charge tuition and have requirements of payback and things like that. So, very similar to the way our military academies operate.

And this is, perhaps, our strongest recommendation and I don't think it is that difficult for the government to do. There is huge demand. There is plenty of universities that would love to advise us and help us. We have had outpourings from many of the States that we have spoken with. They said, look, how can we help; what can we do?

Ms. HOULAHAN. Yes, it sounds like a really intriguing concept and I think something that we probably should take a very hard look at.

I also understand that you have been talking with industry experts in academics that have indicated that they would like to contribute to government missions because of a sense of civic responsibility or interest in unique government missions but they don't want to leave their current career field, even temporarily.

So, as a result, you have made the recommendation to create a National Reserve Digital Corps. Could you all also please elaborate or highlight on the purpose and the fundamentals of the Reserve Digital Corps, please?

Dr. SCHMIDT. Mignon or myself?

Ms. CLYBURN. Either. What this would do, it was patterned itself after ROTC. It will allow for a number of less than 40 days of service. It would enable the infusion of talent to troubleshoot, to triage, and overall to benefit the current ecosystem when it comes to our government, with giving those the flexibility to meet whatever other needs, in terms of economic needs, that they wish to.

The fact of the matter is, as it stands right now, one of the biggest barriers for serving full-time in government is money, is resources. Academia and the private sector attract, oftentimes, some of the better talent and this is one of those ways that we would recognize that, leverage that, without somebody having to make a hard permanent choice.

Ms. HOULAHAN. So I am just making sure that I understand. I was ROTC in the Air Force and went to school with a full scholarship at Stanford and repaid that by serving. Are you suggesting that this is the same kind of a thing with existing colleges and a pathway to repay; whereas, the other concept is the same as the Air Force Academy in this analogy?

Ms. CLYBURN. If I am speaking with the right program, in terms of the program, that you are saying the reservists, correct?

Ms. HOULAHAN. Yes, the Reserve Digital Corps. Yes, ma'am.

Ms. CLYBURN. Right, it would be patterned after that, all of the benefits of that would be——

Ms. HOULAHAN. I am just trying to drill down and understand just for myself what you mean by they don't have the time to commit because it seems as though I had a lot of commitment on the other side of the opportunity.

Ms. CLYBURN. I guess what I am saying, in this particular case, you know sorry about the miss, is that someone who does not want to take a permanent military track.

Dr. SCHMIDT. This is a somewhat lighter version of what you are describing. The ROTC, by the way, is a fantastic program that America has in our universities. Many of the leaders I have worked with have gone through ROTC and it is a great way to build bridges between the civilian and the military sector. And those are lifetime—lifetime commitments. And you are, obviously, a success from that.

One way to think about this is we have got to get a way for people to be able to work in the military—work for the military but not be in the military.

Ms. HOULAHAN. Okay.

Dr. SCHMIDT. This is a mechanism to do this. It is a structural mechanism, where they can say to their employer I am required to do this; you have to let me do this.

Ms. HOULAHAN. So it is a reservist, rather than an ROTC. I have got it.

Dr. SCHMIDT. A reservist. It is a reservist model.

Ms. HOULAHAN. Okay, I apologize. I appreciate the clarification and I yield back.

Ms. CLYBURN. No, and I apologize. I apologize, too, for the confusion.

Mr. LANGEVIN. Very good. Well, we will wrap up this hearing now. I want to thank our witnesses for their extraordinary testimony, for the extraordinary commitment that you have made to the National Security Commission on AI. We look forward to continuing to follow your work and the final report. And again, your testimony today has just been extraordinary and valuable.

So, with that, I want to thank you again. And this hearing now stands adjourned.

[Whereupon, at 2:39 p.m., the subcommittee was adjourned.]

A P P E N D I X

SEPTEMBER 17, 2020

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

SEPTEMBER 17, 2020

Opening Statement
Chairman James R. Langevin
Intelligence and Emerging Threats and Capabilities Subcommittee

Interim Review of the National Security Commission on Artificial Intelligence Effort and Recommendations

September 17, 2020

The subcommittee will come to order.

I would like to welcome the members who are joining today's hearing remotely. Members who are joining remotely must be visible onscreen for the purposes of identity verification, establishing and maintaining a quorum, participating in the proceeding, and voting. Those Members must continue to use the software platform's video function while in attendance, unless they experience connectivity issues or other technical problems that render them unable to participate on camera. If a Member experiences technical difficulties, they should contact the committee's staff for assistance.

Video of Members' participation will be broadcast in the room and via the television/internet feeds. Members participating remotely must seek recognition verbally, and they are asked to mute their microphones when they are not speaking.

Members who are participating remotely are reminded to keep the software platform's video function on the entire time they attend the proceeding. Members may leave and rejoin the proceeding. If Members depart for a short while, for reasons other than joining a different proceeding, they should leave the video function on. If Members will be absent for a significant period, or depart to join a different proceeding, they should exit the software platform entirely and then re-join it if they return. Members may use the software platform's chat feature to communicate with staff regarding technical or logistical support issues only.

With that, I will give my opening statement.

I am pleased to welcome four commissioners from the National Security Commission on Artificial Intelligence, a commission created by this committee in the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2019 to consider the methods and means necessary to advance the development of artificial intelligence, machine learning, and associated technologies to comprehensively address the national security and defense needs of the United States.

Our intent for this commission was to ensure a bipartisan whole-of-government effort focused on solving national security issues, and we appreciate the leadership and hard work of our witnesses in supporting the commission's efforts in that spirit. Today we welcome:

- Dr. Eric Schmidt, Chairman of the Commission;
- HON Robert Work, Vice Chairman;

- HON Mignon Clyburn, commissioner on the workforce and ethics Lines of Effort; and
- Dr. José-Marie Griffiths, commissioner on the ethics Line of Effort, and chair of the workforce team.

Our understanding of Artificial Intelligence (AI) started in the 1950s and '60s through research funded through the Department of Defense's vital science and technology investments by the Defense Advanced Research Projects Agency (DARPA) and the Office of Naval Research and was aided by the convening power of universities.[1] Now more than half a century later, this Commission is working through the difficult issues requiring national investments in research and software development; and new approaches on how to:

- apply AI appropriately for national security missions;
- attract and hold onto the best talent;
- protect and build upon our technical advantages;
- best partner with our allies on AI;
- stay ahead of the threat posed by this technology in the hands of adversaries;
- and implement ethical requirements for responsible American-built AI.

Indeed, last year the Defense Innovation Board, which was also chaired until recently by Dr. Schmidt, helped the Department begin the necessary discussions on Ethics in AI.

I applaud the Commission for being forward leaning by not only releasing an initial and annual report as required in law – but also releasing quarterly recommendations. Ranking Member Stefanik and I, along with Chairman Smith and Ranking Member Thornberry, were pleased to support a package of provisions in this year's House version of the FY21 NDAA based on the Commission's first quarter's recommendations. The House version carried 11 provisions, with the majority deriving from the Commission's call to Strengthen the AI Workforce. We are pleased that both Commissioner Griffiths and Commissioner Clyburn are with us today to testify on the need for action on AI talent.

On that note, we must implement policies that promote a sound economic, political, and strategic environment on U.S. soil where global collaboration, discovery, and innovation can all thrive. The open dialogue and debate resident in academia and the research community can be anathema to the requirement for secrecy in the Department of Defense. But we must recognize – and embrace – how our free society provides the competitive advantage that lets us innovate faster than our great power competitors. Our free society enables a dynamic innovation ecosystem, and federally funded open basic research focused on discovery has allowed American universities to develop an innovation base that has effectively functioned as a talent acquisition program for the U.S. economy. And that talent is

[1] Babb, Colin E., "How We Got Here – A Small Tale of the Autonomy and the Sea", Future Force: Spring Edition 2014

required today as much as ever to solve our most pressing national security challenges.

Indeed, great power competition is also a race for talent.

We are looking forward to hearing about your efforts, the observations and recommendations you've already developed, and your plan to continue until you submit the Commission's final report in the spring.

I'll now turn to Ranking Member Stefanik for her remarks.

Joint Written Testimony of Dr. Eric Schmidt, Sec. Robert O. Work,
Hon. Mignon Clyburn, and Dr. Jose-Marie Griffiths
U.S. House of Representatives Committee on Armed Services
Subcommittee on Intelligence and Emerging Threats and Capabilities
Hearing Titled: "Interim Review of the National Security Commission on Artificial Intelligence Effort and Recommendations"
September 17, 2020

Chairman Langevin, Ranking Member Stefanik, and Members of the Committee, thank you for the opportunity to testify on the initial recommendations of the National Security Commission on Artificial Intelligence, and our continued efforts to develop solutions for the nation's AI-related national security challenges.

Advancing AI for our national security is a bipartisan topic and priority. AI is no longer a long-term basic research challenge or the domain of our innovative private sector. It is not just critical to our future; it is critical to our present. The United States must get AI right to grow our economy, to protect our security—in the broadest sense—and to benefit humanity. The ethical principles we establish, the federal investments we make, the national security applications we field, the organizations we establish, the partnerships we forge, and most importantly the talent we cultivate will determine our place in a very serious strategic competition with authoritarian great powers.

In our judgment, America needs to lead the world in the development of AI. In that regard, however, we are still not where we need to be as a government, as a partner with the private sector, or as a partner with our allies and like-minded nations in the world. We need a fully funded and fully supported strategy to win the AI competition. And we need to build that strategy as just one component of an even more ambitious strategy for winning a broader technology competition that includes several emerging technologies.

The Commission's work is as expansive as the task at hand. One quickly becomes entrepreneurial by necessity when examining the intersection of AI and national security. Today, however, we would like to focus on the areas of our work and recommendations that touch directly on this committee, some of which are included in the pending National Defense Authorization Act (NDAA) for Fiscal Year 2021. We also want to highlight some critical talent and workforce issues. We see an opportunity for bold action to build the human capital the government needs to win the emerging technology competition.

Mandate[1]

The National Security Commission on Artificial Intelligence (NSCAI) was established by Congress to help define the AI challenge and present recommendations for solutions. We are especially heartened by the bipartisan support that the Commission is receiving from both houses of Congress. That support is reflected in the NSCAI proposals that have been included in the House and Senate versions of the NDAA, and in the broad bipartisan interest in the challenges to be addressed in this hearing. We thank the Members of this Committee, in particular Chairman Langevin and Ranking Member Stefanik, for their leadership in advancing a number of the Commission's recommendations, particularly those focused on developing an AI-ready workforce.

In close collaboration with Congress, the White House and executive departments and agencies, the Commission is working to ensure that the many ongoing U.S. Government efforts in AI are complementary and reinforcing. We have enjoyed equal support from leaders in academia, civil society organizations, and the private sector. They have explained their roles in the AI ecosystem, outlined their concerns, and highlighted opportunities for utilizing AI for national security purposes.

Why AI Now?

Artificial intelligence is a technological reality here and now. The compute power, the data, and algorithms are now available to translate many of the theories of the past into applications today. This explosion in AI capabilities is coming at precisely the right time. We need AI applications to help solve critical issues facing our world including the climate crisis and the COVID-19 pandemic. AI has already proven that it can make our lives and society better in everything from diagnosing disease to improving traffic patterns. The potential is exciting. Nevertheless, we are a national security commission and we are concerned that AI, like all technologies, will create new threats and exacerbate some existing challenges.

The International Landscape

The Commission's work is not occurring in a vacuum. We have a pacing competitor in China with a strategy, resources, and, unfortunately, a determination to develop and field AI for purposes that are inimical to U.S. interests. In this regard, AI is not only an "enabling"

[1] Congress created the NSCAI in the John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. 115-232, as an independent federal commission to consider ways to advance U.S. development of artificial intelligence, machine learning, and associated technologies to comprehensively address U.S. national security and defense needs.

technology. AI is a strategic enabler in a global competition encompassing military, economic, and ideological arenas. The competition is intensifying. The technological dimensions of the competition have been elevated. AI's centrality to the competition touches on everything from specific military capabilities, to the future of the innovation economy, to the struggle between authoritarian and democratic systems of government.

Using AI Responsibly

We are deeply concerned with the ethical and strategic implications of *who* is employing AI and for what purposes. Looking abroad, we are troubled by how AI is being utilized and has the potential to be weaponized. In this, we are talking beyond the potential biases in AI algorithms and the unknown reliability of AI-enabled systems—vexing technical challenges at the heart of domestic debates about facial recognition, for example. We are instead talking about AI systems that may, in fact, be extremely reliable and work exactly how they are designed to work, but for terrible purposes.

We have to acknowledge the dark sides of this technology and its many potentially harmful applications. We must understand how AI supercharges adversaries' disinformation campaigns, and how it will likely be employed to sharpen cyberattacks. Authoritarian regimes will use AI technologies to try to consolidate power, homogenize thought, and expand control beyond their borders. We must also recognize how the digital infrastructure of the future—especially 5G—could facilitate the spread of these vile uses of AI if it does not include safeguards. We must think about how to defend against such harmful applications and build an international consensus against their use. We must also encourage commercial alternatives that protect core American values—including individual privacy—to provide Americans and the world choices about the technology they will increasingly rely on.

A National Security Imperative

As we address potential threats and harms, we must also capitalize on the promise of AI technologies for our nation's defense and intelligence capabilities. The Commission has found that in important ways, AI will change how we defend the American homeland, how our intelligence agencies make sense of the world, and how our military deters adversaries and fights on future battlefields.

We must grasp the inevitability of AI and apply it to protect the American people and our allies and partners. The utility of the technology is extremely broad. In the context of homeland security, we see promise in applying AI to border protection, cyber defense and critical infrastructure protection, and counterterrorism and counterintelligence investigations. In the

intelligence realm, AI algorithms can sift through vast amounts of data to find patterns and identify correlations, while automating imagery analysis and other labor-intensive tasks. For our military, AI-enabled autonomous systems open up new possibilities for operational concepts and command decision-making that will give us advantages on the battlefield. If employed responsibly, we believe AI-enabled military systems can also help reduce risks to U.S. service members in the field and protect innocent lives in combat.

Guiding Principles

The Commission's work is guided by seven principles that we believe provide a solid foundation for action.

1. **Global leadership in AI technology is a national security priority.** The U.S. Government retains a core responsibility to steer advancements and make investments in ways that protect the American people and ensure a robust basic research environment. Private sector developments in AI are breathtaking, but federal investment is still necessary to sustain basic research and direct targeted investments for national security purposes.

2. **AI adoption for national security is imperative.** We see no way to protect the American people, U.S. interests, and shape the development of international norms for using AI if the United States is not leading the way in application. The future concepts of operations and capabilities necessary to defend our interests and our allies will be AI-enabled.

3. **Private sector leaders and government officials must build a shared sense of responsibility for the welfare and security of the American people.** The government needs help from industry and academia to maximize the promise of AI and minimize the national security risks posed by AI. Leading private sector developments across the range of applications will have to be "spun into" the government, while the government will have to help private companies—including social media companies—understand the AI threat environment from a national security perspective.

4. **People matter more than ever in the AI competition**. We must cultivate homegrown AI talent and continue to attract the world's best minds. Talent is the critical variable in the new age of competition. We are competing with strategic rivals and with our partners for the best AI talent. We also need to recognize that building an AI-literate national security workforce is a prerequisite for moving the enterprise into the digital age. As we will discuss below, progress will require some audacious action.

5. Actions taken to protect America's AI leadership from foreign threats must **preserve principles of free inquiry, free enterprise, and the free flow of ideas**. As we have seen recently, the government is taking the counterintelligence threat in technical and academic fields seriously, and it is taking action to protect critical technology advantages in fields like microelectronics. We support calibrated and tailored efforts. At the same time, we must not lose sight of enduring American principles and overly securitize basic research or the private sector.

6. At a basic level we see a convergence of interests and concerns between national security officials and those in the AI development and ethics community. Everyone wants safe, reliable AI systems, and at the same time recognizes today's technical limitations. Disagreements will persist about how to develop and use AI, but we believe there is **common ground that can serve as the basis for productive conversations**.

7. **Any use of AI by the United States must incorporate and promote American values**, including the rule of law.

We do not underestimate the challenge of translating principles into concrete recommendations. Much of the Commission's work is dedicated to analyzing the hard problems and doing the policy engineering to accelerate the government's adoption of AI to protect American interests. That includes designing recommendations to overcome the technical, bureaucratic, and cultural obstacles that prevent private sector best practices and technologies from being used for the national interest.

Commission Progress to Date

The Commission has moved with an urgency that is commensurate with the opportunity and the national security threat presented by AI. AI developments could not wait for a traditional approach to government commission work. We could not retreat for a year before delivering a final report. In coordination with the House and Senate Armed Services Committees, we instead decided to make recommendations over the course of 2020. We saw needs, identified practical solutions, and have made over 80 recommendations so far. Our Interim Report last November articulated a series of initial consensus judgments about the current state of affairs. This year, we began publishing a series of quarterly recommendation memos—and will deliver our third next month. We will deliver our final report to Congress and the President in March 2021. The recommendations cover research and development, national security applications, talent and workforce, promotion and protection of critical technologies, international partnerships, and ethics.

The Commission's View of the FY21 NDAA

We are encouraged to see several NSCAI recommendations reflected in the House and Senate versions of this year's NDAA, and would like to take this opportunity to comment on the importance of legislative action in five key areas. We believe it is crucial for these recommendations to reach the President's desk and become law.

1. ***Expanding AI Research and Development***

Both the House and Senate bills feature encouraging actions on federal government investment in AI research and development, public-private coordination, and establishment of technical standards.[2] The Commission shares these priorities.

We want to emphasize the importance of creating a National AI Research Resource. There is a growing divide in AI research between "haves" in the private sector and "have nots" in academia. Much of today's AI research depends on access to resource-intensive computation and large, curated data sets. These are held primarily in companies. We fear that this growing gap will degrade research and training at our universities.

We applaud recent investments made by the National Science Foundation (NSF) and its interagency partners to establish seven national AI institutes. This is a significant step toward building a nationwide network that will advance the technology and support the broad application of AI to science and engineering and across critical sectors of society.

A National AI Research Resource would support and complement this effort, democratizing access to AI R&D by removing the high-cost barrier to entry currently presented by large compute resources. It would also fuel research and training within the NSF institutes and more broadly, through access to machine learning-ready data sets, using real-world U.S. Government data. In effect, this would spread AI R&D beyond elite universities and big technology companies, and across many scientific fields. The result would be more distributed R&D infrastructure nationwide—and stronger connections among government, the commercial sector,

[2] The House version of the NDAA for FY 2021 incorporates the National Artificial Intelligence Initiative Act of 2020 in Division E, which would accelerate federal AI coordination and investment, and stimulate greater public-private partnership and AI standards development. H.R. 6395, The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 116th Cong. (2020) [hereinafter H.R. 6395]. The Senate version includes Amendment 2242, which would advance AI research and standards development, grant opportunities, and initiate an AI Scholarship-for-Service program. S. 4049, National Defense Authorization Act for Fiscal Year 2021, 116th Cong. (2020) [hereinafter S. 4049].

and academia. The provision in the House NDAA that would create a task force to plan for such a national capability is a strong step in the right direction.[3]

2. *DoD Organizational Reforms*

We have made a number of proposals to ensure the Department of Defense (DoD) is well positioned to excel in the AI era. In particular, we want to emphasize the need for a senior-level Steering Committee on Emerging Technology. This top-down approach would help the Department overcome some of the bureaucratic challenges that are impeding AI adoption. It would also focus concept and capability development on emerging threats, and guide defense investments to ensure strategic advantage against near-peer competitors.

Importantly, we believe this Steering Committee must include the Intelligence Community (IC). A central goal of our recommendation is to create a leadership mechanism that bridges DoD and the IC. This would better integrate intelligence analysis related to emerging technologies with defense capability development. And it would help ensure that DoD and the IC have a shared vision of national security needs and coherent, complementary investment strategies.[4]

We also recommend that the Director of the Joint Artificial Intelligence Center (JAIC) should report directly to the Secretary of Defense—or to the Deputy Secretary, if delegated. As with the senior-level Steering Committee, this top-down approach would ensure that AI applications are prioritized within the Department. Secretary Esper has stated that AI is the most important emerging technology to integrate and employ for advantage over our near-peer competitors.[5] We believe this reporting structure would drive organizational focus, preserve the Department's initial AI projects, enable their growth, and ensure the Department can develop the capabilities needed to successfully adopt AI applications at scale. The Commission supports the provision in

---

[3] See H.R. 6395, sec. 5107. For our full recommendation, see *First Quarter Recommendations Memo*, National Security Commission on Artificial Intelligence at 12 (Mar. 2020), https://www.nscai.gov/reports.

[4] The House's version of the NDAA for Fiscal Year 2021 would create a Steering Committee, but it would not include Intelligence Community representation. See H.R. 6395, sec. 241. For our full recommendation, see *First Quarter Recommendations Memo*, National Security Commission on Artificial Intelligence at 23 (Mar. 2020), https://www.nscai.gov/reports.

[5] See Deputy Secretary of Defense Memorandum for the Chief Management Officer on the Designation of a Senior Official with Primary Responsibility for Artificial Intelligence (Oct. 2, 2019); Testimony of The Honorable Mark T. Esper, *Confirmation Hearing on the Nomination of Hon. Mark T. Esper to be Secretary of Defense*, U.S. Senate Committee on Armed Services (July 16, 2019), 64, https://www.armed-services.senate.gov/imo/media/doc/19-59_07-16-19.pdf; Remarks by the Honorable Mark T. Esper, NSCAI Conference on Strength Through Innovation (Nov. 5, 2019).

the House NDAA that would make this change.[6] In addition, we think the JAIC should continue to be led by a three-star general or flag officer with significant operational experience.[7]

3. *Microelectronics*

We believe the United States needs a national strategy for microelectronics. Recent advances in AI have depended heavily on advances in available computing power. To preserve U.S. global leadership in AI, we need to preserve leadership in the underlying microelectronics.

In our initial reports, the Commission has put forward specific recommendations to lay the groundwork for long-term access to resilient, trusted, and assured microelectronics. We propose a portfolio-based approach to take advantage of American strengths and ensure the United States stays ahead of competitors in this field.

These steps should be part of a truly national strategy that would strengthen coordination among government agencies and with industry and academia. The strategy should integrate DoD's requirements and initiatives with actions taken by the Commerce and State Departments, and other agencies. It should promote domestic development of microelectronics, coordination with international allies, and protect against illicit technology transfer to competitors through targeted export controls and investment screening. The strategy would build upon the Defense Advanced Research Projects Agency's Electronics Resurgence Initiative, Department of Energy's (DOE) high-performance computing expertise, and NSF's work at the cutting edge of semiconductor research.

We are encouraged that the House and Senate versions of the NDAA contain a requirement for a microelectronics strategy.[8] The House's version more closely reflects the Commission's recommendations. It specifically calls for an assessment of the feasibility of a national laboratory focused on microelectronics—a concept the Commission has endorsed. Additionally, the House bill would establish an interagency advisory panel. We believe a strategy led by DoD alone would not be the kind of holistic, national strategy we need.

The United States also faces infrastructure and funding gaps for microelectronics research, development, and commercialization in the public and private sectors—all of which are important for maintaining U.S. leadership in semiconductors. The United States must maintain

---

[6] H.R. 6395, sec. 217.
[7] This recommendation is reflected in the conference report of the Senate Armed Services Committee on the NDAA for Fiscal Year 2021. S. 4049, *National Defense Authorization Act for Fiscal Year 2021 Report*, 116th Cong. at 214-215 (2020), https://www.congress.gov/116/crpt/srpt236/CRPT-116srpt236.pdf.
[8] H.R. 6395, sec. 247; S. 4049, sec. 807.

an innovative domestic microelectronics industry and research base to strengthen the U.S. economy and mitigate the threat posed by Chinese industrial policy and corresponding investments.

This is why the Commission strongly supports the provisions from the CHIPS for America Act (H.R. 7178 / S. 3933) that are included in the House and Senate versions of the NDAA.[9] These measures would strengthen the U.S. microelectronics manufacturing and research base. Congress should build on this momentum by fully funding these initiatives, and by passing a semiconductor R&D investment tax credit, which the Commission has endorsed.[10]

4. *Ethical and Responsible Use*

Determining how to use AI responsibly is central to the Commission's work. We recently published a detailed "paradigm" of issues and practices that government agencies should consider in developing and fielding AI. We believe these proposals can help DoD and the IC to operationalize their AI ethics principles.[11]

Within the government, it is important to develop an understanding of these principles and practices, and an awareness of the risks and limitations associated with AI systems. That is why we recommend that DoD, the IC, Department of Homeland Security (DHS), and Federal Bureau of Investigation (FBI) should conduct self-assessments. These should focus on several issues:

- Whether the department/agency has access to adequate in-house expertise—including ethical, legal, and technical expertise—to assist in the development and fielding of responsible AI systems;

- Whether current procurement processes sufficiently encourage or require such expertise to be utilized in acquiring commercial AI systems; and,

---

[9] See H.R. 6395, sec. 1821 and S. 4049, amendment 2244.
[10] For NSCAI recommendation regarding the CHIPS for America Act, see *Second Quarter Recommendations Memo,* National Security Commission on Artificial Intelligence at 67 (July 2020), https://www.nscai.gov/reports.
[11] See *Key Considerations for Responsible Development and Fielding of Artificial Intelligence*, National Security Commission on Artificial Intelligence at 93 (July 2020), https://drive.google.com/file/d/1_zkNkT3Trz3rtFc8KVrEBNlg2R9MaUpi/view. See also *AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense - Supporting Document*, Defense Innovation Board at 19 (Oct. 2019), https://media.defense.gov/2019/Oct/31/2002204459/-1/-1/0/DIB_AI_PRINCIPLES_SUPPORTING_DOCUMENT.PDF; and *Principles of Professional Ethics for the Intelligence Community*, Office of the Director of National Intelligence, https://www.dni.gov/index.php/who-we-are/organizations/clpt/clpt-related-menus/clpt-related-links/ic-principles-of-professional-ethics.

- Whether organizations have the ability and resources to consult outside experts when in-house expertise is insufficient.

If these assessments reveal inadequacies, we hope they lead to further actions to institute reforms. We support the provision in the House NDAA that would require such a self-assessment within DoD, and recommend expanding this provision to include the IC, DHS, and FBI as well.[12]

5. *Workforce Reforms*

Much of the Commission's early work has focused on building an AI-ready national security workforce. This includes recruiting experts and developers, training end users, identifying talented individuals, and promoting education. If the government cannot improve its recruitment and hiring, or raise the level of AI knowledge in its workforce, we will struggle to achieve any significant AI progress.

In particular, we support several provisions in the current versions of the NDAA. These include:

- Training courses in AI and related topics for human resources practitioners, to improve the government's recruitment of AI talent.[13]

- The creation of unclassified workspaces. This would allow organizations to hire and utilize new employees more quickly, while their security clearances are in process.[14]

- A pilot program for the use of electronic portfolios to evaluate applicants for certain technical positions. Because AI and software development are sometimes self-taught fields, experts do not always have resumes that effectively convey their knowledge. The pilot program would pair HR professionals with subject matter experts to better assess candidates' previous work as a tangible demonstration of his or her capabilities.[15]

- A program to track and reward the completion of certified AI training and courses. This would help agencies identify and capitalize on AI talent within the ranks.[16]

---

[12] H.R. 6395, sec. 248. For our full recommendation, see *First Quarter Recommendations Memo*, National Security Commission on Artificial Intelligence at 72 (Mar. 2020).
[13] H.R. 6395, sec. 242.
[14] H.R. 6395, sec. 243.
[15] H.R. 6395, sec. 244.
[16] H.R. 6395, sec. 245.

- A mechanism for hiring university faculty with relevant expertise to serve as part-time researchers in government laboratories. The government would benefit from access to more outside experts. We believe this mechanism should apply not only to DoD but also to DHS, Department of Commerce, DOE, and the IC.[17]

- Expanding the use of public-private talent exchange programs in DoD. We recommend expanding both the number of participants in general and the number of exchanges with AI-focused companies in particular. We also recommend creating an office to manage civilian talent exchanges and hold their billets.[18]

- An addition to the Armed Services Vocational Aptitude Battery Test to include testing for computational thinking. This would provide the military with a systematic way to identify potential AI talent.[19]

Two Bold Workforce Moves

Talent is the centerpiece of any winning AI strategy. The Commission has examined the government's current shortcomings and concluded that we must present a clean sheet approach to building a technology workforce to protect the American people. Existing programs will not bring enough digital talent into public service to meet serious shortages. Scholarship and service programs are limited in scale and will not create a common set of ideas, shared experiences, professional culture, or a common mission to improve the government's digital talent. We must fundamentally re-imagine the way the U.S. Government recruits and builds its digital workforce. In addition to the reforms above, we have made two significant proposals.

1. **Build the U.S. Digital Service Academy:** The U.S. Government should create a United States Digital Service Academy (USDSA) that produces technically educated graduates with a service obligation as civil servants. The USDSA would be an independent entity within the federal government, advised by an interagency board that would be assisted by a federal advisory committee composed of commercial and academic leaders in emerging technology. The academy would be a partnership between the public and private sectors, both working together towards a common goal of developing a modern, digitally proficient workforce.

[17] H.R. 6395, sec. 246 and S. 4049, sec. 216 would apply this mechanism to DoD only.
[18] H.R. 6395, sec. 249 captures our recommendation. For our full recommendation, see *First Quarter Recommendations*, National Security Commission on Artificial Intelligence at 42 (Mar. 2020).
[19] S. 4049, sec. 239 advances a variation of our recommendation. For our full recommendation, see *First Quarter Recommendations*, National Security Commission on Artificial Intelligence at 34 (Mar. 2020).

2. **Establish a National Reserve Digital Corps.** Many of the most talented technologists in the United States are eager to serve their country but are unlikely to become full time government employees or military reservists. The government needs a mechanism to tap this talent reservoir. The government should establish a National Reserve Digital Corps modeled after the military reserves that allows civilians to work for the government 38 days a year as advisors, instructors, and developers. We could incentivize participation with a training and education fund and a scholarship program modeled after Reserve Officer Training Corps or ROTC. While short-term volunteers are not a substitute for full-time employees, they can help improve AI education for both technologists and non-technical leaders, perform data triage and acquisition, help guide projects and frame technical solutions, build bridges between the public and private sector, and other important tasks.

Concluding Thoughts

Winning the AI competition is necessary but not sufficient to win the wider technology competition. AI is the primary enabler of, and the connective tissue in, a constellation of emerging technologies that will shape our future. Congress recognized this when it created NSCAI, wisely giving us the mandate to examine AI and "associated technologies."

While there is no single, definitive list of which technologies are the most important, a general consensus is emerging in government around AI. The Commission examined five recent lists of emerging technologies critical to U.S. national security offered separately by DoD, the Department of Commerce, the President's Council of Advisors on Science and Technology, and in the Senate's Endless Frontier Act (S.3832)—see Figure 1. Each list includes AI as a critical technology, while eight other technologies only appear in a majority of the lists: 1) biotechnology; 2) cybersecurity and data management; 3) quantum computing; 4) semiconductors; 5) robotics; 6) advanced communications; 7) advanced manufacturing; and, 8) hypersonics.

The constellation of technologies and the reality of budget limits presents a complicated equation. We need to consider how each of these emerging technologies will be critical to our long-term national competitiveness and then assess how the government can ensure we lead the way. We will need to place big bets on basic and applied research in several areas. We know calls for a national strategy are easy and frequent. But in this case, we need a comprehensive national technology strategy. AI is a centerpiece in what is really a new era of competition. We will need to understand how developments in one technology will impact others.

It is our mandate to help Congress understand the AI-national security nexus and make recommendations to enhance our security. Our mission is to ensure that the United States retains every advantage in AI so the United States can win the strategic competition. Our commitment is that every recommendation will be made with a deep sense of responsibility for the ethical implications of employing AI. We look forward to working together with Congress, the Executive Branch, the American people, and international partners as we move forward to a Final Report.

Figure 1

Emerging technologies identified in multiple U.S. Government lists of critical technology industries

	2018 National Defense Strategy	DoD List of Critical Emerging Technologies	Commerce ANPRM on Emerging Technologies	PCAST List of Industries of the Future	S.3832 - Endless Frontier Act	TOTAL
Artificial Intelligence / Machine Learning	✔	✔	✔	✔	✔	**5**
Biotechnology	✔	✔	✔	✔	✔	**5**
Cybersecurity, Data Storage and Data Management	✔	✔	✔	✔	✔	**5**
Quantum Computing		✔	✔	✔	✔	**4**
Semiconductors, Supercomputing, and Advanced Hardware	✔	✔	✔		✔	**4**
Robotics and Autonomy	✔	✔	✔		✔	**4**
Advanced Communications Technology / 5G		✔		✔	✔	**3**
Advanced Manufacturing			✔	✔	✔	**3**
Hypersonics	✔	✔	✔			**3**

Chairman

Eric Schmidt
Schmidt Futures

Nominated by then-Chairman and Current Ranking Member Mac Thornberry (R-TX), House Armed Services Committee

Dr. Eric Schmidt is the technical advisor to the board of Alphabet where he was formerly the executive chairman. As executive chairman, he was responsible for the external matters of all of the holding company's businesses, including Google Inc., advising their CEOs and leadership on business and policy issues.

Prior to the establishment of Alphabet, Eric was the chairman of Google Inc. for four years. From 2001-2011, Eric served as Google's chief executive officer, overseeing the company's technical and business strategy alongside founders Sergey Brin and Larry Page. Under his leadership, Google dramatically scaled its infrastructure and diversified its product offerings while maintaining a strong culture of innovation, growing from a Silicon Valley startup to a global leader in technology.

Prior to joining Google, Eric was the chairman and CEO of Novell and chief technology officer at Sun Microsystems, Inc. Previously, he served on the research staff at Xerox Palo Alto Research Center (PARC), Bell Laboratories and Zilog. He holds a bachelor's degree in electrical engineering from Princeton University as well as a master's degree and Ph.D. in computer science from the University of California, Berkeley.

Eric was elected to the National Academy of Engineering in 2006 and inducted into the American Academy of Arts and Sciences as a fellow in 2007. Since 2008, he has been a trustee of the Institute for Advanced Study in Princeton, New Jersey. Since 2012, Eric has been on the board of the Broad Institute and the Mayo Clinic. Eric was a member of the President's Council of Advisors on Science 2009-2017. In 2013, Eric and Jared Cohen co-authored The New York Times bestselling book, The New Digital Age: Transforming Nations, Businesses, and Our Lives. In September 2014, Eric published his second New York Times bestseller, How Google Works, which he and Jonathan Rosenberg co-authored with Alan Eagle. Eric became the Chairman of the Department of Defense's Innovation Board in 2016 and was awarded the Department of Defense Medal for Distinguished Public Service in January of 2017 by Secretary of Defense Ashton Carter.

Vice Chairman

Robert O. Work
Former Deputy Secretary of the Department of Defense

Nominated by Ranking Member Jack Reed (D-RI), Senate Armed Services Committee Secretary

Robert O. Work is the Distinguished Senior Fellow for Defense and National Security at the Center for a New American Security and the owner of TeamWork, LLC, which specializes in national security affairs and the future of warfare. Secretary Work previously served as the Deputy Secretary of Defense, where he was responsible for overseeing the day-to-day business of the Pentagon and developing the Department's $600 billion defense program. He is widely credited for his work with leaders in the Department and the intelligence community on the "Third Offset Strategy," which aimed to restore U.S. conventional overmatch over its strategic rivals and adversaries. He was awarded

DoD's Distinguished Public Service Award (twice), the National Intelligence Distinguished Public Service Award, and the Chairman of the Joint Chiefs of Staff Joint Distinguished Civilian Service Award.

Prior to serving as Deputy Secretary, Secretary Work spent one year as CEO of the CNAS, after serving as Undersecretary of the Navy from 2009–2013 in the first Obama administration. As the principal civilian deputy to the Secretary of the Navy, he was responsible for the smooth running of the U.S. naval global business enterprise, with over 500,000 active duty personnel and 200,000 government civilians, and a budget of $160 billion. He was twice awarded the Department of the Navy's Distinguished Civilian Service Award.

Commissioner

Mignon Clyburn
MLC Strategies

Nominated by then-Ranking Member and Current Chairman Frank Pallone, Jr. (D-NJ)

House Energy and Commerce Committee The Honorable Mignon Clyburn was sworn in for her first term as commissioner on August 3, 2009; sworn in for a second term on February 19, 2013; and served until June 6, 2018. She also served as Acting FCC Chairwoman from May 20, 2013 through November 4, 2013.

While at the FCC, Commissioner Clyburn was committed to closing the digital divide. Specifically, she was an advocate for Lifeline Modernization, which assists low income consumers defray the cost of broadband service, championed diversity in media ownership, initiated Inmate Calling Services reforms, emphasized diversity and inclusion in STEM opportunities, and fought to preserve a free and open internet.

Prior to the FCC, she spent 11 years as a member of the sixth district on the Public Service Commission (PSC) of South Carolina. Prior to the PSC, Clyburn was the publisher and general manager of her family-founded newspaper for 14 years, the Coastal Times, a Charleston-based weekly newspaper that focused primarily on issues affecting the African American community.

Commissioner

José-Marie Griffiths,
Dakota State University

Nominated by then-Chairman John Thune (R-SD), Senate Commerce Committee

Dr. José-Marie Griffiths is president of Dakota State University in Madison, South Dakota. President Griffiths has spent most of her career in research, teaching, public service, corporate leadership, economic development and higher education administration. She has been awarded presidential appointments to the National Science Board, the U.S. President's Information Technology Advisory Committee, and the U.S. National Commission on Libraries and Information. She has led projects for over 28 U.S. federal agencies including the National Science Foundation and NASA, over 20 major corporations such as AT&T Bell Laboratories and IBM, and seven major international organizations that include NATO and the United Nations. She has received over 20 significant awards in science, technology, teaching and the advancement of women in these fields.

WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING

SEPTEMBER 17, 2020

RESPONSE TO QUESTION SUBMITTED BY MR. LANGEVIN

Mr. WORK. The National Defense Authorization Act for Fiscal Year 2019 names the House and Senate Committees on Armed Services, Select Intelligence, and Commerce as the key committees of oversight for NSCAI. However, to get AI for national security right, many of the Commission's recommendations have included the jurisdiction of other committees. Advancing the AI for national security and defense needs requires taking action beyond traditional national security departments and agencies. Recommendations such as expanding research and development, growing an AI-ready workforce, and establishing ethical standards are examples of actions that often begin within other committees. To that end, NSCAI Commissioners and staff have engaged with individual members of Congress and a number of committees beyond our committees of oversight including, but not limited to, the House and Senate Committees on Appropriations; House Committee on Ways & Means; House Committee on Oversight and Reform; Senate Committee on Homeland Security and Governmental Affairs; House and Senate Committees on the Judiciary; House Committee on Science, Space, and Technology; House Committee on Homeland Security; House Committee on Foreign Affairs; Senate Committee on Foreign Relations; and Senate Committee on Energy and Natural Resources.

As we approach NSCAI's final report in March 2021, we welcome engaging further with you and your colleagues, including colleagues on other committees, to inform our findings and recommendations and educate Congress on the vital importance of U.S. leadership on this transformational emerging technology. [See page 15.]

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

SEPTEMBER 17, 2020

QUESTIONS SUBMITTED BY MR. WALTZ

Mr. WALTZ. Looking forward, there will continue to be a need for the government to pave the way on very specific innovations that satisfy specific government needs. But where there is invention in the private sector that can be harnessed, why not focus DOD efforts on enabling and co-opting what is already being done for our national defense? Industry is already heavily investing in R&D for AI technologies, so how can we make sure we are partnering with them?

The COMMISSIONERS. As the Commission noted in our Interim Report, private sector leaders and government officials must build a shared sense of responsibility for the welfare and security of the American people. The government needs help from industry and academia to maximize the promise of AI and minimize the national security risks posed by AI. American companies are at the forefront of AI developments. Their investments dwarf federal R&D; they generate many of the major breakthroughs; and, they are on the frontlines of defending against cyber threats and malicious uses of AI applications. To harness the full potential of private sector innovation, the government must adapt internally, modernizing its platforms, policies, and procedures to improve access to commercial breakthroughs and create the environmental conditions for success. At the same time, the government must also grow the innovation base, investing in early-stage AI research across the commercial sector and academia. In our first quarter and second quarter memos, the Commission recommended a number of Executive and Legislative Branch actions that the U.S. Government could take to improve its ability to leverage commercial advances in AI. While no single recommendation will ensure successful partnership between the private sector, academia, and the government, the Commission believes that these actions could set in motion a closer collaboration between the two sectors, as they would forge a common commitment to protecting our values, free market principles, national defense, and security.

Mr. WALTZ. Keeping up with the general theme of maintaining AI leadership globally, how can the U.S. compete with countries like Russia and China who have much laxer laws on competition, privacy and the like?

The COMMISSIONERS. History has shown that the United States has a unique ability to galvanize international coalitions around core shared values. The Commission believes that the U.S. approach to AI enshrines these shared values and represents an asymmetrical advantage that the United States has over authoritarian regimes. U.S. leadership will endure to the extent the United States can continue to be at the forefront of innovation and technical expertise. Global leadership in AI technology is a national security priority. Given the centrality of AI to the future of our economy, society, and security, the U.S. Government must pursue an investment strategy that extends America's technological edge. Global leadership gives our defense and security agencies access to the best technology, and puts the United States in the best position to secure that technology against vulnerabilities and develop international norms and standards for responsible use. While American companies play a significant role in advancing AI research and development, the government retains a core responsibility to steer advancements in ways that protect the American people and foster a robust basic research environment. People are still essential. Talent remains the most important driver of progress in all facets of AI. We must prioritize cultivating homegrown talent by making long-term investments in STEM education. In the near term, high-skilled immigration is important for rapidly growing America's talent pool. One of America's advantages is the fact that its universities, companies, and innovation culture are magnets for the world's best AI talent. We need to encourage that talent to come, contribute, and stay. Within government, recruiting, training, and retaining AI-talent will be essential to maximize AI's potential. Diplomatically, to maintain global leadership in AI requires the United States to attract partners and allies around these values and take steps to make those partnerships and alliances more resilient—focusing on the economic, security, and technological benefits of alignment with free and open states rather than repressive regimes around world-changing technology like AI. In recent years, we have seen this in action. The rise of several important multilateral coalitions, including the D10 initiative and the Global Partnership on AI, bring together like-minded nations to develop AI norms, principles, and applications consistent with their values. Likewise, U.S. efforts to galvanize worldwide support against Chinese 5G technology has proven significant as the number of nations opposed to Chinese

technology continues to grow. The United States must continue to lead the world. The Commission is committed to driving changes that will maintain this lead by maximizing the role of AI in protecting U.S. security, extending American leadership in emerging technologies, and strengthening our core values, and the Commission will continue to push for these important changes as we work toward our final report due to Congress in March 2021.

Mr. WALTZ. I am concerned about the challenges you identified for the government to find and maintain an adequate AI literate workforce. And I am interested to explore how we can harness the power of our universities to create and strengthen the AI workforce we need. I noticed a new and remarkable partnership between the University of Florida, a top educational institution in my home state that is currently ranked #6 among public universities and #1 in technology transfer and innovation, and NVIDIA, the major computer hardware company in the world. Come December, UF will be the first institution of higher learning in the U.S. to receive NVIDIA's DGX A100 systems, which are designed to accelerate diverse workloads, including AI training, inference, and data analytics. Together with their HiPerGator3 supercomputer, UF will be home to one of the fastest, most powerful computers in higher education. As a comprehensive educational institution, UF will be among the nation's first to integrate AI across all disciplines and make it a ubiquitous part of its curriculum. It will offer certificates and degree programs in AI and data science, with curriculum modules for specific technical and industry-focused domains.

Can you tell us about the concept of creating a U.S. digital academy or AI university that would be on par with the other service academies?

In addition to the academy model, are you considering mirroring the ROTC model of progressive scholarship with a service requirement upon completion to create AI ready graduates to step into government positions?

The COMMISSIONERS. The concept of the United States Digital Service Academy (USDSA) began with our finding that there is a severe shortage of AI knowledge across our United States Government. While addressing issues with the hiring process and expanding scholarship for service programs are both necessary and helpful, they are also insufficient to address the government's overall technologist deficit. To solve this problem, we argue the government must re-imagine the way it recruits and builds its digital workforce.

USDSA would provide two major benefits. First, it would produce large numbers of technically educated graduates that would serve in government. USDSA would be an accredited, degree-granting university, with a mission: "to develop, educate, train, and inspire digital technology leaders and innovators and imbue them with the highest ideals of duty, honor, and service to the United States of America in order to prepare them to lead in service to our nation."

Students would receive a technical education during the school year, and participate in government and private-sector internships during the summer. They would graduate with a degree and the technical competencies that are needed within the government, and owe no student debts. Instead, and to your question, USDSA graduates would become civil servants with a five-year obligation to serve in the U.S. Government. We believe that USDSA should be an independent entity within the Federal Government, advised by an interagency board and assisted by a federal advisory committee composed of commercial and academic leaders in emerging technologies. This interagency board would allow agencies to bring forward their digital workforce requirements through a formal process annually and help align graduates of USDSA to the government's workforce needs by agency and by career field.

With regard to mirroring ROTC, that model is closely aligned to existing scholarship for service programs, which offer a three-year program in school for three years of government service upon graduation. Our Second Quarter memorandum includes a recommendation to significantly expand CyberCorps: Scholarship for Service and SMART: Scholarship-for-Service, with an increased focus on AI-related topics. Our Second Quarter Recommendations memo provided a three-pronged approach to developing a "Digital Corps" concept. The first prong being a civilian reserve force with the National Reserve Digital Corps (NRDC) concept for part-time civilian government work. The second and third prongs were focused on full-time civilian government work in the expansion of scholarship for service programs and the creation of an USDSA. These three recommendations together provide multiple paths to address our current and future government civilian part-time and full-time needs with diverse pipelines to bring talent into the government civilian workforce.

○