FINAL RECOMMENDATIONS OF THE NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS

OF THE

COMMITTEE ON ARMED SERVICES

MEETING JOINTLY WITH THE

SUBCOMMITTEE ON NATIONAL SECURITY

OF THE

COMMITTEE ON OVERSIGHT AND REFORM

[Serial No. 117–7]

HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

HEARING HELD
MARCH 12, 2021

COMMITTEE ON ARMED SERVICES

SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES,
AND INFORMATION SYSTEMS

JAMES R. LANGEVIN, Rhode Island, *Chairman*

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

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

BESS DOPKEEN, *Professional Staff Member*
CHRIS VIESON, *Professional Staff Member*
CAROLINE KEHRLI, *Clerk*

————

COMMITTEE ON OVERSIGHT AND REFORM

SUBCOMMITTEE ON NATIONAL SECURITY

STEPHEN F. LYNCH, Massachusetts, *Chairman*

PETER WELCH, Vermont
HENRY C. "HANK" JOHNSON, JR., Georgia
MARK DeSAULNIER, California
KWEISI MFUME, Maryland
DEBBIE WASSERMAN SCHULTZ, Florida
JACKIE SPEIER, California

GLENN GROTHMAN, Wisconsin, *Ranking Member*
PAUL A. GOSAR, Arizona
VIRGINIA FOXX, North Carolina
BOB GIBBS, Ohio
CLAY HIGGINS, Louisiana

RUSS ANELLO, *Majority Staff Director*
MARK MARIN, *Minority Staff Director*
DAN REBNORD, *Subcommittee Staff Director*

CONTENTS

_____

FINAL RECOMMENDATIONS OF THE NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

––––––––––

HOUSE OF REPRESENTATIVES, COMMITTEE ON ARMED SERVICES, SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS, MEETING JOINTLY WITH THE COMMITTEE ON OVERSIGHT AND RE-FORM, SUBCOMMITTEE ON NATIONAL SECURITY, *Washington, DC, Friday, March 12, 2021.*

The subcommittee met, pursuant to call, at 11:03 a.m., in room 2118, Rayburn House Office Building, Hon. James Langevin (chairman of the Subcommittee on Cyber, Innovative Technologies, and Information Systems) presiding.

OPENING STATEMENT OF HON. JAMES R. LANGEVIN, A REPRE-SENTATIVE FROM RHODE ISLAND, CHAIRMAN, SUBCOMMIT-TEE ON CYBER, INNOVATIVE TECHNOLOGIES, AND INFOR-MATION SYSTEMS, COMMITTEE ON ARMED SERVICES

Mr. LANGEVIN. Good morning, everyone. I call this joint sub-committee hearing together with the Subcommittee on Cyber, Innovation Technologies, and Information Systems, along with the Sub-committee on Oversight and Government Reform—National Security Subcommittee.

Good morning, everyone. Before I begin my opening statement, I'm just going to give a brief technical readout for those members that are participating remotely. I think most members are participating remotely this morning.

But, again, I want to welcome members who are joining us at today's joint hearing remotely. Members who are joining remotely must be visible on screen for the purposes of identifying—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 are experiencing 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. Video of members' participation will be broadcast in the room and via the television internet feeds.

Members participating remotely must be—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 software platform videos—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 for a— 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've designated a committee staff member to, if necessary, mute unrecognized members' microphones to cancel any inadvertent background noise that may disrupt the proceeding.

So with that technical message out of the way, I'm now going to proceed with my opening statement and then turn to Ranking Member Stefanik.

Well, I want to welcome everyone to our joint hearing with the House Committee on Oversight and Reform Subcommittee on National Security, which will review the final recommendations of the National Security Commission on Artificial Intelligence.

We welcome the subcommittee chairman, Stephen Lynch, my good friend from Massachusetts, and Ranking Member Glenn Grothman, and we are also pleased to host our House Armed Services Committee Chairman Adam Smith and Ranking Member Mike Rogers. Looks like we have a full house today. So I'm looking forward to this very meaningful and exciting hearing.

So I'm pleased to welcome, of course, most especially, four commissioners for the National Security Commission on Artificial Intelligence, a commission that was created by the House Armed Services Committee in the National Defense Authorization Act for Fiscal Year 2019 to help us advance the development of artificial intelligence, machine learning, and associated technologies to prepare the defense enterprise for the national security challenges of the future.

We asked this commission to produce a bipartisan whole-of-government effort focused on solving national security issues. We appreciate the leadership and hard work of our witnesses and we owe each of them an immense debt of gratitude.

Today, we welcome Dr. Eric Schmidt, chairman of the Commission; also, the Honorable Robert Work, vice chairman; the Honorable Mignon Clyburn, commissioner on the workforce and ethics lines of effort; and Dr. Gilman Louie, commissioner on the lines of effort focused on protecting and building on AI advantages, marshaling global cooperation, and threat analysis and response actions.

While many of the commissioners hail from the tech sector, the world's understanding of artificial intelligence truly began in government defense labs, and specifically with investments by the Department of Defense Advanced Research Projects Agency, DARPA, and the Office of Naval Research.

Now, decades later, we must redouble our focus on the power of defense science and technology research to propel us into the future. So I look forward to hearing the commissioners' recommenda-

tions on investments in basic and applied research and how to encourage faster adoption of innovative and cutting-edge capabilities.

The next-generation challenges are upon us, and in our last subcommittee hearing we talked about how the Department can transform innovation into reality, specifically by orienting ourselves, the software, and data capabilities that are often the beating heart of the platforms we require and that promise to dramatically improve decision-making and optimization processes.

The battlespace of the future will be a complex web of software, networks, and data—and data integrated across domains and among our allies. Artificial intelligence and other next-generation innovations will be crucial in order to harness the power of data to give our men and women in uniform an edge in any future conflict.

Our potential adversaries, of course, are already investing heavily in this future as well. So this Commission has undertaken the difficult task to articulate the potential of artificial intelligence and the risks and benefits that lie ahead.

They have worked through these issues and identified recommendations related to research and software development, opportunities for international partnerships, safeguarding against our adversaries' advancements in this space, and cultivating a 21st century workforce.

Above all, the Commission has crucial recommendations related to building and deploying AI [artificial intelligence] in an ethical manner that is respectful of human rights. Indeed, that last category is what sets our Nation apart.

I commend the Defense Innovation Board, which was also chaired until last year by Dr. Schmidt, to helping the Department begin important discussions on ethics in AI.

Last year, Ranking Member Stefanik and I, along with Chairman Smith and Ranking Member Thornberry, championed a package of provisions based on the Commission's first quarter recommendations that yielded 13 provisions in the National Defense Authorization Act for Fiscal Year 2021, with the majority deriving from the Commission's call to strengthen the AI workforce.

That STEM [science, technology, engineering, and mathematics] 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. We must move past old models of training and learning, and establish a system to dynamically upskill our workforce as the technology evolves.

Ranking Member Stefanik and I were pleased to invite Commission representatives for a review of the interim recommendations last fall and we look forward to hearing about your recently released final recommendations to Congress.

Incredibly, there are over 100 in total and over 50 related to the purview of the Armed Services Committee.

So we commend you for all your work that you put into this effort these past 2 years. We are grateful for that work and that due diligence, and we look forward to receiving your testimony today.

So with that, I'll now turn to Ranking Member Stefanik for her remarks.

[The prepared statement of Mr. Langevin can be found in the Appendix on page 51.]

STATEMENT OF HON. ELISE STEFANIK, A REPRESENTATIVE FROM NEW YORK, RANKING MEMBER, SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS, COMMITTEE ON ARMED SERVICES

Ms. STEFANIK. Thank you, Chairman Langevin.

The National Security Commission on Artificial Intelligence is a critical step forward that I'm proud to have championed in the House with my colleagues on a bipartisan basis, and today's hearing is a culmination of years of hard work of our Commission

Chairman Schmidt, Vice Chairman Work, Commissioner Clyburn, and Commissioner Louie, thank you for serving on the Commission and for testifying today. Your efforts will serve as a blueprint for how our country will respond to, develop, and lead the world in artificial intelligence capabilities.

As we know, AI not only brings immense technological opportunities and innovation, but AI will also bring significant risks as our adversaries will deploy AI to challenge American interests and securities on our shores and abroad.

And importantly, as you laid out in your final recommendations, AI will affect every facet of life going forward, from civil society to our economy and, of course, national security.

For the Department of Defense [DOD] specifically, this final report is stark in its assessment. China will surpass the United States in AI leadership and win the innovation race if we fail to invest in emerging technologies and if we fail to take a whole-of-government approach to AI.

The impact on our national security is profound and disturbing, and the report concluded that China will achieve superiority over the U.S. within the next decade if we don't solve our organizational and investment challenges by 2025, just 4 years from now.

We face hard choices, given our limited resources to maintain that technological advantage over China. Future conflicts will take place on an AI battlefield and we must consider the future of systems that are not AI enabled.

Simply put, DOD must be willing to take on risk and Congress should support those efforts. Further, the U.S. cannot win this competition if we don't have the right workforce. The Commission highlighted our talent deficit and concluded this problem is the greatest impediment to being AI-ready by 2025.

Chairman Langevin and I are committed to solving this talent deficit, and last year we introduced legislation to retain technical talent here in the U.S. I also look forward to hearing more about the Digital Service Academy recommendation and other ways we can develop the necessary workforce within the DOD.

Alternatively, our private sector is driving many of the advancements in AI and we should encourage increased collaboration between the Department and private sector partners.

This subcommittee understands the issues many companies have interacting with DOD, primarily the onerous acquisition process. This report underscores the importance of reducing red tape so the Department doesn't hinder cooperation with the private sector.

Again, I'm very proud of the work accomplished by this Commission and the work that we did to include many of the recommendations in last year's NDAA [National Defense Authorization Act].

But more work must be done. Our warfighters must have most advanced technological capabilities to deter and defeat our adversaries in an AI environment.

To improve the lethality capabilities of our forces, we must continue supporting the Joint Artificial Intelligence Center and enable the services and combatant commands to develop, tailor, and deploy AI systems to the battlespace.

I look forward to the presentation today and the discussion, and I yield back.

Mr. LANGEVIN. Thank you, Ranking Member Stefanik.

I now recognize Chairman Lynch for his remarks.

STATEMENT OF HON. STEPHEN LYNCH, A REPRESENTATIVE FROM MASSACHUSETTS, CHAIRMAN, SUBCOMMITTEE ON NATIONAL SECURITY, COMMITTEE ON OVERSIGHT AND RE-FORM

Mr. LYNCH. Good morning, Mr. Chairman. Thank you very much.

Before I begin, I do want to thank you, Mr. Chairman, for your continued leadership in the areas of cyberspace operations, artificial intelligence, and other developing technologies, all with critical implications for our national security.

I'm pleased to join Chairman Smith, Ranking Member Stefanik, and Ranking Member Grothman as our subcommittee conducts today's important work to examine the final report released earlier this month by the National Security Commission on Artificial Intelligence.

AI carries the remarkable potential to enhance and even transform our national security. We're already beginning to integrate AI algorithms, applications, and systems to facilitate intelligence collection and analysis, including to detect and prevent future terrorist attacks.

We're also deploying AI to support battlefield medical evacuations, logistical missions, and military operations in Iraq, Syria, and Afghanistan, and other conflict zones.

On the Financial Services Committee, where I serve as chairman of the Task Force on Financial Technology, we're seeing the use of AI and machine-learning technology to enhance international investigations to combat terrorism, financing, and money laundering.

However, the evolution of artificial intelligence has also heightened the prospect that America's adversaries will win the race to develop and deploy AI, and to do so for malign purposes.

To the great detriment of our national security, as reported by the National Security Commission on Artificial Intelligence, and this is a quote, "AI is expanding the window of vulnerability that the United States has already entered. For the first time since World War II, America's technological predominance, the backbone of its economic and military power, is under threat," closed quote.

Clearly, cybersecurity has become synonymous with national security, and our fundamental duty to protect our democracy requires that we become, quote, "AI-ready," with resources, personnel, and strategies necessary to meet these urgent challenges.

According to the Commission, however, we are a long way from that goal. Absent shifting trends, quote, "China possesses the might, the talent, and ambition to surpass the United States as the world's leader in AI in the next decade."

In his 2020 book, "The Kill Chain: Defending America in the Future of High-Tech Warfare," Christian Brose, who is a former staff director of the Senate Armed Services Committee under Chairman John McCain, articulates that, quote, "A core pillar of the Chinese Communist Party's plan in harnessing emerging technology is to leapfrog the United States and become the world's preeminent power."

In fact, the 2017 development plan on artificial intelligence issued by China's State Council envisioned that China will lead the international AI sector as soon as 2030.

It's also worth noting that in the race to develop and deploy AI, our adversaries, such as the Russian Federation and the People's Republic of China, do not struggle with the moral restrictions faced by democratic governments on the use of AI-enabled autonomous weapons, nor are they hindered by moral considerations regarding the impact of AI on civil liberties.

However, thanks to the expertise and the dedication of the NSCAI [National Security Commission on Artificial Intelligence] commissioners and their staff, this final report that they have released earlier this month sets forth a comprehensive blueprint to help the new administration and Congress allocate appropriate Federal resources toward the advancement and integration of AI technologies, technical infrastructure, and a digitally proficient workforce.

We must also work together to ensure that these efforts maximize the opportunity for robust oversight, transparency and accountability that reflect our compelling national interest in safeguarding the civil liberties of all Americans.

To that end, I'm proud to be an original co-sponsor of Representative Lori Trahan's upcoming legislation to establish a Digital Service Academy. The creation of a fully accredited university to train future public servants in artificial intelligence and other digital fields is a principal recommendation included in the Commission's final report.

I want to thank you, Mr. Chairman. I look forward to today's hearing and discussing these issues with our distinguished panelists.

And I yield back the balance of my time.

Mr. LANGEVIN. Thank you, Chairman Lynch. And again, I'm grateful that you and I could team up to bring our two subcommittees together on this very important topic, and I thank you for your leadership.

With that, we'll now turn to Ranking Member Grothman for his remarks.

STATEMENT OF HON. GLENN GROTHMAN, A REPRESENTATIVE FROM WISCONSIN, RANKING MEMBER, SUBCOMMITTEE ON NATIONAL SECURITY, COMMITTEE ON OVERSIGHT AND RE-FORM

Mr. GROTHMAN. All very pleasant today. Great to start off the day by hearing a nice Boston accent.

I first want to thank Chairman Langevin and Ranking Member Stefanik for inviting us to join in this important meeting. I thank Chairman Lynch as well for having us.

Advancing American technology safely and effectively should be a bipartisan policy priority. I also want to thank our witnesses here today, and I particularly thank you for not having us see you on a Zoom. To see you live and in person is a real treat for us Congressmen.

You authored an impressive and thorough report on the future of artificial intelligence, or AI, and gave Congress and the executive a roadmap on how to proceed. Government use of artificial intelligence poses significant and potentially positive outcomes, but also significant challenges, particularly surrounding ethical use and data security.

I think it's the duty of Congress to examine both the positives and negatives of AI prior to authorizing what is likely to be billions of dollars for decades.

Your report highlights much of this but I want to focus on two main topics: improving the government and ensuring privacy.

The purpose of civilian government use of AI should be to decrease the footprint and size while increasing the efficiency and effectiveness of the Federal Government. It would defeat the purpose of massive investment in an automation technology to simply expand the size and scope of agencies instead of streamlining the workforce.

An analysis by Deloitte suggests that smart use of AI can save billions of man-hours and billions of dollars. The level of—this level of savings can only be experienced if the government makes cuts where AI allows us. We can see these benefits already taking place all over the government, like at the Social Security Administration and the Patent and Trademark Office.

As the technology grows and advances, so must our workforce. The government growth—let me see here. The government must get better at recruiting and retaining top talent. To achieve the benefits of AI, we must be able to assure our fellow Americans that the data is safe and the technology is being used ethically.

AI can be prone to false positives and negatives and overreliance on suspected patterns. It also relies on massive amounts of data in order to continue to learn and evolve. We must protect this data through data stewardship requirements, data transparency and disclosure rules, data governance rules, and data collection rules.

These protections must be put in place. We can see the dangers of runaway AI use in China. Using AI to support genocide in Xinjiang and suppress democracy in Hong Kong provides insight into how our adversaries view and use this technology—I'll say rather than suppress democracy, I guess I should say suppress freedom—as a way to suppress dissent and to become a global and economic military power.

It is vital that the U.S. counter these actions. I look forward to hearing from our witnesses today about how we can balance the new global arms race with government efficiency and privacy.

Thank you. I yield back.

Mr. LANGEVIN. Thank you, Ranking Member Grothman, for your remarks. We will now hear from our witnesses, then move into the question and answer session.

With that—and I just want to make sure that Chairman Smith or Ranking Member Rogers didn't have any opening comments.

Mr. SMITH. I'm good. Thanks, Jim.

Mr. LANGEVIN. Okay, very good. And I don't know if the ranking member is on, if he had any comments.

Hearing none, okay. Then we will—we will now turn to our witnesses, as I said, and then move to the question and answer period.

I'd like to now recognize Dr. Eric Schmidt, Chairman of the Commission. Dr. Schmidt is the co-founder of Schmidt Futures, was the technical adviser to the board of Alphabet, and before that, the CEO [chief executive officer] of Google. He has a distinguished record of contributions to the national security technology community, including chairing the Defense Innovation Board.

Dr. Schmidt, as a commissioner on the Cyberspace Solarium Commission, I just want to say a big thank you for your commitment to ensuring that the two Commissions work together, and let me say how pleased I am to see you champion some of the Solarium's recommendations as well.

So we are deeply in your debt. I'm grateful for your contributions in these areas, and I now recognize you to summarize your testimony for 5 minutes.

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

Dr. SCHMIDT. Well, thank you, Chairman Langevin, Ranking Member Stefanik, Chairman Lynch, Ranking Member Grothman, and the members of all the committees.

I am very pleased on behalf of all the commissioners to present 751 pages, which you asked us to produce more than 2 years ago, and I could not be prouder of this report and its—both the quality and the heft are worth noting.

More than 2 years ago, this committee, the House Armed Services Committee, foresaw the huge impact of AI on our society and our national security, and also foresaw the future and potential, perhaps likely, threats from our opponents.

And that process, along the way we worked with you in the NDAA a year ago to get some important changes in the legislation that will really help our Nation.

Just overall, I cannot say enough about the way we've worked together, the support that you all have given us, and an opportunity that you've given us to serve the Nation.

What I thought I'd do right now is just give a quick summary of where the report is, and my fellow commissioners can take you into some of the very interesting detail.

We reached a number of overarching judgments. The first is that the government is not organized nor resourced to win the technology competition against a committed competitor, and it's not pre-

pared to defend against AI-enabled threats and we strongly believe that our Nation needs to be AI-ready by 2025 to defend and compete in the coming era of AI-accelerated competition and conflict.

So we put the report into two parts. The first part is "Part I: Defending America in the AI Era," and it's fundamentally how the U.S. government can use AI technologies to protect the American people and our interests. It focuses on the implications of applications of AI for defense and security.

The second part is "Winning the Technology Competition." It's obvious, by the way, we should win that. Recommends government actions to promote AI innovation, promote national competitiveness, and protect critical U.S. advantages in the larger strategic competition with China.

In the idea of simplifying what we need to get done, we came up with four priorities with a great many details, as you'll hear about.

The first one is leadership. The government isn't quite ready for this fight. It's not organized in the right way. We need organizational structures that accelerate the government's integration of AI and the promotion of AI across the country.

There needs to be something at the White House. We're proposing a Technology Competitiveness Council reporting in to the Vice President that would precisely monitor and drive this transformation that we need.

And by the way, it's not just the government. It's also in private sector.

Talent. As you've identified—a number of you have in your opening comments—there's a huge talent deficit in the government. We need to build new digital talent pipelines and expand existing programs.

We need to cultivate AI talent nationwide and ensure the best technologists come to the U.S. and stay in the U.S. and don't go to our competitors. Seems sort of obvious but incredibly important to emphasize.

In hardware, the AI systems are critically dependent upon powerful hardware and we, as a country, are too dependent on semiconductor manufacturing in East Asia and Taiwan in particular.

Most cutting-edge plants are produced in a specific plant that's 110 miles from China. That's got to be an issue. We must revitalize U.S. cutting-edge semiconductor fabs and implement a national microelectronics strategy.

We state very clearly in our report that the objectives is to stay two generations ahead of the Chinese effort. It could not be clearer, in our view.

And the fourth, of course, is innovation. AI research is very expensive. We need the government to help set the conditions for broad-based innovation across the country.

We need, for example, a national AI research infrastructure so more than the top five companies have the resources to innovate, and in particular, startups and universities need this facility.

And we also need to add, we think over 5, 6, 7 years, up to $40 billion in annual funding in the next 5 years to cover AI R&D [research and development] for defense and nondefense purposes.

And as you highlighted, Mr. Chairman, in your comments, there are other things that are crossing edge. The first is partnerships.

We need to build coalitions with like-minded nations, the technology democracies—the techno democracies, in my own verbiage—to advance the development and use of AI in emerging technologies that support our values, which is critical. We spent a lot of time on our report talking about values.

And the second one, consistent with the values, is responsible use. In the face of digital authoritarianism, we need, we, the U.S., need to present a democratic model of responsible use of AI for national security.

You can imagine the opponents and how they might use or misuse these things. The trust of our Nation, the trust of our citizens, will hinge on justified assurance that the government's use of AI will respect privacy, civil liberties, and civil rights. We have a set of recommendations along those lines.

I really thank you all for giving us this opportunity. It has been a true privilege for me to be part of this and to help lead it.

Thank you very much.

[The joint prepared statement of Dr. Schmidt, Secretary Work, Ms. Clyburn, and Mr. Louie can be found in the Appendix on page 54.]

Mr. LANGEVIN. Thank you, Chairman Schmidt.

With that, next we will hear from the Honorable Robert Work, Vice Chair of the Commission. Secretary Work is a former Deputy Secretary of Defense and Under Secretary of the Navy.

Secretary Work's commitment to innovative strategic thinking is well known, and I welcome him back before us today.

Dr. Work, you are now recognized to summarize your testimony for 5 minutes.

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

Secretary WORK. Thank you, Chairman Langevin, Ranking Member Stefanik, Chairman Lynch, Ranking Member Grothman, and members of the committee. Thank you for having us today. It's a great opportunity to testify before you.

I'd like to follow Eric's broad overview with a focus on the parts of our report that deal with national defense. The Commission fears that our Armed Forces will lose their competitive military technical advantage within the next decade if they do not accelerate the adoption of AI across all their military missions.

Now, the intelligence record, we think, is quite clear. I also would just like to note that we have a classified annex that I would commend to all of the members. It is a summation of the intelligence record of what we think or know what our competitors are doing with AI.

We're not going to be able to defend against AI-enabled threats without ubiquitous AI capabilities of our own, and new warfighting concepts and paradigms. Without question, an AI-enabled force is going to be more effective. AI-enabled systems can make targeting more discriminant and precise, thereby reducing civilian casualties and damage to civilian infrastructure and other protected entities.

It will improve the tempo, speed, and scale of operations and it will enhance the way the battlefield can be monitored. It will help

the way that commanders understand what is happening in the battlespace.

It will also augment the abilities of service members including the way they perceive, understand, decide, adapt, and act in the course of all their missions.

As Eric has said, if we are going to win this competition, we think we need to be what we call AI-ready by 2025, which by that we mean we will have the foundation in place for the widespread integration of AI across the force.

There are four main ingredients to achieve this vision. First is top down leadership and strategic direction. On a transformation of the scale that we believe is necessary, you have to have strong top-down leadership.

They set the priorities. They overcome the barriers to change. We think the JAIC's [Joint Artificial Intelligence Center's] new reporting structure established in the NDAA is a strong first step. Congress should also direct the Department, in our view, to form a steering committee on emerging technology that includes representation from the intelligence community, and this steering committee would drive action on AI and emerging technologies.

Priorities should be implemented through a technology annex in the National Defense and Intelligence Strategies. The committee would align priorities, strategy, and resources across OSD [Office of the Secretary of Defense], the Joint Staff, and the intelligence community.

Effective integration of the AI is absolutely going to require a close partnership between the technologists and the warfighters. To ensure technical expertise informs capability and requirements decisions at the highest level, we recommend that the U.S.—the Under Secretary of Defense for Research and Engineering be made the co-chair and the Chief Science Advisor for the Joint Requirements Oversight Council, or JROC.

We also believe the Department should set specific AI readiness performance goals by the end of fiscal year 2021, and this will drive the outcomes of being AI-ready by 2025.

Second, the Department, we think, must ensure it has in place the resources, processes, and organizations to enable AI innovation. The Department needs to establish a common digital ecosystem.

It's called the Joint Common Foundation in the Department of Defense. That's good for a start. That's the technical foundation for all AI development fielding. So it's going to include access to a secure cloud, AI software, trained models, data, and algorithms, as well as high-performance computing power and a development environment that allows the entire AI stack to be put together in a way that is secure and will do what we expect it to do on the battlefield.

We think JAIC should be designated as the Department's AI accelerant. The JAIC, in our view, should focus on applications, not on hard research. Essentially, the JAIC's role is to try to get as many applications into the field as possible, and they provide the resources through the digital ecosystem or the Joint Common Foundation.

They also can provide subject matter expertise to support AI efforts across the Department without becoming a central clearing-

house. The Department has to expand the use of specialized acquisition pathways and contracting authorities to source and deliver the best AI.

Ranking Member Stefanik mentioned this. Software and algorithms are just a different kettle of fish than ships, airplanes, missiles, et cetera, and we have to come up with ways that are specific to get those algorithms and models developed and into the hands of our warfighters.

We have to come together also to reform the planning, programming, budgeting, and execution process. Congress has provided us—excuse me, provided the Department of Defense with an expanded toolkit of acquisition and contracting approaches, and the Department's effort to adopt AI will be impeded by processes that are unsuited to digital technologies and the pace of development of AI right now.

The Department should also increase its overall S&T [science and technology] spending and increase AI R&D to $8 billion annually by 2025.

We think that's totally appropriate within the size of the DOD R&D budget, which is the largest in its history.

Third, we think AI adoption has to be accelerated. We think one of the ways to get these algorithms and models across the valley of death and into the hands of the warfighter would be if Congress could create a dedicated AI fund specifically designed to speed operational prototyping and transition, overseen by the Under Secretary of Defense for R&E.

We think the Department should prioritize adoption of commercial AI solutions, especially to its core business processes and administrative processes, as well as logistics and sustainment systems.

Technologists should be integrated at every level in the Department, in the administrative side as well as the operational side. This would mean, for example, standing up AI development teams at the COCOMs [combatant commands].

And fourth and finally, as Eric said, we need the adoption of these technologies among our allies and partners, and promote AI interoperability.

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

Mr. LANGEVIN. Thank you, Secretary Work. Greatly appreciate your contributions and efforts on this extraordinary report and effort. Thank you.

We'll now receive testimony from the Honorable Mignon Clyburn. Commissioner Clyburn spent 9 years on the Federal Communications Commission where she worked to close the digital divide.

She has a distinguished career fighting for diversity in the communications sector, and I welcome her back to share more of her thoughts on workforce and ethics from the Commission.

Commissioner Clyburn, you are now recognized to summarize your testimony for 5 minutes.

**STATEMENT OF HON. MIGNON CLYBURN, COMMISSIONER, NA-
TIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLI-
GENCE**

Ms. CLYBURN. Thank you very much.

Chairman Langevin, Ranking Member Stefanik—sorry, Stefanik.
Stefanik. We're friends.

[Laughter.]

Ms. CLYBURN. Chairman Lynch, Ranking Member Grothman—
I'm having a tongue-tied morning—and members of the committee,
thank you for the opportunity to appear before you to highlight the
Commission's workforce recommendations.

But first, I would like to thank the members of the committee,
particularly Chairman Langevin and Ranking Member Stefanik,
for your leadership and for advancing many of the Commission's
recommendations in this area.

Each time my fellow commissioners discussed the workforce, we
arrived at the same conclusions. The military needs to have exper-
tise both in and out of uniform or it will be unable to build the sys-
tems to perform the task described in our report, and the DOD is
unlikely to develop expertise quickly enough on its own.

As a result, if the Department of Defense is going to become AI-
ready, especially by 2025, as we have recommended, congressional
action will be needed.

Allow me to briefly describe four high priority recommendations
in the report.

First, and most critical for the AI workforce, is the need for mili-
tary and civilian career fields in software development, data
science, and artificial intelligence. The inability of military digital
subject matter experts to spend their careers working in digital
fields is, arguably, the single most important issue impeding mod-
ernization.

Without this career path, DOD will continue to struggle to re-
cruit new talent, identify talent, and retain the talent it already
has. I should note that many of the military and civilian experts
we spoke with when the Commission started have since left gov-
ernment service because they were unable to continue working on
AI.

We must stop bleeding talent. This is a well-known problem with
a relatively straightforward solution. Unfortunately, we have not
seen enough progress and it is time for us to take concrete steps
to address the hemorrhaging when it comes to talent.

Our second priority is training junior leaders. We must funda-
mentally change how junior leaders use and interact with AI and
other information-processing agents. Junior leaders must not only
understand how to team with machines, but learn when to trust
machine outputs.

We recommend the military services integrate AI topics into pre-
commissioning and entry level training for junior officers and train-
ing for both junior and senior noncommissioned officers.

Our third priority is to incentivize emerging technology literacy
among senior officers. We often speak of the need for a cultural
change in DOD. But the most effective way to change culture is to
change incentives.

Using the Goldwater-Nichols Act's incentivization of joint competency as a model, Congress should require DOD to create an emerging technology certification process in critical billets.

Service members should earn their certification by serving in noncritical emerging technology billets, fellowships with industry and academia, graduating certified courses, and earning commercial certifications.

Finally, we recommend a United States Digital Service Academy, an accredited degree-granting university. The academy would help meet the government's needs for expertise in artificial intelligence, software engineering, electrical engineering, computational biology, and several other areas.

Students would attend the school tuition free and receive a highly technical education. Graduates would then enter the government as civil servants with a 5-year service obligation.

Our staff will be available to work with you on further details of each recommendation. But for your convenience and consideration, we have produced a draft—we have produced draft legislative language for your review.

Thank you again for the opportunity to appear before you and I look forward to any questions you may have.

Mr. LANGEVIN. Thank you very much, Commission Clyburn. We appreciate your testimony today and what you had to say.

And, lastly, we'll receive testimony from Mr. Gilman Louie. Mr. Louie is a co-founder and partner of Alsop Louie Partners, an early-stage technology venture capital firm, and he was the very first CEO of In-Q-Tel, the venture capital firm established with the backing of the Central Intelligence Agency.

I welcome him now to share his insights from the Commission on technological advantages, global cooperation, and threat analysis.

Commissioner Louie, you are now recognized to summarize your testimony for 5 minutes.

STATEMENT OF HON. GILMAN LOUIE, COMMISSIONER, NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

Mr. LOUIE. Thank you very much.

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

Our report took a broad view of national security to compass economic competitiveness, as Eric has noted, as well as defense, as Bob has discussed, and wanted to focus on a series of cross-cutting national security problems related to AI that needs urgent attention.

What these have in common is that our adversaries are aiming to take advantage of the free and open nature of our society.

First, our society's digital dependency leaves us vulnerable to emerging AI-enabled threats. For example, adversaries are using AI to enhance disinformation campaigns and cyber attacks.

They're also harvesting data on Americans to build profiles of their beliefs, behavior, and biological makeup to be used for tailored attempts to manipulate or coerce individuals.

This is a gathering storm of foreign influence and interference, and requires organizational and policy reforms to bolster our resilience.

You should stand up a task force and 24/7 operation center to confront digital disinformation. The government needs to better secure its own databases and prioritize data security and foreign investment screening, supply chain risk management, and national data protection legislation.

We need AI-enabled cyber defenses to protect against AI-enabled cyber attacks. And as the pandemic has made clear, biosecurity must become a top tier priority in national security policy.

Second, competitors are making every effort to steal our technology, research, and intellectual property. As the margin of U.S. technological advantages narrows and foreign efforts to acquire American know-how increases, we need to examine how to best protect our ideas, universities, labs, and companies without unduly hindering innovation.

We need to modernize export controls and foreign investments screening to better protect dual-use technologies like AI. We need to protect U.S. research institutions as national assets. They need tools and resources to assess risks and share information as well as cybersecurity support, and we need to elevate intellectual property [IP] policy reforms as a national security priority in light of China's effort to leverage and exploit IP policies to its own advantage.

Finally, to protect our country in all these areas, we need to better—have better intelligence. The report makes significant judgments that intelligence will benefit from AI more than any other national security mission. The intelligence community should integrate AI across all aspects of its work, from collection to analysis.

We need to empower science and technology leaders in the IC [intelligence community]. We need to leverage open source information, and we need new approaches to intelligence fusion and human-machine teaming to develop better insights and augment human judgment.

Let me close by saying that just as AI is posed [to] impact all sectors of society, it also poses to impact all dimensions of national security.

I urge Congress to review the full range of national security problems addressed in this report and adopt our recommendations to address them.

Thank you, and I look forward to your questions.

Mr. LANGEVIN. Thank you, Commissioner Louie. I deeply appreciate you lending your expertise and efforts to this Commission, and thank you for your testimony today.

We'll now turn to member questions, and we'll recognize members for 5 minutes. I'll begin by recognizing myself for 5 minutes.

Dr. Schmidt and Mr. Louie, are there better ways that DOD could leverage industry and academia to field the AI systems more quickly than going through the normal acquisition pipeline?

Will the software acquisition pathway, by way of example, provided in the FY [fiscal year] 2020 NDAA and the Budget Activity 8 software budgeting pilots help DOD's efforts?

Dr. SCHMIDT. Thank you, Mr. Chairman.

The pathway that you all provided is helpful but is not sufficient, and the cultural aspect of training people to treat software differently has taken—has been harder and taken longer than I thought.

I do know many, many software companies who want to work with the government and, in particular, the DOD, and they cannot find a corresponding customer or user or buyer or someone who can work with them.

My own view is that the DOD should set up some kind of technology insertion program where they, literally, go and try to get this stuff in because it's so strategic and so important to the mission of the DOD.

Gilman.

Mr. LOUIE. Thank you, Dr. Schmidt.

Software and AI are joined at the hip, and until the Department is able to acquire software as software, not as hardware, not in the form of block upgrades, but as consumed as a field that fuels our system.

We have a saying that we did back who worked—many of us who worked on SWAP [Software Acquisition and Practices] report. We said software is something that never ends. It's a continual process. But all of our acquisitions are designed for building big systems in these kind of monolithic upgrades.

Our adversaries are not doing that. For us to be competitive and for us to have the best software as it's happening, we need to reform on how we do it.

A single color of money is a start, but it's only a start. The culture needs to change. We need professionals who know how to acquire software, and understands the basic underpinnings of AI.

Mr. LANGEVIN. Very good. Thank you, Dr. Louie.

If I could continue with you, Dr. Louie—Commissioner Louie. We're all aware that China views talent as central to its technological advancement. The Commission addressed many recommendations towards the U.S.'s need to attract and retain the best foreign talent to study, live, and work in the United States. Can you speak to why this is so important to our national security and how others will capitalize on our policies if we do not find a way to keep the best talent here?

Mr. LOUIE. Sure.

First of all, China realizes it has a major disadvantage when it comes to attracting talent. Talent comes to democracies where good ideas flourish and individuals can chase their own pursuits in order to improve research and development.

In doing so, we must not give away that advantage. We attract the best and the brightest from all over the world for the past 50 years. It's a fundamental U.S. advantage. The Chinese realize that they cannot compete with our top 1 percent when it comes to AI.

Their strategy is to use their talents to apply what we discover. That discovery capability lies in our ability to work not only in our universities and research labs from individuals both from here domestically and from all over the world, but to share those ideas in the open and shared platform called Open Science.

China is not an open society. It does not believe in open science. We do. Please don't give up that advantage.

Mr. LANGEVIN. Yeah. Well said, Commissioner Louie.

Finally, Dr. Schmidt, of all your recommendations that focus on the Department of Defense and its adoption of AI, what do you believe are the Commission's most consequential recommendations that Congress has not yet acted upon?

Dr. SCHMIDT. There are many—and Commissioner Work can probably add here—there are many aspects of the recommendations around talent that have not been adopted, in particular, retaining specialized talent.

And the other issue has to do with the regulatory structure. As you highlighted in your earlier comment, the regulations are, essentially, antithetical to prioritizing AI.

They're built around large weapon systems of a hardware kind, and the real strength of our Nation will come from the strength of our software and AI activities.

Mr. LANGEVIN. Commissioner Work, did you have anything to add, Mr. Secretary?

Secretary WORK. Sir, I'll just say that there's three general areas. I don't have a single answer. So with your forbearance, I'll give you three.

The first is under leadership and strategy. We think that tri-chair steering committee is absolutely central to provide the top-down leadership and push for the integration of AI throughout the force. And having the JROC as the co-chair—excuse me, having the Under Secretary of Defense for R&E as the co-chair for the JROC will make sure the technology and capabilities and requirements are absolutely synced up.

Under enabling the resources, processing, and organizational constructs, getting that common digital infrastructure, which means secure cloud, we hope we can get to a secure cloud for the Department.

But having the algorithmic libraries, et cetera, and having JAIC established as the AI accelerator is probably the most important thing at the applications level. And then under accelerated adoption, it's trying to get these teams out to the field, out to the COCOMs.

Dr. Schmidt and I visited SOCOM [U.S. Special Operations Command], for example, and what they're doing down there, where the combatant commander himself has taken this as a personal mission and established the talent and team to push it, has really seen some remarkable advances in special operations capabilities.

We need to have those type—same type of teams and approaches in the Indo-Pacific Command and European Command. So thinking of it in terms of leadership, enabling resources and processes, and accelerating adoption would be the three things that I would say are the most consequential.

Mr. LANGEVIN. Thank you, Secretary Work, and thank you all for your answers.

With that, Ranking Member Stefanik is now recognized for 5 minutes.

Ms. STEFANIK. Thank you, Chairman Langevin.

An idea that each witness and each commissioner has highlighted today, as well as the chair of the Oversight and Government Reform Committee, is this bipartisan proposal for a Digital

Service Academy and how the issue of workforce and talent is going to make or break whether the United States is able to lead in AI.

So my question is for Chairman Schmidt. Can you expand upon this recommendation to include how such an academy should be established? And then I also want to hear what have been the impediments to this recommendation.

Dr. SCHMIDT. If it's okay, I prefer that Commissioner Clyburn answer.

Ms. STEFANIK. Great.

Ms. CLYBURN. Thank you, again, very much.

The need is very clear. We have a clogged pipeline, and so the Commission was very bold in its recommendation. It recognizes that there are a number of impediments.

Many of them are economic, and so what we attempted to do here was to identify what could be a platform that would be targeted when it comes to STEM education, be unapologetic about educating to meet the needs that we have in government from a civilian point of view, and this academy is a part of the solution.

Some of the things that I have heard that have been maybe a little less embracing is what does it mean in terms of the other service academies. You know, do we need another institution? How expensive will it be? How long will it be to onboard?

It is not going to be inexpensive. It will take up to 7 years to graduate the first class. But what I will say is we—that pipeline problem that I recommend—that I mentioned, everyone knows that it's there.

We need to be big, bold, and targeted and intentional, and this is one way we thought it was unwaveringly, you know, obvious that we were serious about addressing the pipeline deficit.

Ms. STEFANIK. Thank you, Ms.——

Dr. SCHMIDT. May I—may I——

Ms. STEFANIK. Oh, sure. Go ahead, Eric.

Dr. SCHMIDT. Yeah, let me just—let me add that a number of universities have offered to help us get this set up if the legislation proceeds as we've described, and it should ultimately be very good economically because of the payback requirement. If you graduate, you have to work for the government for 5 years.

We strongly endorse this idea.

Ms. STEFANIK. Well, I appreciate that. I think this is going to be one of the most important ways and important strategies that we need to work on a bipartisan basis to embrace in order to make sure that we maintain a competitive edge.

And my other question is on the timeline issue related to workforce and talent.

Commissioner Clyburn, you talked about the 7-year time periods to even graduate students from a Digital Service Academy. But yet the report talks about this 2025 timeline in order for the—for the United States to maintain that edge against China.

Are there any steps we can take now to address this talent deficit before 2025 or before that 7-year period with the Digital Service Academy, and if yes, what are those steps?

Ms. CLYBURN. Yes, ma'am. Thank you for that, and forgive me for struggling with your name. We say a lot of long A's and long E's so forgive me. I'm from South Carolina.

Ms. STEFANIK. It's okay.

Ms. CLYBURN. So one of the things that we recommend is an agency-specific digital corps, and this would be modeled after the Army's Medical Corps. And this would allow for specialized personnel and policies and guidelines for promotion.

One of the issues, when I mentioned those who have left government, is there was no way to stay on an AI track and to get promoted and for us to benefit from that. The National Reserve Digital Corps, again, another civilian track, you know, modeled after the other, you know, reservist opportunities.

We can quickly get those committed and on board to offer 38— at least 38 days a year for service. They could triage. They could help. They could assist and they could augment.

The scholarship—we have, you know, scholarship service, you know, programs that we need to expand and we need to expand the cyber—well, again, the cyber corps for civilian—excuse me, scholarship service.

That would be NSF [National Science Foundation] managed. That would allow those who qualified to work in an agency. There are some things that we can do right now that will ensure a pipeline while we wait for that first graduating class.

Ms. STEFANIK. Great. Thank you so much, Commissioner Clyburn. Thank you, Chairman Schmidt, and all the commissioners for your emphasis on the workforce challenge.

Yield back.

Mr. LANGEVIN. Thank you, Ranking Member Stefanik.

The chair now recognizes Chairman Lynch.

Dr. SCHMIDT. Chairman Work wanted to make a comment.

Mr. LANGEVIN. Oh.

Mr. LYNCH. Thank you, Mr. Chairman.

First of all, I want to thank the panel for all of your work. First of all, coming here today in person, I think, speaks to the urgency of the issue, and we appreciate that.

And also, we're thankful for this report. You know, normally in Congress when we see a 750-page document, we assume that it was compiled for the purpose of defending itself against the risk of being read.

But I'm happy to say that your document is an exception. And I want to just point out to my colleagues and staff that in Appendix D, so not only did it make recommendations about what might be done to address the problem, but it also includes draft legislation in rudimentary form to really—so it's all worked out, pretty much.

It can be refined a bit. But it's a head start on a lot of the work that we are engaged in here at the Capitol, and I appreciate your work.

I do want to follow up on Ms. Stefanik's inquiry regarding several of you have talked about the dearth of talent, and the fact that we have got to get more young people into the pipeline.

I am a co-sponsor of Ms. Trahan's bill for the academy. But, you know, I've had a similar problem in my own district. I represent a big part of Boston. A lot of the jobs in my area that are being

created were really heavily reliant on a math and science background, and in the traditional public schools we weren't getting that.

So I actually founded a charter school that triples the amount of math and science that the kids would have gotten had they gone to the traditional public schools.

So—and there are a lot of schools around the country that are doing this, both traditional public schools and charter schools.

Is there a way that we might be able to incentivize that type of activity? Because we have got to not just think about people who might serve in government tomorrow, literally, but also increasing that or animating that pursuit around issues like cyber, artificial intelligence, you know, so many other areas that are coming at us at a pace that is unprecedented.

The velocity of change is breathtaking in terms of what we're grasping, you know, both in Congress, but also in our society. Is there a way that we might incentivize that learning at a much lower level than we're talking about for this academy?

Ms. CLYBURN. Yes, sir, I believe we can. I think we need to just demystify what STEM is or what STEAM [science, technology, engineering, the arts, and mathematics] is. When people hear about that they think it's for a certain segment of the community. They don't recognize that if a young person creates any type of product, a designer that creates lipstick, that's science.

And so what we need to do, I think, a better job of messaging is saying, this is what it is. It is a part of your everyday—you know, your everyday culture. This is science. This is engineering.

And we need to help our teachers become better facilitators and supportive, and we really need to recognize some of the existing cultural barriers when it comes to especially women and underrepresented groups.

So afterschool programs, that's important. NSF has, you know, programs. We need an all-of-the-above approach in order to erase some of the challenges that you see, and kudos to you for starting the charter school with that focus.

Mr. LYNCH. Mr. Chairman, we're about to consider several immigration bills in Congress. We have already begun debate about that. They're being put together.

Is there an opportunity for us to use the visa program and that immigration bill as a way of getting talent? I see that Canada does a very good job at this. There's actually a little tension between the Chinese government and the Canadian government because Canada has been so successful in recruiting some really top-line talent from China and Asia.

You know, I tend to think we should be doing the same thing, using the promise of America to attract, you know, some of the—some of the talent that would like to get to work on some of the issues that we have in the country.

Is there a way to do that through our upcoming immigration debate?

Dr. SCHMIDT. There's no question that the United States will be stronger if we encourage high-skills immigration. In the last administration, mostly what would happen is that the visas would be very difficult to get and that companies would park employees in

places like Canada, Vancouver, and so forth, waiting for the H–1B lottery.

This is not in America's interest. So everything that we can do to get high-skills immigration into the right places is welcome.

The argument is relatively simple. If we don't welcome them, they will create companies and efforts in countries that may ultimately not consistent with our best interest.

The other obvious point is once we let them in the country or once we educate them in the country, we need to give them some way of staying in the country, consistent with the law and their good behavior.

It's stupid, frankly, if I may say that, to fully educate a brilliant quantum physicist and then send him to China where he creates a quantum physics program that competes with our military activities, which, indeed, is what we did.

Gilman, you may have something to add here.

Mr. LOUIE. Thank you, Dr. Schmidt.

We had some very specific recommendations in our report.

First, we should expand our O/M/J visa programs. We have many talented individuals who want to stay in the United States, but they don't do it through the classical means of having published reports and things of that nature. For that, that's terrific.

But AI is moving so rapidly, we need to open our aperture on who should be eligible for that class of visa.

Second, we want entrepreneurs, entrepreneurs who come to the United States, create jobs for Americans, and we should develop and expand that lane for individuals, particularly in these areas of high competitions in science and technology. We want those entrepreneurs. We want them to create jobs here and build great American businesses.

And finally, we made a recommendation. With the appropriate screening in place, we believe that anybody receiving a doctorate degree in the science and technology area or areas of critical requirements should be granted a visa.

We want these individuals to stay, not go back and develop competing capabilities elsewhere.

Mr. LYNCH. Mr. Chairman, thank you.

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

Yes?

Secretary WORK. I was just going to say, and this goes back to a Ranking Member Stefanik's question, you know, we looked at this as a—we wanted to exploit our homegrown talent. We wanted to attract worldwide talent. And we wanted to ID [identify] and use the talent we have on hand.

So exploiting homegrown talent, Commissioner Clyburn continually just said, look, we have got a lot of people who want to get into STEM. They don't have the opportunity to do it because they can't afford to go to college.

So the national research—the National Digital Corps—National Reserve Digital Corps was designed to do just that. It's like the NROTC [Naval Reserve Officers' Training Corps] program or the ROTC [Reserve Officers' Training Corps] program.

Anybody can apply. They'd get a full ride, and when they graduate, they would owe—they would—38 days a year like a National

Guardsman or someone in the National Guard where 2 days out of every month, they would come into a unit and say, how can AI or these advanced technologies help you accomplish your mission better. I'm here to help you do that. And then 2 weeks out of the year, they'd go to a military exercise and say, geez, if you just implied machine learning in this particular application, you're going to be 15 times more effective.

And so that was really trying to attract homegrown talent. The National Digital Academy is designed to get people into the government for a long period of time so we can exploit them.

Attracting the worldwide talent, Commissioner Louie and Commissioner Clyburn have already talked about this. But the third thing I wanted to say, which we haven't talked, is, there's a lot of talent in the Department of Defense right now. These young men and women, many of them are great coders. All they want to do is have an opportunity to get on a software development team and they will rock the world.

So many of the suggestions we have is how do you identify those people? Give them a classifier that we can follow and assign, and that's how we're confident we could get to 2025 before we're getting 700 graduates from the Digital Academy. So we took it from a holistic view, Mr. Chairman.

Mr. LANGEVIN. Thank you for that.

Mr. LYNCH. Mr. Chairman, I yield back.

Mr. LANGEVIN. Thank you, Chairman Lynch.

Mr. Grothman—Ranking Member Grothman is now recognized 5 minutes.

Mr. GROTHMAN. Sure, a few questions.

There's nothing—I didn't anticipate the debate here would wind up over immigration. But it's an interesting topic. Do you think we should have some sort of math and science tests as we decide who's going to be able to immigrate in this country?

Mr. LANGEVIN. I don't think your microphone is on.

Mr. LOUIE. I think math and science is critical. I think, particularly in our recommendations for the doctorate lane, clearly, S&T should be one of the testing variables that we should be looking at.

That's the talent that we need in this country and we should be very explicit to the rest of the world. If you want to come to the United States and use your talents and use it well here, we welcome you.

Mr. GROTHMAN. Absolutely. When I talk to immigrants in my area, they sometimes complain that the smartest people are going to Australia, New Zealand, Canada, and we're getting the ones who aren't. So if the chairman wants to put a math and science requirement in immigration, it's something to look at.

Now, we talk about ways and the government getting more involved in AI. Are there areas of the government that you think will be able to be cut as we improve in artificial intelligence, since presumably, it will, you know, improve a variety of things? I feel sorry; all of a sudden now Chairman Schmidt had to put a mask on. It was great seeing you without the mask.

Dr. SCHMIDT. I'm trying to follow the rules.

Bob, do you want to answer the government question?

Secretary WORK. Well, I—you've sent shivers down my spine because now I'm going back to my time as the Deputy Secretary, and every time a question like this came up, I would always hate to answer it.

But, generally, we know that AI is going to have a tremendous impact on all the back office processes in the Department of Defense and the Federal Government, and it will become more efficient and you will require fewer people to do the work.

So I would expect this to have some reduction in the overall Federal workforce as AI is completely implemented across the government and in the Department of Defense.

Mr. GROTHMAN. Do you think it would be a good idea to have targets right now? Because you know what happens. Nobody ever wants to cut the government.

And I agree with you. Hypothetically, one of the benefits of artificial intelligence is that it should make things more streamlined and reduce the number of positions.

But people around here don't like to do that and that's what I'm trying to ask you right now so we know in advance when we're putting together the budget in 2028 where we can expect to have reductions in personnel.

Dr. SCHMIDT. I think it's reasonable to expect that some of the overhead functions will be smaller and that the specialized functions will be larger, and the easiest way to achieve that would be not to do what you're describing, but instead, put some guidance on the kind of people that are being hired now because the hiring pipeline takes a while.

So the government loses, you know, 10 percent of the employees a year and it's hiring 10 percent new, some number like that. You all would know the exact number. You could establish a threshold that among the new hires that occur every year, a certain percentage of them have to meet a science and technology type threshold, a specialized threshold, and that would achieve your objective without having to go through the fighting over budgets argument.

We're really focused on the people, not the money, because the people will drive everything else.

Mr. LOUIE. I also think that the other part of the equation here is increasing the productivity of our people. Look, our adversaries are not holding back. You know, China has already set out its goals: to compete with the U.S. in AI by 2025—underneath "Made in China 2025"—to surpass the U.S. capabilities by 2030, and to win in any domain anywhere in the world in any kind of a hostile action by 2049.

The issue is not so much the savings but where do we deploy our talent? Where do we put them in places where they are going to be the most productive and how are we going to compete with an adversary who's committed its entire nation to win in the fourth industrial revolution?

We need to meet that challenge head on. We need to deploy our personnel, educate them, and skill them to be able to fight in this next arms race.

Mr. GROTHMAN. What majors right now in American colleges, to you if you're going to major in that, signals that you would be good in the AI field?

Mr. LOUIE. Mathematics, clearly. Statistics, for example, is something that we should be teaching in our high schools because it's critical to the way we're thinking.

Second, even if you're in non-S&T areas, understanding how AI—what you can trust it for, what you need to augment it with, what you need to question about it, is going to be critically important as well.

Ms. CLYBURN. And, sir, I would follow my niece in biomedical engineering.

Dr. SCHMIDT. And let me add that there is good news here. Universities of the United States are generally seeing a huge supply of computer science graduates and majors, and in virtually every university I've studied, computer science is now the number one major ahead of, for example, economics, which is sort of a big surprise.

That workforce is coming into the private sector. It's not coming into the government sector the way it should be. Because in the private sector, they get to work on this stuff. For the government, they have to do this billet and that billet and so forth.

When I was running the DIB [Defense Innovation Board], we met a brilliant—we were doing a Russia review in the National Security Council—this brilliant young man who was busy doing cyber attack analysis, and I asked what was his career path. He said, next week I'm being transferred to a nontechnical position in another part of my rotation. That's insane, and that's how the government works. We need to address those issues, and those are covered in our report.

Mr. GROTHMAN. Thank you for giving me additional time.

Mr. LANGEVIN. Thank you, Ranking Member Grothman.

Mr. Larsen is now recognized for 5 minutes.

Mr. LARSEN. Over here. Thank you, Mr. Chairman, for recognizing me.

Twenty years ago when I came to Congress, I don't think I would ever predicted 20 years later I would have said, I'm really excited to read a report on AI. But I am, and two particular sections or pages, I'm real excited about pages 77 and 78 and about 297 through about 300. Those are the education bits, and I'll get the—Mr. Work, I'll let you know. You don't have to read it.

But on that, a few years back we included in the NDAA direction to the JAIC to develop an AI education strategy, which they are beginning to roll out. My vision of it is to go as deep as possible with as many folks—if I could just ask the guys on the clock, they didn't reset the time.

Sorry about that. Yeah.

I think every woman and man in uniform and civilian in the DOD should have some basic AI education. They don't have to be coders. They don't have to be the ones leading the project, but have some basic education, which is why page 77 is interesting. I'm excited about having an AI-ready DOD by 2025 or warfighters are enabled with baseline digital literacy and so on.

And then getting to pages 297 to 300, implementing that even more. So I want to start with you, Commissioner Clyburn. What exactly, you know, is your vision within the DOD on AI education? Again, not everyone needs to be a coder. Not everyone needs to be

writing the software. But my idea is that they should at least understand the weapon they're using, whether it's an electronic or a software weapon, a hardware weapon, the weapon someone else is using against us.

What's the—what was the vision of the Commission when you came up with these recommendations?

Microphone.

Ms. CLYBURN. It was a recognition that the next major conflict will likely not be on the ground. But it will be AI-inspired. And so you're right, from headquarters to the tactical edge is how we phrase it and I really embrace that.

We have to be AI-ready. We have to be AI-trained. Those who protect us should have that digital foundation. Those who excel in computational thinking within the ranks, they should be identified and supported.

It's a shame that we're losing all that talent, and they should be able to advance. You know, those who are employ—we need upskilling within the ranks. Junior officers from the beginning need to be trained in AI concepts and they need to continually be educated and certified.

So we can't stand still. We cannot ignore the fact that, again, we are in an AI—we might not recognize it, but we are in a AI revolution and we need to be prepared.

Mr. LARSEN. Did you look at the JAIC's current work done on this education strategy with these recommendations?

Ms. CLYBURN. Yes, we did, and I will yield the rest of my time to Mr. Work.

Mr. LARSEN. Yeah, I was going to ask him. Good.

Secretary WORK. Well, I'd just like to start, sir. Andrew Moore—Dr. Andrew Moore, formerly of Carnegie Mellon, now at Google, is one of our commissioners who leads line of effort one, which is the research and development line of effort.

And I remember quite clearly the first time he was talking to us and he said, look, you can get a lot accomplished with young men and women who aren't a computer science graduate.

What they have to have is understanding of is computational thinking, and that had a big impact on the way we were thinking of this because he made the case that there's a lot of innate talent in the force, we just have to identify those people.

He recommended, for example, if we gave just one class, like, at the 7th grade, and another class in the 11th grade on computational thinking, that you would have people who graduate who would be immediately able to step onto a COCOM development team.

So this led us to say we ought to add a section on computational thinking in the Armed Forces—the ASVAB, the Armed Services Vocational Aptitude Battery—and identify those folks so that we could do it.

So computational thinking is as important for the whole force as the hardcore Ph.D.s who would go into dedicated R&D billets. So that would be one thing that I would say we all need to think about how we would do that, and we recommend a new National Defense Education Act II, and I would recommend that Congress think about, you know, should there be computational thinking

type requirements that we establish to allow the entire workforce that's going into the government and into commercial sector, academia, et cetera, to expand these things.

I'd also like to go back to one of the things on——

Mr. LARSEN. If I—if I could, I wanted to go to Mr. Schmidt.

Secretary WORK. I'm sorry, sir.

Mr. LARSEN. The—I'll be really quick with a question. We talked in the past about China's declarative policy to want to lead by 2030 in AI, and so why don't we just have a declarative policy we're going to lead by 2029 and just go do it.

We have no idea how China is going to do it. They're just going to say they're going to do it. And, frankly, whether or not they're successful they would probably say they are leading, in my view.

Why don't we just have a declarative policy we're going to lead in AI? Does being AI-ready by 2025 in the DOD, as you state in your report, does that equate with the general U.S. leadership if we do the things in this report?

Mr. LANGEVIN. If you can answer briefly.

Dr. SCHMIDT. It's a component but not sufficient. We actually call for a technology competitive council to cover not just AI but some of the other key areas. It's crucial that the United States have a national plan for competitiveness globally that addresses AI, semiconductors, synthetic bio, and a few others, energy, et cetera.

Mr. LARSEN. Yeah. Thank you.

Thank you, Mr. Chairman, for your indulgence. Thank you.

Mr. LANGEVIN. Thank you, Mr. Larsen.

The ranking member of the full committee, Mr. Rogers, is now recognized.

Mr. ROGERS. Thank you, Mr. Chairman. Can you hear me?

Mr. LANGEVIN. Yes, I can.

Mr. ROGERS. Great.

Dr. Schmidt, just to follow up on Mr. Larsen's question, is China leading in AI?

Dr. SCHMIDT. We spent a lot of time looking at this question, and, in general, we are a little bit ahead but not very much. They have more people coming. We're doing better in algorithms, but they're coming.

They are doing better in some industries, in particular, in financial transactions, electronic commerce, and surveillance. We're doing better in some other areas of research. It's a close race.

At the moment we're ahead. Our report specifically says that we can lose our lead within a few years.

Mr. ROGERS. Well, I share Mr. Larsen and Mr. Lynch's observation. This Commission did some great work. This report is not just going to sit on a shelf. We're going to do some stuff here that's really meaningful. So I want to commend all of you and thank you for your time in putting this together because it's going to make a difference.

Commissioner Clyburn, I wanted to follow up on Ranking Members Stefanik's questions about how we can get folks into these jobs earlier than the 7-year timeline it would take to graduate our first class.

Are there some scholarship opportunities that we can provide people now to go to an existing university? We have got some fine

existing universities in this country right now that can get some people trained earlier while we're standing up the Digital Service Academy and getting the first few people through there.

Ms. CLYBURN. So we talk about the Reserve Officer Training Corps. We talk about expanding that CyberCorps Scholarship for Service program that is—that it is in place.

So, yes, sir, and there are some things that—outside of that that I think are possible. So being targeted and sending the signal. If you were to highlight just the two or three things that I mentioned, I think that will encourage others to follow.

So it's that down payment that we should make with the existing programs and others modeled after successful programs that I think will make a difference and enable us to move in the right direction.

Mr. LOUIE. Let me also add that not every field requires the degree.

Mr. ROGERS. Exactly.

Mr. LOUIE. We have a great—we have a great enlisted force. I mean, amazing. These kids know all about AI. How do I know that? They're playing it on their video games.

Mr. ROGERS. Yes.

Mr. LOUIE. What they're missing is the linkage between what they're seeing in those games and what they're seeing in their Department of Defense.

Mr. ROGERS. Yes.

Mr. LOUIE. So with the appropriate certification and badging program, we could also get our enlisted teams up and ready and AI-certified and ready.

Dr. SCHMIDT. And imagine——

Mr. ROGERS. Yeah, and that's what I was getting at, too.

Dr. SCHMIDT. Sir, imagine if you had a call for talent where there was some kind of a test and a competition. I think all of the commissioners would say to you you're going to be really pleasantly surprised by the existing talent in the government that's not correctly being used.

Mr. ROGERS. Yeah, and I agree, and that's one of the things I was hoping is that, you know, when we have this structure, set up this Digital Service Academy, that it's not just focused on getting people a BA [bachelor of arts] or an MS [master of science] or Ph.D., that there are—other folks can get certified that can go ahead and get in the workforce right away.

And I'm also hopeful—you know, I first talked about this concept with Dr. Schmidt about a year ago and very excited about it. I'm curious to know, do you envision this being a purely public sector entity that we stand up or is it going to be a public-private partnership? How do you think it would be structured? And also, I would ask this. You know, obviously, this committee is concerned with the Defense Department making sure we can defend ourselves with these technologies and this skilled workforce.

But as you know, the Department of Homeland Security, the Department of Treasury—there are other government agencies that have the same shortfall in cyber and digital employees. Can you see this [inaudible] as one day being opened up to other agencies within the Federal Government?

Dr. SCHMIDT. We foresee it immediately being available for all of the Federal activities, and my—I always prefer public partner or public partner—public-private partnership, excuse me—PPP—for the reasons that I think that's when America is strongest.

Mr. ROGERS. Great. Commissioner——

Ms. CLYBURN. Sir, if you'll allow me a quick——

Mr. ROGERS. Yes, go ahead.

Ms. CLYBURN. I'm sorry. If you'll allow me a quick bite at the apple. I could not go back home without affirming that the 2-year colleges offer substantial support and opportunities, and they don't just offer 2-year degrees. They offer other certifications that will enable this, too. So I couldn't go back home without mentioning that.

Mr. ROGERS. Well, I'm glad you did because that's exactly what I was thinking about. It's a resource that we definitely need to be tapping into because it would help fill a need that we have got.

Commissioner Louie, do you believe the private sector even wants to work with the Department of Defense or the government on these kind of national security issues involving AI and cyber?

Mr. LOUIE. I had the fortunate opportunity of standing up In-Q-Tel, and there were a lot of people betting against it. They asked the question, why would a young entrepreneur walk across Sand Hill Road and ring the doorbell for In-Q-Tel or a Federal intelligence agency?

Turns out that there are plenty of Americans who want to serve and put their technologies in a way that protects this country. There are some, of course, who will opt out, and that's the American way.

We're not China, right. We can't—we do not compel companies and individuals to work for the government or give up their information. That sets us different—in a different and better place than, I think, our competitors. So——

Mr. ROGERS. Great. Thank you, Mr. Chair.

Mr. LANGEVIN. Very good. Thank you, Ranking Member, for your questions.

And chair now recognizes Mr. Welch for 5 minutes.

Mr. WELCH. Thank you very much. We really appreciate this hearing and the work of the Commission.

One of the frustrations that I'm experiencing in listening to this is that there appears to be a consensus—a bipartisan consensus on the absolute urgency of following through on the recommendations that you make.

Yet, on a practical level, there's impediments from us doing it. Some are bureaucratic and, to some extent, potentially congressional.

And I'll start with you, Dr. Schmidt. You do mention it's the people who are the most important. But if they're in a structure where the mission that they're doing is about overcoming obstacles that hasn't integrated that mission into its stated policy, how do we overcome that?

Dr. SCHMIDT. Part of our recommendations, as Chairman Work recommended earlier, is to take the AI efforts and cause them to report higher inside the military, and in the military, because it's

very hierarchical, having AI be a major component of strategy at every level is one of the ways that the top-down can work.

I always favor a top-down and bottoms-up approach. So I'd like to see a DOD statement around AI that's much stronger than we currently have with the JAIC. I'd also like to have a higher reporting level, more resources, and so forth. But I'd also like to have individual control at the commander level and the COCOM level where they have flexible teams which can be used to solve important national security problems, which would include AI expertise.

You want to get both flexibility for the commanders as well as priority at the highest level.

Mr. WELCH. Mr. Work, let me go to you. Thank you for that.

What are the implications of a decision that AI is now core and existential to our defense versus supplemental and discretionary with respect to how it would affect other weapons systems?

We have—as one of the witnesses said, we have these huge platforms that have been components, major components, of our defense strategy and it appears that AI cyberwarfare is really the biggest threat.

So can you just elaborate on what would be involved in a Pentagon shift in thinking and, frankly, a congressional shift in thinking where implications would affect jobs in many members' districts?

Secretary WORK. We do not talk about this specifically in the report. But very broadly, Mr. Welch, we are shifting into an era of systems warfare. Both our adversaries—I mean, our adversaries explicitly say this, and say the way we will defeat the U.S. military is to have better operational systems, and the better to way—and the way to get there is to inject AI applications and autonomy into the system so it operates at a faster speed and can operate more effectively.

So this is a big shift in thinking, going from platform-like thinking to systems thinking, and trying to figure out how these applications improve.

And in my view, all you need to have is, you know, cross-functional teams that look at, say, our sensor group, and the cross-functional team says the biggest return on investment is to do machine learning on the sensor so that it can go through the information and just pass on the data that is required, which would make everything go faster, wouldn't clog the pipes, et cetera.

And you would have someone do the same thing for our command, control, and communications, and intelligence grids. How would we have an AI-enabled application that would help decision making?

So this is—this will literally affect every operation mission that we do, and it's going to require a different way of training our commanders and our people, a different way of educating them and a different way of training them.

Mr. WELCH. But it also requires the confidence of our defense leaders that a change in direction is not only desirable but, really, essential, that has implications on the way we're doing business now—I mean, the higher education process and political process. Care to comment in my remaining 12 seconds?

Secretary WORK. Amen, sir. It all starts with trust. As soon as we have demonstrated applications enough to where commanders trust them, then you will see an accelerated adoption. But trust is absolutely key.

Ms. CLYBURN. And education starts at the top and continues through the ranks.

Mr. WELCH. Thank you. Thank you, Commissioner. Thank you all.

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

Ms. Foxx is now recognized for 5 minutes.

Ms. FOXX. Thank you, Mr. Chairman. For some reason, when I turn on my mic, my video goes off. But there goes the video. So I hope you can hear me.

Thank you for having this hearing, and it's been very, very informative and very enlightening. And it's nice to see such bipartisan agreement.

Mr. Schmidt, I know you're most comfortable with monopolies from your days at Google, but why should we create a monopoly in 5G?

Why can one company in concert with the Department of Defense have a monopoly on 5G spectrum when having multiple facility-based competition is what made the U.S. 4G market so successful and why the app economy originated here?

Dr. SCHMIDT. Our report does not specifically suggest what you just asked me about. But let me comment in general, that we have taken a look at the 5G situation and China is perhaps 10 times ahead of us both in terms of speed as well as the number of towers.

They have planned 1.3 million towers, for example, this year in total, and it looks like the leadership that China is going to have in 5G will become a significant national security threat to the United States, partly because 5G is used in autonomy, which we discuss in our report, and also because it will create an ecosystem of applications.

Imagine if the key applications that are used 5 years from now are based on the Chinese 5G network and not on American 5G leadership. Over the last decade, we have, essentially, given up leadership in that area, having—after having done a fantastic job in 4G.

My view is that it is a national security problem that we are not leading in 5G. I'll let you all debate the specific solutions to that. I would encourage you to demand a strategy from the various players that gets us at least equal to China in terms of performance and coverage.

Ms. FOXX. Well, thank you for that. You know, it's been reported that the spectrum-sharing arrangement would constitute a boom for Alphabet and other big tech firms. This sharing scheme seems to be closer to the nationalization of our spectrum markets than anything else. To be blunt, I think all our constituents, but particularly mine and the ones I hear from, are tired of the stranglehold big tech firms have over the markets.

The unchecked power of big tech's ability to corner markets, marginalize competitors, and silence my fellow Americans cannot be tolerated any further.

With that, Congress shouldn't be empowering market mobiliza-
tion—monopolization in this critical space. Our 5G infrastructure
creates digital highways that artificial intelligence can drive on,
and this Congress should not be risking our competitive advantage
over China by investing in this untested and unproven nationaliza-
tion framework.

Doing so would put broadband development—rural broadband
projects, and even national security at risk. As I said, I believe that
there's bipartisan concern about big tech's antitrust problems.

I want to——

Dr. SCHMIDT. May I respond? May I respond, madam?

Ms. FOXX. Okay.

Dr. SCHMIDT. So in the first place, I no longer work at Alphabet,
but I have a large stock position in Alphabet. Alphabet is not one
of the beneficiaries of any of these 5G activities at the moment, and
the argument that you're making about sharing is not technically
correct. Your argument is, fundamentally, that it would be better
to have a highway occupied by one car rather than having a high-
way have lots of different cars on it.

The CBRS [Citizens Broadband Radio Service] option, which is
in the 3.5 gigahertz phase, proves that sharing works. We need to
solve our bandwidth problem. Personally, I have my own technical
views of how to solve this. But I do not want to allow your state-
ment to go unchallenged with respect to the statement that we're
okay.

We're not okay and we need a solution in this space that is com-
petitive with China.

Mr. LOUIE. Let me add, since I was one of the co-authors on the
5G report for the Defense Innovation Board, we are not in favor of
monopolies. We do not believe that one company should own it all.
I think that's, fundamentally, anti-American.

On the other side of that equation, for us to be competitive in 5G
we need to have large continuous blocks of spectrum available and
not little small segments. Think of it like this.

Think of going down the freeway in which you sell each lane to
a particular company, and you cannot change your lane once you
get on that road. Sharing, particularly in the DOD spectrum, is the
only way to allow broader use of our spectrum and protect our mili-
tary systems.

Our radars, our air-to-air, surface-to-air, our satellite comms
[communications] require sharing. Without that sharing, we will
not be competitive. The U.S. 5G is one of the slowest in the world
where our average throughputs are less than 50 megabits, com-
pared to China, which is going at 300 megabits, going to 1 gigabit.

If we want to be competitive and we want AI to drive on the in-
formation highway, we have got to free up the lane. One car a lane
is not a solution.

Mr. LANGEVIN. Very good.

Ms. FOXX. Thank you both. I want to build on something also
that Representative Rogers mentioned and——

Mr. LANGEVIN. I believe the gentlelady's time has expired, but
briefly.

Ms. Foxx. Oh. Well, I wanted to push certification, Mr. Chairman. I think we need to get alternatives to baccalaureate degrees and push certification where we can.

Thank you for indulging me.

Mr. Langevin. Certainly. I thank the gentlelady for her line of questions.

Mr. Khanna is now recognized for 5 minutes.

Mr. Khanna. Thank you, Chairman Langevin, and thank you to Dr. Schmidt and particularly Commissioner Clyburn, and all the commissioners for your excellent work.

Before I get to my question, I do have to address what probably should be the headline of this hearing, Representative Grothman's comments that somehow that the smartest immigrants are going to Australia and New Zealand and we're not getting the smartest immigrants.

I have a number of comments, but I guess I just for educational purposes, maybe Dr. Schmidt, could you comment on the intelligence of Sergey Brin and Satya Nadella and Eric Yuan? I don't see Australia and New Zealand having produced all these tech companies. And what—how would you characterize the, quote/unquote, "intelligence" of immigrants coming to the United States?

Dr. Schmidt. America has benefitted enormously from high-skills immigration. I have personally been the beneficiary as the companies that I have been working for were founded by such people, and they're incredibly brilliant.

We need them to drive our tech sector. We need to create wealth in our stock market. We need them to pay—help pay the taxes for our government. I can go on and on about the quality of immigration.

At one point, I was sitting at Google and I realized half people in the senior executives were immigrants, many them from South, Southern Asia.

Mr. Khanna. You know, the other thing that I think I understood Congressman Grothman to be saying is that we should have some kind of a math and science requirement for immigrants.

I think the American public would love to have a math and science requirement for Members of Congress. I think that would probably be a better start. I would challenge Congressman Grothman.

Maybe you and I can take a math and science test and ask all of our immigrants also take a hypothetical test, and my guess is I wouldn't be surprised what the results are. I hope you'll take me up on that.

But what do the commissioners think of the idea of having a math or science test for immigrants? I don't understand.

Did Madison or Jefferson put that in the Constitution that we should have math scores for who should let in—we should let into this country? Would any of the commissioners please comment on that statement?

Mr. Louie. I'm happy to answer at least part of it. The particular line of questioning around having science and technology skills for our recommended visas for anybody with a degree in S&T is pretty straightforward.

I don't think any of us are advocating that we should have a generic test like the way you have to pass the other immigration examination on American citizenship or any other kinds of activities.

But we need science and technology skills and that is clear. We are not going to be competitive without that talent. We need to grow them internally, we need to get them from outside, and we need to encourage people who are educated in this country of our very best universities, both public and private, to allow them to practice their knowledge in the United States and not abroad.

Mr. KHANNA. Personally, I agree with that. But just to be clear, you, clearly, disagree with Representative Grothman's suggestion that somehow we should have a math or science requirement for our immigrants.

Mr. LOUIE. I don't believe that was the question I was answering.

Mr. KHANNA. I'm saying you would disagree with his statement on that, correct, and the Commission would? I don't think anyone in America, a reasonable person, thinks we should have requirements for immigrants to take math and science tests.

Dr. SCHMIDT. In the excess of clarity, the report does not make a claim in this area, and so speaking for the Commission, the Commission does not take a position on this. We have said repeatedly high-skills immigration in our Nation is very important.

Mr. KHANNA. Let me just change directions, because I was just so struck by those comments of Representative Grothman I don't—I thought they had to be addressed.

But let me ask the final question, which is on a AI, and a two-part question. One, it seems to me that it's in our country's advantage to move towards forms of AI that aren't relying simply on data, and when you look at some of the work Jeff Hawkins has done on how the human mind works in terms of maps of reference, and you look at Tenenbaum at MIT [Massachusetts Institute of Technology] and what he's being able to do, saying, you know, a child doesn't need thousands of pictures to understand what a cat is but understanding how categories of human perception work, and that it would be valuable for the United States to invest in that kind of a general learning AI so that we're not dependent on data because China will have a huge advantage over data.

If you could address that, and then second, address what it means for us to have human judgment still and human control so that the defense decisions are not being just made by algorithmic AI but by people, really, still having human judgment over that.

Dr. SCHMIDT. Quick answer to the first part. Bob, you'll take the second part.

You're exactly right that, right now, these algorithms need an enormous amount of data. There's very promising research about much more limited data training models, and I think eventually this issue around data will become less important and the rise of this next generation of algorithms that you have suggested will be the story.

It's crucially important that this next generation of algorithms get invented in the United States.

Bob.

Secretary WORK. DARPA describes AI coming in three waves.

The first wave was what it refers to as expert systems. These are physics-based models that are quite capable. But they have now been supplanted by second-wave systems, which are statistical machine learning.

There are a lot of applications still for first-wave systems. So I would agree with you that there will be applications that just are physics-based models or rules-based models, if then.

They're very, very good to explain. Like, if you had a safety accident, you can go back through the coding and say this is exactly what caused the accident, and in machine learning sometimes we won't know exactly why the algorithm chose the action that it did.

As far as defense decisions, the clearest expression that I can offer you, sir, is DODD, Department of Defense Directive, 3000.09, for example, that says, "For weapons with autonomous functionalities, they will be designed and operated to maintain appropriate human judgment over the use of force," period, end of story. The DOD Law of War manual says you cannot transfer responsibility to a machine under any circumstances.

So in my view, the Department of Defense has been very clear that when it comes to decisions over human life that will always be a human making those decisions.

We also make a clear recommendation that we should declare that machines will never ever be given the authority to order a preemptive nuclear strike. The use of nuclear weapons should be off the table and we should enter in discussions with all of our rivals to see if everyone would agree with that.

Mr. LOUIE. Let me just add——

Mr. KHANNA. Thank you. Yeah, please.

Mr. LANGEVIN. Briefly. The gentleman's time has expired.

Mr. LOUIE. Just quickly. Look, we were very clear not only in 3000.09 that we must continue to comply with international humanitarian laws. That is what separates the U.S. from some of our competitors, and that humans, commanders, to be held accountable for the deployment of any such weapons onto the battlefield.

Mr. LANGEVIN. Yeah. And it's why—I'll just comment, that's why it's so important that we have international engagement and leadership on AI. Although we may view things that way, other countries that are not as friendly to us may view things and do things very differently. We can't let that happen. So international engagement is going to be critical on that topic, going forward.

Mr. Khanna, thank you for your questions.

Mr. KHANNA. Thank you.

Mr. LANGEVIN. Mr. Moore is now recognized for 5 minutes.

Mr. MOORE. Thank you, Chairman. I am encouraged by Commissioner Clyburn's focus on retention. It reflects many of my concerns about a greater retention issue that we have across sort of all branches of military among our Active Duty labor force.

And, admittedly, while I'm new to the committee and new to my time in Congress—so I'm early in my tenure—some of that is anecdotal, as I speak with—as I speak with fighter pilots in the OPSTEMPO [operations tempo] that the incentives to go to the private sector are great and there's—it's growing in that regard. And I have—I have big concerns there and I hope to use my time in this committee to address that.

And so with that same thought process, I want to make sure that we're not going down the same path, that maybe as we talk about the potential of an academy, which, with bipartisan support, is something that I could very well be excited about, you know, is 5 years enough, right.

This concept of, you know, just putting a time limit on what you're expected to do, is that enough, or do we—are we going to see some of the same issues as soon as that 5-year timeline kind of hits there's—because there's so much need in the private sector right now with AI and cybersecurity. Are we going to see that same retention or attrition issues there?

So I'll direct my question to Commissioner Clyburn. Anybody, any of you are welcome to comment. Thank you.

Dr. SCHMIDT. Can I add something ahead of Commissioner Clyburn?

Mr. MOORE. Please.

Dr. SCHMIDT. I was really struck in my work with the Defense Department of how many people work there for low pay and in difficult conditions because they were patriotic. And the ones that I spoke with did not, fundamentally, leave for money.

They left because the opportunity in their career was more interesting in the private sector, that the work that they wanted to do, they could not do well as Federal or military employees.

That's got to get fixed. To provide leadership at the national level, we're going to have to have places for these people to serve while they're in the government, and this is true not just for the DOD but any aspects of the Federal Government.

We stated earlier we believe these people to exist, we believe they're already in your employ, and we believe they're underutilized.

To me, that's a big priority for this committee to think about. How do we create it so we keep these people rather than allow them to become disaffected and then leave for higher paying jobs. Commissioner Clyburn.

Ms. CLYBURN. So I will do something that's unusual and be brief. I believe what we can do and what we should do is ensure that the tools and the infrastructure inside of government for those who want to stay, who are willing to stay, as the chairman mentioned, that they have the tools needed in order to be productive, in order to be challenged, in order for us to meet our national security objectives.

That's the biggest issue. It's the frustration inside of the infrastructure that needs to be fixed. So if we fix that, I don't think we will have as much of a retention problem. Those who want to run after money, they will do so.

But there are more people who want to serve, but they are not going to go to work every day and get frustrated about advancing, being onboarded, and a lot of the other issues that we enumerate in this 450-plus pages of light reading.

Mr. LOUIE. Let me just add 10 seconds to this level.

In our discussions both in the AI Commission and my work with the DIB, it was pretty clear we had a large number of junior officers departing and the reason why they were departing was because of the lack of understanding by their senior officers of what

these technologies can do. That frustration forced them to go choose employment elsewhere.

They are committed to this country. They are committed to the services. But we need to educate our seniors, not just our junior officers.

Mr. MOORE. There's an incredible amount of bureaucracy that does exist in these situations. I think that actually gets to a lot of your points. I support that and hope to be a part of finding ways for that labor force to be engaged and committed to continuing to move forward.

Because while it's a great thing for private economies, to have such good training at the government level, we do have to address this. So I appreciate those comments and hope to work with you on all of that.

Thank you. I yield back.

Mr. LANGEVIN. Thank you, Mr. Moore.

Mr. DeSaulnier is recognized for 5 minutes.

[No response.]

Mr. LANGEVIN. Is Mr. DeSaulnier there? Oh, you're on mute.

Mr. DESAULNIER. I just have to have the mental adeptness to remember to turn my mute off, Mr. Chairman. Thank you.

I just—I was saying that I want to concur with my colleague from the Bay Area, Mr. Khanna's comments about immigration, the best and the brightest and testing.

Clearly, we have seen it here in my district and I know he has there in terms of the importance of what Dr. Schmidt said of attracting and having attracted so many good people to this field and others.

I want to switch a little bit to—or a lot—to bots. I have had a fair amount of success around this issue in legislation, and some of the comments in your report about AI and botnets.

There's a quote in the report from the Justice Department: "Control of hundreds of thousands or even millions of computers to advance their schemes using AI and botnets."

We know from our investigation of the last elections and the Mueller report how these were used. We know how they're used domestically and for foreign.

So the Commission, again, says in its report that this may become more powerful with advanced AI, not just directly spreading malware but harvesting both computerization power and data to put forward further offensive training in ways that were not previously possible.

Now, Mr. Louie, can you talk about this threat to our infrastructure—transportation, utilities, health, and financial—please?

Mr. LOUIE. This is a real threat to our critical infrastructure flow. As problematic as botnets are, AI-driven botnets are operating at machine speeds against our defenses, which have, still, people in the loop rather than on the loop. It's a losing strategy and it's clear to us that our adversaries are using not only advanced technologies like botnets, they're going after supply chain as with the SolarWinds attacks and they're also using it in disinformation campaigns.

And the next step is to use disinformation campaigns against machines, to give machines and feed machines disinformation to

make machines do the wrong thing. That adversarial AI is a real threat.

Mr. DESAULNIER. And, Mr. Louie, just following up, there is a section that the commissioner recommends us passing in Section 4 of the International Cyber Crime Prevention Act.

To the degree you're capable, could you talk on my comments or the ability of that to help stem this threat—pardon the—pardon the choice of words—and what might we do in addition to this?

Mr. LOUIE. It's clear we have to defend forward, right. Playing a defensive posture waiting for the attack and trying to build a higher wall or a deeper moat is a failed strategy.

Second is that we have to work with our allies. If there are criminal activities, we need to raise the costs of those activities to those individuals or the nation-states that are prosecuting the attack against us.

Right now, the cost to attack is so low, the consequences are almost nonexistent, that we are inviting attack after attack after attack, and we will not stem it by simply having a higher wall of cyber defense.

Mr. DESAULNIER. Thank you.

Dr. SCHMIDT. Could I add——

Mr. DESAULNIER. Sure.

Dr. SCHMIDT. Could I add, Representative? The traditional framing of this is the Russia election attacks of 2016, which were done by humans, not by computers, as best we could tell.

There's every reason to think that not only will a country like Russia try to do this, but that many nonaligned groups—terrorist groups, unrelated groups—that are trying to disrupt the democratic processes of the democratic countries for whatever reason—economic, financial, political, just evil—because the technologies are now so broadly available.

So one of the things we talk about in the attack—in the book is that the software diffusion, right, the ability for people to access this is now—is the cat is out of the bag, whatever metaphor you care about.

And we have got to get ourselves organized around the fact that there will be continuous attacks on our information space, which you are describing as bots. But they're really much more than that.

It's attacks in terms of the quality of information, the target of information, attacks on the individuals involved, misusing their personal information, and this is also a national security issue coming forward.

Mr. DESAULNIER. And I would add in the sophistication of neuroscience and targeting, not just to individuals and demographics, but as you know.

Dr. Schmidt, if I could just—I want to take this opportunity because you're here, as somebody from the Bay Area who is very proud of our tech industry but recently has become critical and chagrined, in the sense of national security we often hear about scale. That's important to have scale, not just in tech but in finance we've heard it.

So could you comment on that, just briefly, the importance of scale with some of the challenges we have had in regards to concentration, to Ms. Foxx's comments?

Dr. SCHMIDT. I know here there is a concern about this. I will tell you that I would like to win the global competition and have America win in global competition.

That is going to require large companies because of the scale issues, the economic issues, the number of people. The projects and products that we talk about in these economies—in these companies take thousands and thousands of people and many, many hundreds of millions of dollars to build.

Those are problems of scale. We have an incredibly vibrant and diverse venture ecosystem with an awful lot of new startups, huge valuations. It's all incredibly exciting.

My strong—and this is my recommendation and has nothing to do with the AI report—my strong recommendation is if you don't like what one of the big tech companies are doing, find a way to regulate their behavior through the normal mechanisms.

I'm sure there are issues that need to be regulated. I would do it that way.

Mr. DESAULNIER. Mr. Chairman, thank you. I'd love to follow up with you, Dr. Schmidt, because we want to get the right balance in here.

Thank you, Mr. Chairman, for your indulgence.

Mr. LANGEVIN. Thank you, Mr. DeSaulnier.

Now the chair recognizes Mr. Higgins for 5 minutes.

Mr. HIGGINS. Thank you, Mr. Chairman. The timing and purpose of this joint hearing is crucial, as we discussed last month in our joint hearing with the House Homeland Security Committee.

Our foreign adversaries have elevated the battlefields into the cyber realm, artificial intelligence, and let us not—let us not fail to observe the Chinese tremendous advancements in quantum technologies, which I believe is inseparable from the conversation regarding artificial intelligence.

And I would like to ask the panel and want to get to my question rather quickly because I expect the answer to be complex. The theft of our technologies as of last year—as recent as last year the FBI [Federal Bureau of Investigation] advised that they investigated more than a thousand cases of Chinese theft of U.S. technology.

That's inside our universities and our government research and development laboratories, and I believe—and I would like the panelists to consider how we take further action to protect our technologies.

The report that we're discussing today is incredible work. I believe it'll be recognized as very significant work that you ladies and gentlemen have done, and we thank you for it.

It's going to take us a while to get our head wrapped around this. A line struck me from your report. You stated that for the first time since World War II, America's technological predominance, the backbone of its economic and military power, is under threat, and that's a quote.

I asked Dr. Schmidt to reflect upon that statement and tell America how the Federal Government and the private sector can work together to train the next generation of patriots, both civilian and military, to protect our research from theft and to gain dominance in these fields.

And as related to that question, then I'm going to turn it to you, Dr. Schmidt, until recently, every nation in our—in our military academies we teach that each nation enjoys a certain degree of elements of power, that being the military, geographic, economic, cultural, and political.

It seems to me and many of us that a new element of power must be considered as we balance our own strengths against that of the world.

That would be artificial intelligence and the quantum era. And it seems to me that China appears to be leading the world in artificial intelligence theft and quantum technology.

Dr. Schmidt, will you address that, please? Based upon your background, I believe you can give us a solid answer or at least guide us.

Dr. SCHMIDT. Thank you. Two years ago, China announced a strategy with a goal to dominate the following industries: software, AI, semiconductors, energy, robotics, and high-speed transportation and biotech and quantum.

Well, that's my whole world. That's everything I care about. It's furthermore everything that is driving the renaissance in America in American manufacturing, American leadership, American global platforms.

We lack a strategy as a country to work in those areas. We must organize it.

Mr. HIGGINS. Exactly.

Dr. SCHMIDT. We must, must, must. It's a huge issue. You highlighted the quantum issue. It should upset us that quantum leadership in China is ahead of America in certain aspects of the quantum work. We need to get our act together.

In order to do that, we need to do a number of things. The first is we need to work on our own workforce, our own STEM education, as we highlighted. We also need to recognize that we are critically dependent upon foreign researchers and foreign graduate students.

One of the things we did in the AI report is we studied where were the top researchers coming from, and many of the top researchers are, in fact, graduate students who are coming from China, who are learning and researching in our universities.

So we're empathetic that we have to keep them coming and keep them in the country and keep working on these things to help our Nation. Those are the best solutions that I have for you.

There's, obviously, a concern about intellectual property theft. To the degree that it occurs and we know it occurs, it should be prosecuted to the fullest possibility of the law.

And you can imagine that for Chinese students, for example, you could do investigations in that matter. You could also have all sorts of other ways about validating.

But we need these people in America working on these hard problems and we need a national strategy to win.

Mr. LOUIE. And we need to have—give the tools to our universities and research centers and companies to protect themselves. Well, it's really hard to protect yourself against a nation-state.

We tend to look at cybersecurity breaches as an IT [information technology] problem. Our adversaries look at it as a domain of war-

fare, and you're not going to win in that strategy. We need to better share information, create useful interchanges between enterprises, academia, research centers, and the government.

We can protect not everything but we can protect those things that are most vital to us. What's the point of leading in research if the other guy can just simply steal it?

We have to put up the appropriate protections. We need to reform our IP laws and we need to have partnerships with our allies to make it expensive for those acts to continue to go unchecked.

Ms. CLYBURN. And, sir, we need to give the tools to law enforcement in order to recognize and take action.

Mr. HIGGINS. I thank the chairman and the panelists.

Mr. Chairman, God bless you for allowing us some indulgence with time, and I yield, good sir.

Mr. LANGEVIN. Very good. Thank you. Mr. Higgins.

Mr. Kim is now recognized for 5 minutes.

Mr. KIM. Thank you, Chairman. Thank you everybody for coming together here.

And I've had the chance to be able to go through the report at length and then sat down with your staff. So I've gone through a lot of that and feel very good about the recommendations and I'm grateful for your work on that.

But I wanted us to kind of take a step back here. As we're looking at something that would be potentially just a major undertaking in terms of structuring our national security, our defense innovation efforts, and potentially billions of dollars to be able to jettison, you know, some of the old standing ways in which we have been doing this, the question that I struggle with is, how do we best explain this to the American people?

You know, how do we talk about this complexity in a human way to people in my district? And, you know, so I want to just ask Dr. Schmidt and then Secretary Work, when it comes to clearly articulating in a very understandable way how the threat will manifest and what people can understand and wrap their heads around, both in terms of the threats and the opportunities.

I would appreciate your perspective on that because I think people in my district, they understand the threats of transnational terrorism. They understand the threats of conventional warfare, that kind of way. It's something that is visible and tangible to them.

But they struggle, and, frankly, I struggle and others struggle to really understand what exactly are we talking about in terms of a threat here?

Dr. SCHMIDT. Well, I always start from the standpoint of America as a place of great freedom and our values, and I am concerned that if we lose leadership in this area, the information freedom we have, the free speech we have, all of the things that have made us as a great country will be materially affected by those changes.

And the way that would occur is because AI is, fundamentally, software and software can be deployed to change the way you perceive the world, as we have discussed in the testimony so far.

There are plenty of military comments that Bob should make. But I think the impact on our society when a targeted opponent comes into our networks and our information space and begins to

screw around could lead to a real increase in distrust in our government, a lack of patriotism, and a lack of belief in our country.

Secretary WORK. I would have started exactly where Chairman Schmidt did. A technological competition is a values competition at its core. The way these applications will be used will reflect the governance system of the country that is pursuing them.

For our American citizens, all we have to do is say look at how these technologies are being used in China: population surveillance, lack of privacy, lack of civil liberties, minority suppression.

We do not want a world in which these values are reflected through technology and the infrastructures that support them. And it is important for the United States, as the greatest democracy in the world, to apply these applications in a way that are consistent with privacy, civil liberties, and law.

Depending on who you listen to, either a McKinsey or a BCG [Boston Consulting Group], the winner of the AI competition will accrue a $13 to $15 trillion economic advantage. They also say same things for, like, 5G. 5G might be $5 to $7 billion—trillion, excuse me.

So these technologies will affect our lives in ways that will make our citizens healthier, live longer, have better lives, be able to do their work better, be able to have just new ways of entertainment.

This is a technology competition that is very important for us to win.

Mr. KIM. Yeah. Well, thank you.

Ms. CLYBURN. Sir.

Mr. KIM. Go ahead.

Ms. CLYBURN. I'm sorry. Sir, when I got my first coupon in the checkout line, I was excited. Oh, my gosh, I'm saving money here. Then I started noticing my social interactions online and seeing these ads pop up, and then I started wondering and learning more about algorithms.

Then I started figuring certain things out, that my digital footprint, my information, my pattern, can not only be monetized but can be used against me.

So when it comes to what we're speaking of today and explaining to everyday—your constituents, everyday people who are trying to save money and trying to make their lives easier—that convenience, used in the wrong way in the wrong hands, could make us the most vulnerable people ever, and that's why this is important.

Mr. KIM. Thank you. Well, look, I'd like to build out that story and that narrative with you all. So let's keep working on that.

Chairman, I yield back.

Mr. LANGEVIN. Thank you, Mr. Kim.

Mr. Johnson is now recognized for 5 minutes.

Mr. JOHNSON OF GEORGIA. Johnson from Georgia?

Mr. LANGEVIN. That's you, sir.

Mr. JOHNSON OF GEORGIA. All right, thank you. I want to thank you, Mr. Chairman, and also Chairman Lynch for holding this hearing.

China has embarked on what the Commission described in its report as a, quote, "multi-pronged campaign of licit and illicit transfer—technology transfer. In effect," the Commission argues, "China

is using American taxpayers' dollars to fund its military and economic modernization," end quote.

By some estimates, China's technology theft costs the United States between $300 billion and $600 billion a year. One of the several ways that China is seeking to gain a competitive edge is through venture capital investments in U.S.-based AI startups.

In response, the Commission recommends in its final report that Congress require investors from U.S. competitors to disclose transactions in a broader set of sensitive technologies to the Committee on Foreign Investment in the United States.

Mr. Louie, how broad is Chinese investment in U.S.-based AI startups?

Mr. LOUIE. The Chinese are—both companies as well as regional and university organizations are active throughout the entire United States doing investments.

Some of it's benign. Some of it's just because they want to make money. Some of it's suspect. But here's our challenge. CFIUS still remains fundamentally a voluntary series of regulations.

We need to make sure that it is no longer voluntary. If you're taking money from potential adversaries or competitors, like China and Russia, it needs to be disclosed.

Second, we have to make—we have been waiting for years now in the technology community for the list of the critical technologies that will be deemed critical for the United States.

We still have not produced that list. Technology companies are guessing on whether or not something requires disclosure or not. We need to make it clear that these kinds of technologies like AI, like microelectronics, like quantum computing, any of these critical—biotechnologies—any of these critical areas, if you're taking direct foreign investment or indirect investments from these nation-states, they need to be disclosed.

Most will be fine. But a few of them may not be. But we need to know and companies have a responsibility to disclose that.

Mr. JOHNSON OF GEORGIA. Thank you.

What regulatory framework for disclosure of transactions is currently in place for venture capital investments and how would requiring disclosure to CFIUS help to protect sensitive AI technologies?

Mr. LOUIE. It's hard to protect what you don't know it's happening. So the first one is just bring their knowledge up.

Second is for those critical pieces of technology that we deemed as critical, we need to make sure that State is empowered and has the skill sets to review those technologies aggressively.

You have this thing called a short form and a long form that you have to fill out, right? There's a lot of paperwork in the long form, and the short form is a little bit easier.

I think we should take a look at the filing requirements, particularly for venture capital, and to make sure that people are well educated in the regulatory regime.

The good news is most tech companies and early startups use very competent law firms. Having the law firms be a partner in this matter is going to be really critical for us to be able to not only protect the technologies, but quite frankly, protect those entrepreneurs' technologies.

The last thing an entrepreneur wants to do is invest it, take some technology that they put their hearts and lives in and have a competitor overseas suddenly show up with that technology and compete against them.

Mr. JOHNSON OF GEORGIA. Thank you. Would any of the other panelists like to comment?

[No response.]

Mr. JOHNSON OF GEORGIA. Okay. In a July 2020 report, the Center for Security and Emerging Technology at Georgetown found that out of 208 global Chinese professional associations, or CPAs, more than half advertised on their websites that they, quote, "exchange technical information, bring scientists to China, or contributed to specific Chinese talent plans," end quote.

Interestingly, however, the report also found that CPAs that advertise the transfer of technology in Chinese also are more likely to omit this information about that aspect of their missions from the English-language versions of their websites.

Mr. Louie, why might CPAs hide this information from English-speaking members?

Mr. LANGEVIN. If you could answer briefly, please, Mr. Louie, because the gentleman's time has expired.

Mr. LOUIE. I think it's difficult to read people's minds. But I would say that they are, clearly, attempting to encourage American companies to put technologies overseas.

And my biggest point is the relationship between technology transfer from U.S. to China and China to U.S. is asymmetric. For Americans to invest in Chinese companies require huge amounts of regulatory—Chinese regulatory hurdles that you have to come, whereas Chinese investments in the U.S. has almost none, and we've got to fix that asymmetry. It doesn't help us on either—in either direction.

Mr. JOHNSON OF GEORGIA. Thank you. I yield back.

Mr. LANGEVIN. Thank you, Mr. Johnson.

Ms. Houlahan is now recognized for 5 minutes.

Ms. HOULAHAN. Thank you, Chairman, and I hope you all can hear me. I have a lot of questions and so I'll try and move through them quickly.

My first set of questions is for Chairman Schmidt. I really appreciate the commissioners'—the Commission's conclusion and recommendations that help us find and build a full-time cadre for public servants with digital experience, and our success and failure in this definitely will hinge on the Federal Government's ability to compete with the private sector. And I'm really enthusiastic about the idea and concept of a Digital Service Academy.

But I'd like to hear more about your cost estimates for that, time and other resources, what it takes to get this kind of an undertaking off the ground, and could you also talk us through your cost-benefit analysis, if there is one, of alternatives that might be less expensive like, perhaps, dramatically scaling up STEM-focused ROTC programs such as the one that I participated in?

Dr. SCHMIDT. Perhaps Commissioner Clyburn would like to help me. These—it's a false equivalency to say that these somehow are related to the military and ROTC activities.

We strongly support the military and ROTC activities, and they are phenomenal and we should invest more in them, especially with respect to specialized skills—the digital skills.

In addition, the civilian workforce needs upgrading and the two are separate. The economics around the civilian workforce one are pretty straightforward.

The cost of hiring the people, the cost of paying them, and so forth and so on, is much less expensive if they're going through a 4-year program which has been subsidized to some degree by the government and where they have a 5-year commitment to work.

So the economics actually work.

Mignon.

Ms. CLYBURN. Yes, I will have to get back in touch with you in terms of the actual amount of shoring up a full academy. But the per student—the last figure I remember was a $50,000 per, you know, life cycle in terms of the actual expenditure per student.

But my answer to you is what's the cost of not doing anything? That cost is—cannot be quantified. It is a negative and a burden on our system, and we must address this immediately.

Ms. HOULAHAN. Yeah, I completely agree with that. In fact, that's kind of part of my follow-on question, which is that I believe, Chairman Schmidt, you mentioned something about the universities having offered to help get the DSA, the Digital Service Academy, stood up.

Could you maybe explain how that might happen, how they might plan to do that? And how do universities foresee being able to be supportive of this kind of initiative?

Secretary WORK. Well, ma'am, just to follow up, Appendix E in the report outlines what we believe are the recommended investments and all of our recommendations. Our estimate for the Digital Service Academy is that a $40 million initial investment would get us on the way.

We did not make a calculation on how many—how much per year. But, for example, the STEM Corps or the Digital Corps in the Department of Defense, we thought $5 million in FY 2022 and $5 million in FY 2023 would allow you to essentially start the framework, and the National Reserve Digital Corps, managed through the Office of Management and Budget, about $16 million.

Now, these——

Ms. HOULAHAN. And that—and that actually leads, and I'm sorry to interrupt. I'm just trying to make sure that I ask, you know, probative questions that help kind of get us to where we need to be, which is, I believe, in support of these kinds of ideas.

This last question is for Commissioner Clyburn and it has to do with the Digital Corps that we're just talking about.

I'm also really interested in the idea of a Reserve Component. I also was a reservist myself for many years and was never, frankly, called upon. I'm an engineer.

And I was wondering if you might, you know, kind of think about how to imagine the opportunity for people to participate in that while coming in and out of private—the private sector. How do you recommend the idea and how do we address potential conflicts with that?

Ms. CLYBURN. Your last thing was potential—well, let me say that the benefits are many. These individuals could come in, triage, help, assist, augment, at critical points in the cycle. If they are dedicated to a particular agency, it could make a world of difference.

And I struggled over the last part of your question.

Ms. HOULAHAN. Just the potential conflicts. You know, if you're coming in and out of the private sector, maybe even the defense industrial sector, and you are coming in and out as a reservist into this Digital Corps concept, what kind of conflicts could we foresee and how would we be able to address them?

Ms. CLYBURN. Well, Dr. Schmidt might be able to speak on that head on. But there would not be a—there should be a vetting process. There should be, I believe, you know, ways to address that, at least initially, in terms of the skills—the digital skills and the opportunity to enhance that three P or P3 partnership is worth some of the risks, I believe, moving forward.

Ms. HOULAHAN. Thank you. And I apologize. I've run out of time so I will yield back, Chairman.

Dr. SCHMIDT. Just as a comment, Congresswoman, your service and in the Reserves was not called on because undoubtedly they didn't know how to find you and why you were so valuable.

So there is a demand-side problem where the government doesn't know that you're available and they can't take advantage of your skills. We have got to get that fixed.

Ms. HOULAHAN. Concur. Thank you, sir.

Mr. LANGEVIN. Yeah, completely concur. That was a great point to raise. Very good.

Well, this has been a great discussion. Are there any members that have not asked a question that would like to recognized?

[No response.]

Mr. LANGEVIN. Okay. Hearing none, I just want to thank our witnesses for your testimony today. This has been invaluable.

The report that you've produced is going to be both foundational and enduring, I have no doubt, as we confront the challenges and opportunities presented before us in harnessing the power of AI, and I know it will be very informative for Members of Congress and staff as we draw upon your expertise and all the time and the effort that went into your hearings and putting the report together.

Before I close out the hearing, I just wanted to yield to the ranking member in case you had any final thoughts or comments, Elise.

Ms. STEFANIK. Thank you so much, Chairman Langevin, and thank you, thank you, to the commissioners for their tremendous work. It is going to help guide us in the future for an effective whole-of-government approach.

I also appreciate your focus on the workforce challenge that is so urgent that lies in front of us. There is significant bipartisan interest in tackling this workforce issue with alacrity.

So thank you for the great work. We look forward to integrating many of your recommendations through the National Defense Authorization Act this year, as we did in the last Congress, working on a bipartisan basis with Jim and our colleagues on the subcommittee and full committee.

And thanks for coming in today and dedicating so much time. I yield back.

Mr. LANGEVIN. Thank you. Yeah, well said.

Dr. SCHMIDT. And, Mr. Chairman, on behalf of the Commission, I would like to say, once again, that it has been a privilege and an honor for the commissioners and Commission to serve you.

We remain ready and able and willing to work on this to make sure that we get to the great outcome for America.

Thank you so much.

Mr. LANGEVIN. Thank you.

Secretary WORK. And, Mr. Chairman, if you'd allow me——

Mr. LANGEVIN. Yes, go ahead, Mr. Grothman. Go ahead, Ranking Member Grothman, go ahead.

Mr. GROTHMAN. Right. I'd just like to thank you as well. It is a very important issue. It's an issue we cannot afford to fail on and can't afford to lose on. I hope this committee has other hearings on this topic as time goes on.

I appreciate all the work that went into report. the report, and thank you for coming to Washington today.

Mr. LANGEVIN. Excellent.

Secretary WORK. Mr. Chairman, I just wanted to add that we can provide the committees with a classified briefing to give a fuller picture of how China and Russia are approaching this competition, and I feel like I'm probably as immersed in this as much as anyone and there are things in the intelligence record that, quite frankly, surprised me very much.

So we stand ready to come over and give that briefing to either the committee or to members of the committee or however you would like to see it.

Mr. LANGEVIN. Very good. Yeah, and thank you, Secretary Work, for raising that point and we will certainly take you up on that. I look forward to a classified session where we can get into some of those more sensitive details.

But, again, on behalf of all of my colleagues on both committees, I know Mr. Lynch had to leave but on his behalf as well, we just want to thank you for your extraordinary contributions to this area of artificial intelligence.

As I said, it will be a foundational document and very instructive in helping us and guiding us as we develop policies and legislation, going forward, to maximize the opportunities of AI.

So thank you all very much. I look forward to staying in touch. With that, I thank the members for their questions and, with that, this hearing stands adjourned.

I thank staff for all their hard work in putting this together, too. Thank you.

Hearing is adjourned.

[Whereupon, at 1:35 p.m., the subcommittees were adjourned.]

A P P E N D I X

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

MARCH 12, 2021

Opening Statement
Chairman James R. Langevin
Cyber, Innovative Technologies, and Information Systems Subcommittee
Final Recommendations of
the National Security Commission on Artificial Intelligence
March 12, 2021

I would like to welcome the members who are joining today's joint 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.

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

With that, I will give my opening statement. Welcome to our joint hearing with the House Committee on Oversight & Reform's Subcommittee on National Security, which will review the final recommendations of the National Security Commission on Artificial Intelligence. We welcome the Subcommittee Chairman Stephen Lynch and Ranking Member Glenn Grothman. And we also are pleased to host our House Armed Services Committee Chairman Adam Smith and Ranking Member Mike Rogers. It looks like a full house today.

I am pleased to welcome four commissioners from the National Security Commission on Artificial Intelligence, a commission created by this committee in the National Defense Authorization Act for Fiscal Year 2019 to help us advance the development of artificial intelligence, machine learning, and associated technologies to prepare the defense enterprise for the national security challenges of the future.

We asked this commission to produce a bipartisan whole-of-government effort focused on solving national security issues. We appreciate the leadership and hard work of our witnesses. Today we welcome:

- Dr. Eric Schmidt, Chairman of the Commission;
- The Honorable Robert Work, Vice Chairman;
- The Honorable Mignon Clyburn, commissioner on the workforce and ethics Lines of Effort; and
- Dr. Gilman Louie, commissioner on the Lines of Effort focused on protecting and building on AI advantages, marshaling global cooperation, and threat analysis and response actions.

While many of the commissioners hail from the tech sector, the world's understanding of artificial intelligence truly began in government defense labs—and specifically with investments by the Defense Advanced Research Projects Agency (DARPA) and the Office of Naval Research. Now, decades later, we must redouble our focus on the power of defense science and technology research to propel us into the future. I look forward to hearing the commissioners' recommendations on investments in basic and applied research, and how to encourage faster adoption of innovative and cutting-edge capabilities.

The next generation of challenges is upon us. In our last subcommittee hearing, we talked about how the Department can transform innovation into reality—specifically by orienting ourselves on the software and data capabilities that are often the beating heart of the platforms we acquire and that promise dramatically improved decision-making and optimization processes. The battlespace of the future will be a complex web of software, networks, and data, integrated across domains and among our allies. Artificial intelligence and other next generation innovations will be crucial to harness the power of data to give our men and women in uniform an edge in any future conflict. Our potential adversaries are already investing heavily in this future.

This commission has undertaken the difficult task to articulate the potential of artificial intelligence and the risks and benefits that lie ahead. They have worked through these issues and identified recommendations related to research and software development; opportunities for international partnerships; safeguarding against our adversaries' advancements in this space; and cultivating a 21st century workforce. Above all, the commission has crucial recommendations related to building and deploying AI in an ethical manner that is respectful of human rights. Indeed, that last category is what sets our nation apart. I commend the Defense Innovation Board, which was chaired until last year by Dr. Schmidt, for helping the Department begin important discussions on ethics in AI.

Last year Ranking Member Stefanik and I, along with Chairman Smith and Ranking Member Thornberry, championed a package of provisions based on the Commission's first quarter recommendations that yielded 13 provisions in the National Defense Authorization Act for Fiscal Year 2021, with the majority deriving from the Commission's call to Strengthen the AI Workforce. That STEM

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. We must move past old models of training and learning and establish a system to dynamically upskill our workforce as the technology evolves.

Ranking Member Stefanik and I were pleased to invite Commission representatives for a review of the interim recommendations last fall, and we look forward to hearing about your recently released final recommendations to Congress. Incredibly, there are over 100 in total, and over 50 related to the purview of the Armed Services Committee. We commend you for all the work you've put into this effort these past two years and we look forward to receiving your testimony.

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

Joint Written Testimony of Chair Dr. Eric Schmidt, Vice Chair HON Robert Work,
HON Mignon Clyburn, and Mr. Gilman Louie
U.S. House Armed Services Subcommittee on Cyber, Innovative Technologies, and Information Systems and the
U.S. House Committee on Oversight and Reform Subcommittee on National Security
Joint Hearing Titled: "Final Recommendations of the National Security Commission on Artificial Intelligence"
March 12, 2021

Chairman Langevin, Ranking Member Stefanik, Chairman Lynch, Ranking Member Grothman, Members of the Committees, thank you for the opportunity to testify today on the Final Report of the National Security Commission on Artificial Intelligence.

We are here on behalf of the full group of commissioners—a diverse group of technologists, business executives, academic leaders, and national security professionals who were nominated by Congress and the Executive Branch. Our task was to examine the implications of AI and associated technologies for national security and defense, and to make recommendations for government action and reform.

Over the past two years, we have operated in a transparent manner and have emphasized the need for action. We sought to learn from a wide range of stakeholders and delivered recommendations on a continuous basis. We commend Congress for adopting a number of our recommendations in last year's defense authorization legislation.

We humbly acknowledge how much remains to be discovered about AI and its future applications. Nevertheless, we know enough about AI today to begin with two convictions.

First, the rapidly improving ability of computer systems to solve problems and to perform tasks that would otherwise require human intelligence—and in some instances exceed human performance—is world altering. AI technologies are the most powerful tools in generations for expanding knowledge, increasing prosperity, and enriching the human experience. AI is also the quintessential "dual-use" technology. The ability of a machine to perceive, evaluate, and act more quickly and accurately than a human represents a competitive advantage in any field—civilian or military. AI technologies will be a source of enormous power for the companies and countries that harness them.

Second, AI is expanding the window of vulnerability the United States has already entered. For the first time since World War II, America's technological predominance—the backbone of its economic and military power—is under threat. China possesses the might, talent, and ambition to surpass the United States as the world's leader in AI in the next decade if current trends do not

change. Simultaneously, AI is deepening the threat posed by cyber-attacks and disinformation campaigns that Russia, China, and others are using to infiltrate our society, steal our data, and interfere in our democracy. The limited uses of AI-enabled attacks to date represent the tip of the iceberg. Meanwhile, global crises exemplified by the COVID-19 pandemic and climate change highlight the need to expand our conception of national security and find innovative AI-enabled solutions.

Given these convictions, the Commission concludes that the United States must act now to field AI systems and invest substantially more resources in AI innovation to protect its security, promote its prosperity, and safeguard the future of democracy. Today, the government is neither organizing nor investing to win the technology competition against a committed competitor. It is not prepared to defend against AI-enabled threats and rapidly adopt AI applications for national security purposes. This is not a time for incremental toggles to federal research budgets or adding a few new positions in the Pentagon for Silicon Valley technologists. Winning the technology competition will be expensive and require a significant change in mindset. America needs White House leadership, Cabinet-member action, and bipartisan Congressional support to win in the AI era.

The NSCAI Final Report presents an integrated national strategy to reorganize the government, reorient the nation, and rally our closest allies and partners to defend and compete in the coming era of AI-accelerated competition and conflict. It is divided into two parts.

- Part I, "Defending America in the AI Era," outlines the stakes, explains what the United States must do to defend against the spectrum of AI-related threats, and recommends how the U.S. government can responsibly use AI technologies to protect the American people and our interests.
- Part II, "Winning the Technology Competition," addresses the critical elements of the AI competition and recommends actions the government must take to promote AI innovation to improve national competitiveness and protect critical U.S. advantages.

The recommendations are designed as interlocking and mutually reinforcing actions that work best when taken together. The 16 chapters in the Main Report provide top-line recommendations. The accompanying Blueprints for Action outline concrete steps that Congress and the Executive Branch can take to implement the recommendations. The Commission has provided as much specificity as possible—including by drafting proposed legislative text and executive orders—to help the President and Congress move rapidly.

Part I: Defending America in the AI Era

AI-enhanced capabilities will be the tools of first resort in a new era of conflict as strategic competitors develop AI concepts and technologies for military and other malign uses and cheap and commercially available AI applications ranging from "deepfakes" to lethal drones become available to rogue states, terrorists, and criminals. The United States must prepare to defend against these threats by quickly and responsibly adopting AI for national security and defense purposes. Defending against AI-capable adversaries launching attacks at machine speeds without employing AI is an invitation to disaster. Human operators will not be able to keep up with or defend against AI-enabled cyber or disinformation attacks, drone swarms, or missile raids without the assistance of AI-enabled machines. National security professionals must have access to the world's best technology to protect themselves, perform their missions, and defend us. The Commission recommends that the government take the following actions:

Defend against emerging AI-enabled threats to America's free and open society. Digital dependence in all walks of life is transforming personal and commercial vulnerabilities into potential national security weaknesses. Adversaries are using AI systems to enhance disinformation campaigns and cyber-attacks. They are harvesting data on Americans to build profiles of their beliefs, behavior, and biological makeup for tailored attempts to manipulate or coerce individuals. This gathering storm of foreign influence and interference requires organizational and policy reforms to bolster our resilience. The government needs to stand up a task force and 24/7 operations center to confront digital disinformation. It needs to better secure its own databases and prioritize data security in foreign investment screening, supply chain risk management, and national data protection legislation. The government should leverage AI-enabled cyber defenses to protect against AI-enabled cyber-attacks. And given the way AI will drive transformative advancements in biotechnology, some of which may threaten our security and competitiveness, biosecurity must become a top-tier priority in national security policy.

Prepare for future warfare. Our armed forces' competitive military-technical advantage could be lost within the next decade if they do not accelerate the adoption of AI applications across their missions, and develop new operating concepts to exploit the power of AI. This will require marrying top-down leadership with bottom-up innovation to put operationally relevant AI applications into place. The Department of Defense (DoD) should:

- First, establish the foundations for widespread integration of AI by 2025. This includes building a common digital infrastructure, developing a digitally-literate workforce, and instituting more agile acquisition, budget, and oversight processes. It also requires strategically divesting from military systems that are ill-equipped for AI-enabled warfare and instead investing in next-generation capabilities.

- Second, achieve a state of military AI readiness by 2025. Pentagon leadership must act now to drive organizational reforms, design innovative warfighting concepts, establish AI and digital readiness performance goals, and define a joint warfighting network architecture. DoD must also augment and focus its AI R&D portfolio. Readiness will also require promoting AI interoperability with allies and partners.

Manage risks associated with AI-enabled and autonomous weapons. AI will enable new levels of performance and autonomy for weapon systems. But it also raises important legal, ethical, and strategic questions surrounding the use of lethal force. Provided their use is authorized by a human commander or operator, properly designed and tested AI-enabled and autonomous weapon systems can be used in ways that are consistent with international humanitarian law. DoD's rigorous, existing weapons review and targeting procedures, including its dedicated protocols for autonomous weapon systems and commitment to strong AI ethical principles, are capable of ensuring that the United States will field safe and reliable AI-enabled and autonomous weapon systems and use them in a lawful manner. While it is neither feasible nor currently in the interests of the United States to pursue a global prohibition of AI-enabled and autonomous weapon systems, the global, unchecked use of such systems could increase risks of unintended conflict escalation and crisis instability. To reduce the risks, the United States should:

- clearly and publicly affirm existing U.S. policy that only human beings can authorize employment of nuclear weapons and seek similar commitments from Russia and China;
- establish venues to discuss AI's impact on crisis stability with competitors; and
- develop international standards of practice for the development, testing, and use of AI-enabled and autonomous weapon systems.

Transform national intelligence. The Intelligence Community (IC) should adopt and integrate AI-enabled capabilities across all aspects of its work, from collection to analysis. Intelligence will benefit from AI more than any other national security mission. To capitalize on AI, the Office of the Director of National Intelligence needs to empower and resource its science and technology leaders. The entire IC should leverage open-source and publicly available information in its analysis and prioritize collection of scientific and technical intelligence. For better insights, intelligence agencies will need to develop innovative approaches to human-machine teaming that use AI to augment human judgment.

Scale up digital talent in government. National security agencies need more digital experts now or they will remain unprepared to buy, build, and use AI and associated technologies. The talent deficit in DoD and the IC represents the greatest impediment to being AI-ready by 2025. The government needs new talent pipelines, including a U.S. Digital Service Academy to train

58

current and future employees. It needs a civilian National Digital Reserve Corps to recruit people with the right skills—including industry experts, academics, and recent college graduates. And it needs a Digital Corps, modeled on the Army Medical Corps, to organize technologists already serving in government.

Establish justified confidence in AI systems. If AI systems routinely do not work as designed or are unpredictable in ways that can have significant negative consequences, then leaders will not adopt them, operators will not use them, Congress will not fund them, and the American people will not support them. To establish justified confidence, the government should focus on ensuring that its AI systems are robust and reliable, including through research and development (R&D) investments in AI security and advancing human-AI teaming through a sustained initiative led by the national research labs. It should also enhance DoD's testing and evaluation capabilities as AI-enabled systems grow in number, scope, and complexity. Senior-level responsible AI leads should be appointed across the government to improve executive leadership and policy oversight.

Present a democratic model of AI use for national security. AI tools are critical for U.S. intelligence, homeland security, and law enforcement agencies. Public trust will hinge on justified assurance that government use of AI will respect privacy, civil liberties, and civil rights. The government must earn that trust and ensure that its use of AI tools is effective, legitimate, and lawful. This imperative calls for developing AI tools to enhance oversight and auditing, increasing public transparency about AI use, and building AI systems that advance the goals of privacy preservation and fairness. It also requires ensuring that those impacted by government actions involving AI can seek redress and have due process. The government should strengthen oversight and governance mechanisms and establish a task force to assess evolving concerns about AI and privacy, civil liberties, and civil rights.

Part II: Winning the Technology Competition

The race to research, develop, and deploy AI and associated technologies is intensifying the technology competition that underpins a wider strategic competition. China is organized, resourced, and determined to win this contest. The United States retains advantages in critical areas, but current trends are concerning. While a competitive response is complicated by deep academic and commercial interconnections, the United States must do what it takes to retain its innovation leadership and position in the world. The U.S. government must embrace the AI competition and organize to win it by orchestrating and aligning U.S. strengths.

Organize with a White House–led strategy for technology competition. The United States must elevate AI considerations from the technical to the strategic level. Emerging technologies led by AI now underpin our economic prosperity, security, and welfare. The White House should

establish a new Technology Competitiveness Council led by the Vice President to integrate security, economic, and scientific considerations; develop a comprehensive technology strategy; and oversee its implementation.

Win the global talent competition. The United States risks losing the global competition for scarce AI expertise if it does not cultivate more potential talent at home and recruit and retain more existing talent from abroad. The United States must move aggressively on both fronts. Congress should pass a National Defense Education Act II to address deficiencies across the American educational system—from K-12 and job reskilling to investing in thousands of undergraduate- and graduate-level fellowships in fields critical to the AI future. At the same time, Congress should pursue a comprehensive immigration strategy for highly skilled immigrants to encourage more AI talent to study, work, and remain in the United States through new incentives and visa, green card, and job-portability reforms.

Accelerate AI innovation at home. The government must make major new investments in AI R&D and establish a national AI research infrastructure that democratizes access to the resources that fuel AI development across the nation. The government should:

- double non-defense funding for AI R&D annually to reach $32 billion per year by 2026, establish a National Technology Foundation, and triple the number of National AI Research Institutes;
- establish a National AI Research Infrastructure composed of cloud computing resources, test beds, large-scale open training data, and an open knowledge network that will broaden access to AI and support experimentation in new fields of science and engineering; and
- strengthen commercial competitiveness by creating markets for AI and by forming a network of regional innovation clusters.

Implement comprehensive intellectual property (IP) policies and regimes. The United States must recognize IP policy as a national security priority critical for preserving America's leadership in AI and emerging technologies. This is especially important in light of China's efforts to leverage and exploit IP policies. The United States lacks the comprehensive IP policies it needs for the AI era and is hindered by legal uncertainties in current U.S. patent eligibility and patentability doctrine. The U.S. government needs a plan to reform IP policies and regimes in ways that are designed to further national security priorities.

Build a resilient domestic base for designing and fabricating microelectronics. After decades leading the microelectronics industry, the United States is now almost entirely reliant on foreign sources for production of the cutting-edge semiconductors that power all the AI algorithms critical for defense systems and everything else. Put simply: the U.S. supply chain for advanced

60

chips is at risk without concerted government action. Rebuilding domestic chip manufacturing will be expensive, but the time to act is now. The United States should commit to a strategy to stay at least two generations ahead of China in state-of-the-art microelectronics and commit the funding and incentives to maintain multiple sources of cutting-edge microelectronics fabrication in the United States.

Protect America's technology advantages. As the margin of U.S. technological advantage narrows and foreign efforts to acquire American know-how and dual-use technologies increase, the United States must reexamine how to best protect ideas, technology, and companies without unduly hindering innovation. The United States must:

- First, modernize export controls and foreign investment screening to better protect critical dual-use technologies—including by building regulatory capacity and fully implementing recent legislative reforms, implementing coordinated export controls on advanced semiconductor manufacturing equipment with allies, and expanding disclosure requirements for investors from competitor nations.

- Second, protect the U.S. research enterprise as a national asset—by providing government agencies, law enforcement, and research institutions with tools and resources to conduct nuanced risk assessments and share information on specific threats and tactics, coordinating research protection efforts with allies and partners, bolstering cybersecurity support for research institutions, and strengthening visa vetting to limit problematic research collaborations.

Build a favorable international technology order. The United States must work hand-in-hand with allies and partners to promote the use of emerging technologies to strengthen democratic norms and values, coordinate policies and investments to advance global adoption of digital infrastructure and technologies, defend the integrity of international technical standards, cooperate to advance AI innovation, and share practices and resources to defend against malign uses of technology and the influence of authoritarian states in democratic societies. The United States should lead an Emerging Technology Coalition to achieve these goals and establish a Multilateral AI Research Institute to enhance the United States' position as a global research hub for emerging technology. The Department of State should be reoriented, reorganized, and resourced to lead diplomacy in emerging technologies.

Win the associated technologies competitions. Leadership in AI is necessary but not sufficient for overall U.S. technological leadership. AI sits at the center of the constellation of emerging technologies, enabling some and enabled by others. The United States must therefore develop a single, authoritative list of the technologies that will underpin national competitiveness in the 21st century and take bold action to catalyze U.S. leadership in AI, microelectronics,

Page 7 of 8

biotechnology, quantum computing, 5G, robotics and autonomous systems, additive manufacturing, and energy storage technology. U.S. leadership across these technologies requires investing in specific platforms that will enable transformational breakthroughs and building vibrant domestic manufacturing ecosystems in each. At the same time, the government will need to continuously identify and prioritize emerging technologies farther over the horizon.

* * *

The Final Report represents an important step, but it is not the Commission's final act. For the remaining life of the Commission, our work will focus on implementation to help both the President and Congress make the investments and take the actions recommended to win the AI era.

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

Gilman Louie
Alsop Louie Partners

Nominated by Secretary Wilbur Ross, United States Department of Commerce

Gilman Louie is Co-Founder and Partner of Alsop Louie Partners, an early-stage technology venture capital firm founded in 2006 and located in San Francisco. The firm focuses on disruptive and innovative technologies, and has made investments in the areas of cyber security, predictive analytics, education, and entertainment.

From 1999 until 2006, Mr. Louie was the first CEO of In-Q-Tel, an independent, non-profit venture capital firm established with the backing of the Central Intelligence Agency. Under Mr. Louie's leadership, In-Q-Tel invested in and worked with more than 80 companies that have had a significant impact on national security. Some of these companies include Arcsight, Keyhole (now Google Earth), Palantir, Language Weaver, Endeca, and Decru. George Tenet, former Director of Central Intelligence once stated that "the In-Q-Tel alliance has put the Agency back at the leading edge of technology."

Previous to In-Q-Tel, Gilman built a career as a pioneer in the interactive entertainment industry, with accomplishments that include the design and development of the Falcon F- 16 flight simulator, as well as the licensing of Tetris, the world's most popular computer game, from its developers in the Soviet Union. During that career, Gilman founded and ran a publicly traded company called Spectrum HoloByte, later acquired by the Hasbro Corporation. Gilman served as Chief Creative Officer of Hasbro Interactive and General Manager of the Games.com group before founding In-Q-Tel.

He serves as a member of the Board of Directors for the Markle Foundation, Niantic (Creators of Pokemon Go), Lookingglass Cyber Solutions, and various other private companies and non-profit foundations. Mr. Louie is Chairman of the Board of the Federation of American Scientists and of Vricon, Inc. (a joint venture between Digital Globe and SAAB).

Mr. Louie is an active advisor to the intelligence community and serves on the Board of Visitors for the National Intelligence University, is a member of National Security Commission on Artificial Intelligence and is a consultant to the Defense Innovation Board of the Department of Defense. He has served as a member of the Technical Advisory Group of the United States Senate Select Committee on Intelligence, and as a Commissioner of the National Commission for Review of Research and Development Programs of the United States Intelligence Community. He has also served as a member of the board of the CIA Officer's Memorial Foundation.

Mr. Louie has a long record of public service intermixed with his entrepreneurial activities and has received dozens of awards for his various achievements, including medallions from the NGA, CIA, and DNI. He is also a recipient of the CIA's Director's Award.

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

March 12, 2021

QUESTIONS SUBMITTED BY MR. MOULTON

Mr. MOULTON. Dr. Schmidt, your report cites the Future of Defense Task Force report, which I co-led last year. Both our reports agree that the Department of Defense has a long way to go before it can achieve competitive advantage in the field of AI, and both reports recognize that achieving that competitive advantage will require significant investment from the Department and U.S. Government writ-large. The Department pays a lot of lip service to technologies of the future like AI, but continues to pour billions of dollars into platforms of the past. Do you believe the Department can achieve its modernization goals, and the goals of your report, without reallocating investments that currently go to legacy systems, platforms, and concepts of operation?

Dr. SCHMIDT. The AI Commission's Final Report does not identify specific systems, platforms, or concepts that the Department should retire, or suggest specific areas where the Department should reduce its investments. Instead, the report outlines how the Department should approach the development and management of competitive technology investments. As a first step, DOD should produce a Technology Annex to the National Defense Strategy (NDS). This annex should identify and prioritize emerging technologies and applications that can enable the capabilities and concepts that will be required to solve the operational challenges outlined in the NDS. The annex should be more than a simple list of technologies; it should be an integrated strategy that marshals resource allocation, R&D, and acquisition processes toward common ends. The development of such an annex should be overseen by a Tri-Chair Steering Committee on Emerging Technology, led by the Deputy Secretary of Defense, the Principal Deputy Director for National Intelligence, and the Vice Chairman of the Joint Chiefs of Staff, as our report recommends. In addition, DOD should institutionalize a Department-wide, enduring review and decision-making process to divest from legacy systems. Priority threats and challenges should guide decisions to divest or reallocate funds. The U.S. military needs to integrate AI across its missions. Our report argues that if it is too costly or ineffective to equip a platform or system with AI—or to make it compatible with AI-enabled systems—then DOD should divest from that platform or system.

Our report also notes that there is an obvious use case for AI technologies to be leveraged as decision support tools in conducting this kind of analysis. In particular, AI should aid the Department in weighing data to compare the risk/reward tradeoffs between new versus old technologies and operating concepts. Finally, the report argues that efforts to develop and field next generation capabilities must be adequately resourced. We recommend that DOD should commit 3.4% of its annual budget to science and technology, which aligns with recommendations from the Future of Defense Task Force and the Defense Science Board. Based on our analysis of DOD spending on AI to date, we also recommend allocating $8 billion for R&D of core AI annually.

Mr. MOULTON. Mr. Work, your report repeatedly points to the benefits of international AI collaboration, both for the Department of Defense and U.S. Government writ large. I strongly agree that we should push for increased collaboration, for all the reasons you listed in the report and more: we need our technology to integrate with our allies' technologies, we should be able to leverage the research and development of our allies, and most importantly we need to set the tone for ethical and responsible global use of these technologies. At the same time, the Department has a reasonable instinct to protect its information and technologies, which sometimes creates a roadblock for collaboration. How can the Department better balance its responsibilities to protect certain information and technologies with this clear need for increased international cooperation and collaboration?

Secretary WORK. Extending U.S. and allied technology advantages requires establishing an effective protection regime that safeguards sensitive technologies and preserves the integrity of our research and commercial environment. It also requires cultivating international collaboration to accelerate innovation. We cannot do just one or the other; we must do both. The AI Commission's Final Report argues that the United States should take a judicious approach to export controls for emerging technologies. This approach would focus primarily on discrete chokepoints that the

United States and our allies control and that have substantial downstream effects on technology development. High-end semiconductor manufacturing equipment, such as EUV and ArF immersion photolithography equipment, is a clear example of such a technology. We must also work with our allies to strengthen our collective ability to protect the integrity of our innovation environment. The report recommends building a coalition committed to research integrity, and sidelining those who do not abide by the values that underpin innovation and global science cooperation. It also recommends sharpening the focus of CFIUS and research protection efforts to address the concerning actions of U.S. competitors, while working to exempt trusted allies and facilitate closer cooperation. Additionally, the United States must work to strengthen allied capabilities on technology protection, particularly as we further integrate our national security innovation bases with our partners in Europe and Asia. Our collective technology protection efforts will only be as strong as our weakest link. Finally, the report recommends collaborating with like-minded allies and partners, through an Emerging Technology Coalition, in a number of concrete areas that would enable the U.S. government to increase collaboration that protects innovation and research. For example, the United States, with allies and partners, should work to advance R&D on privacy-preserving machine learning or develop data-sharing best practices. Likewise, we see the Coalition as a forum for nations to explore alignment on regulatory mechanisms to protect innovation—such as export controls, intellectual property, and trade. Collaboration in the context of military and intelligence activities presents a different set of challenges. In the NATO context, for example, differential technology adoption and expertise across the alliance present challenges to AI interoperability, which is fundamental to joint operations. The Commission has called for DOD to prioritize its efforts to accelerate adoption of AI and other emerging technologies at NATO. As this work is done, it is critical that AI systems are developed and adopted in a responsible manner. That means that they must comply with the rule of law and ethical principles, and that systems should be secure, reliable, and trustworthy.

Mr. MOULTON. Dr. Louie, this report makes it clear that both the government and private sector have important roles to play in the development and deployment of AI. However, balancing those roles is no easy task. How should the Department of Defense balance its reliance on private-sector capabilities with its efforts to build internal capability, both in terms of personnel training and infrastructure? What elements of AI development and deployment should the Department work to master internally, and for what elements should the Department expect to rely on the private sector, both in the near and long term?

Mr. LOUIE. The Department of Defense (DOD) needs to shift from concepts of "reliance" and "dependencies" and to those of "partnerships" and "mutual interests." The U.S. industrial technology base is a significant source of this country's competitive advantage and innovation. The DOD should not duplicate U.S. private sector and industrial efforts. Instead, the federal government should use its buying power as this country's largest purchaser of capabilities and advanced technologies to speed the development, adoption, and deployment of cutting-edge technologies internally. This will drive transformation and deliver new and powerful capabilities to the DOD. The DOD should increase public-private partnerships with academia and industry to encourage new R&D efforts to benefit those institutions and the U.S. national security community mutually. To achieve the Commission's goal of an AI Ready DOD by 2025, the DOD requires a core group of people with deep technical expertise, as well as baseline digital literacy, across much of its workforce to understand how to use new emerging technologies effectively. Even military personnel who do not have deep technical expertise must develop core competencies in building, using, and responsibly teaming with machines. At a minimum, ensuring these competencies are present and prevalent throughout the force will help DOD personnel be better consumers of contractor-developed applications and technologies. However, it will also ensure our military can develop and update applications real-time to solve mission-specific challenges where it's most critical, such as the tactical edge. The way we manage the careers of our military personnel must change. The most significant hurdle to developing this technical expertise is the lack of career fields in software development, data science, and artificial intelligence. We must incentivize digital literacy like we incentivize joint warfighting, through a system of critical billets and an emerging technology certification process. Our acquisition workforce must also build digital literacy. Acquisition professionals must have sufficient understanding of digital and emerging technologies in order to thoughtfully apply the full breadth of acquisition pathways and contracting approaches. Our report recognizes that there are a number of acquisition workforce training initiatives underway across the Department related to digital and emerging technologies. These initiatives should be coordinated for maximum impact. It is also critical that

acquisition personnel have common access to digital technology courses available across the enterprise, as well as best practices and a community of experts that illustrate how different acquisition and contracting approaches can be used to deliver best of breed technologies. It is important to note that our recommendations do not necessarily seek to promote internal development over private sector-led development. The private sector will continue to be a critical partner for the Department in the development and deployment of AI. To better leverage the limited STEM resources and talent available in the United States and increase the rate of adoption of critical new technologies, the DOD should purchase and implement commercial off-the-shelf (COTS) whenever possible, and only invest in government-only-solutions (GOTS) in areas that COTS cannot address. Applications already proven in the commercial sector can generate labor and cost savings, speed administrative actions, and inform decision-making with superior insights if adopted by the Department. Off-the-shelf technologies will be particularly useful to optimize core business and administrative processes, as well as logistics and sustainment systems. Other applications, including those fielded in the operational environment, will satisfy unique needs and use-cases of the Department. Using this approach would help strengthen our industrial base, focus our government spending and talent on applications that will give us unique capabilities, and a competitive advantage over our competitors and adversaries.

There are several steps outlined in our report that are critical to accelerating AI adoption in DOD. Many of these same steps can lay the foundation for even more productive collaboration with the private sector. They include:

- Building an integrated technology scouting program that mobilizes a community of practice from across the DOD, the IC, federal, private, and international partners to constantly monitor emerging technology efforts across industry, the USG, adversaries, and allies.
- Based on inputs from the technology scouting program, producing a Technology Annex to the National Defense Strategy that identifies, prioritizes, and resources emerging technologies and applications, including AI applications, that solve the most critical operational challenges and drive new concepts of operations.
- Communicating technology priorities to the private sector by publicly publishing an unclassified complement to the Technology Annex that identifies specific operational challenges and capability gaps that the private sector could help solve.
- Establishing a common digital ecosystem to provide the technical foundation for ubiquitous AI development and fielding and provide access to AI software, trained models, data, and compute, as well as development environments.

————

QUESTIONS SUBMITTED BY MRS. BICE

Mrs. BICE. We know that investments in STEM education are needed to maintain our competitive advantage over our nation's adversaries in AI technology. What additional actions do you think the private sector could take to aid in growing a skilled workforce that aren't already being done? Are there incentives that Congress should consider providing to defense contractors to encourage additional engagement with students in the STEM fields?

The COMMISSIONERS. The United States needs to make significant investments in STEM education. New investments could help address the lack of diversity in STEM programs and provide for more equitable access to STEM education for all Americans. Without accelerating the growth of a skilled technical workforce, the United States will fall behind in the global technology competition. Much of the best STEM talent is in the private sector. Many experts in the private sector would be willing to contribute to government work if there were more effective ways to do so. The AI Commission's Final Report suggests several ways for the government to improve its partnerships with the private sector; there are actions the private sector can take to reciprocate as well. Recommended actions include:

- Public-private partnerships at the state and local level for K–12, community college, and university education. Addressing the shortfall of digital talent in America will require public-private partnerships at all levels of education. High poverty and low-performing schools in the K–12 academic system are ripe for opportunities for partnerships that will benefit American students and widen accessibility for a quality education. There are also pockets of private-public partnerships that have helped higher education institutions respond to the required digital talent needs of local areas, but more can be done to incentivize cooperation.

- Pass a National Defense Education Act II (NDEA II). The Commission believes the time is right for a second NDEA, one that mirrors the intent of the first legislation to increase the technology education of the nation's youth, but with important distinctions. NDEA II should focus on funding students acquiring digital skills, like mathematics, computer science, information science, data science, and statistics. NDEA II should include K–12 education and reskilling programs that address deficiencies across the spectrum of the American educational system, purposefully targeting under-resourced school districts. The Commission also recommends investments in university-level STEM programs with 25,000 undergraduate, 5,000 graduate, and 500 PhD-level scholarships. Undergraduate scholarships should include credit hours at community colleges to ensure more Americans have access to affordable STEM education. Ultimately, the goal of NDEA II is to widen the digital talent pool by incentivizing programs for underrepresented Americans.
- Direct participation on government advisory boards. There are several areas where public-private partnerships could allow for technology leaders and innovators to sit on advisory boards to assist with curriculum development or program execution, such as with the STEM Corp and the United States Digital Service Academy (USDSA) proposed by the Commission. Our STEM Corps recommendation includes a scholarship program, advisory board, private-sector partnership program, and STEM Corps member management program. Our USDSA recommendation includes a Federal Advisory Committee composed of private sector and academic technology leaders.
- Internships. Our report called for a National Reserve Digital Corps (NRDC) to allow for part-time support for the government as well as a United States Digital Service Academy (USDSA). Both of these programs would need private partners that would take in interns or fellows as part of their programs.
- Faculty exchanges and government online courses. There is a wide array of available online courses and training that already exists in the private sector. Much of this—and the content developers who produce it—could be used to augment existing programs and implement our recommendations. USDSA, for example, could recruit adjunct faculty, primarily from private-sector technology companies, to augment its tenure-tracked faculty, and ensure that it keeps relevant with industry best practices and commercial state-of-the-practice techniques. Additionally, the private sector could offer to the government already-developed content at low cost or lowered government rates.
- Short courses for leaders at all levels. Our recommendations called for the Department of Defense to establish a short course on emerging technologies for general and flag officers and senior executive-level civilian leaders. Industry could also offer other opportunities to take in government leaders at all levels for short courses where they can be exposed to technologies and software that they do not have readily available through their existing government infrastructure. They could be shown new and interesting ways to think through and solve problems using hardware and software that they might then take back to their government departments and agencies.

○