[H.A.S.C. No. 117–3]

INNOVATION OPPORTUNITIES AND VISION FOR THE SCIENCE AND TECHNOLOGY ENTERPRISE

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

HEARING HELD
FEBRUARY 23, 2021

U.S. GOVERNMENT PUBLISHING OFFICE
44–409 WASHINGTON : 2021

SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS

JAMES R. LANGEVIN, Rhode Island, *Chairman*

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

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*

CONTENTS

Page

STATEMENTS PRESENTED BY MEMBERS OF CONGRESS

Langevin, Hon. James R., a Representative from Rhode Island, Chairman, Subcommittee on Cyber, Innovative Technologies, and Information Systems 1
Stefanik, Hon. Elise M., a Representative from New York, Ranking Member, Subcommittee on Cyber, Innovative Technologies, and Information Systems 4

WITNESSES

Coleman, Dr. Victoria, Former Director of Defense Advanced Research Projects Agency, Senior Advisor to the Director, Center for Information Technology Research in the Interest of Society, University of California, Berkeley 7
Fox, Hon. Christine, Former Acting Deputy Secretary of Defense, Assistant Director for Policy and Analysis, Johns Hopkins University Applied Physics Laboratory 6
Kitchen, Klon, Resident Fellow, American Enterprise Institute 9

APPENDIX

PREPARED STATEMENTS:
Coleman, Dr. Victoria 52
Fox, Hon. Christine 42
Kitchen, Klon 63
Langevin, Hon. James R. 39

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

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

QUESTIONS SUBMITTED BY MEMBERS POST HEARING:
Mr. Langevin 79
Mr. Moore 80
Mr. Moulton 79

INNOVATION OPPORTUNITIES AND VISION FOR THE SCIENCE AND TECHNOLOGY ENTERPRISE

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS,
Washington, DC, Tuesday, February 23, 2021.

The subcommittee met, pursuant to call, at 11:00 a.m., in room 2118, Rayburn House Office Building, Hon. James Langevin (chairman of the subcommittee) presiding.

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

Mr. LANGEVIN. With that, the subcommittee will come to order. I'd like to welcome the members who are joining today's hearing remotely.

Members who are joining remotely must be visible on screen for the purposes of identity verification, establishing and maintaining a quorum, participating in the proceedings, and voting.

Those members must continue to use the software platform's video function while in attendance unless they experience connectivity issues or other technical problems that render them unable to participate on camera.

If a member experiences technical difficulties, they should contact committee 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 proceedings. Members may leave and rejoin the proceeding.

If members depart for a short while for reasons other than joining a different proceeding, they should leave the video function on. If members will be absent for a significant period or depart to join a different proceeding, they should exit the software platform entirely and then rejoin if they are able to 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, we'll get going with the formal part of the hearing and, with that, I'll give my opening statement.

So good morning, everyone. I'm pleased to welcome everyone to the first hearing of our newly established Subcommittee on Cyber, Innovative Technologies, and Information Systems, and I'm proud to be chairing this committee alongside with my good friend and distinguished colleague, Ranking Member Elise Stefanik, and I look forward to our continued record of bipartisan collaboration.

We welcome back our returning Intelligence and Emerging Threats and Capabilities Subcommittee members from the 116th Congress: Representative Rick Larsen, Ro Khanna, Bill Keating, Andy Kim, Chrissy Houlahan, Jason Crow, and Elissa Slotkin, and Representatives Mo Brooks and Mike Gallagher.

And we welcome our new members: Representatives Seth Moulton, Veronica Escobar, and Joe Morelle, and Representatives Matt Gaetz, Mike Johnson, Stephanie Bice, Scott Franklin, Blake Moore, and Pat Fallon.

So welcome to everyone. It's going to be an exciting year and term and I look forward to diving into some very important issues within the jurisdiction of the subcommittee.

So, as we enter the 117th Congress and a new administration, we are pleased to launch our oversight activities by welcoming our first witnesses to frame the Department of Defense's current innovation landscape and what the Department should do to invest in, harness, scale, and transition the innovation, science, and technology required to ensure that the U.S. military—ensure the U.S. military's future edge.

Today, we welcome, in their personal capacities, the Honorable Christine Fox, Dr. Victoria Coleman, and Mr. Klon Kitchen. I want to thank you all for joining us today.

In a time when our national defense planning has shifted focus to great power competition, addressing the challenge of rising science powers requires an ambitious strategy of national investment and aggressive development in science and technology.

Funding for basic research, applied research, and advanced technology development in our universities, laboratories, small businesses, and the tech sector plants the seeds required for our next-generation military engagements.

Yet even with bipartisan support for significant increases in investment in our national security innovation base, somehow growth in the science and technology budget is almost always sacrificed to field the mature technologies of today.

Well, while supporting our troops in the field is absolutely essential, we are putting our next generation of soldiers at severe disadvantage when we fail to prepare for the battlefield of the future.

If the U.S. is to remain a global leader in technology, we cannot simply rest on our laurels. We must actively execute a comprehensive S&T [science and technology] strategy to advance innovation.

We must invest in STEM [science, technology, engineering, and mathematics] education, university research, and programs that

develop junior talent into future leaders. We must also actively endeavor to diversify our S&T [science and technology] workforce.

Indeed, a strong diversity of background and perspectives is vital for any organization that aims to foster novelty and innovation.

So on that note, we must implement policies that promote a sound economic, political, and strategic environment on U.S. soil where global collaboration, discovery, and innovation all thrive.

The open dialogue and debate resident in academia and the research community can be anathema to the requirement for secrecy in the Department of Defense. But we must recognize and embrace how our free society provides the competitive advantage that lets us innovate faster than our great power competitors.

So our free society establishes a dynamic innovations ecosystem, and federally funded open basic research focused on discovery has allowed American universities to develop an innovation base that has effectively functioned as a talent acquisition program for the U.S. economy, and that talent is required today more than ever, as much as ever, to solve our most pressing national security challenges.

Indeed, great power competition is also a race for talent, and we must do better. That is why last year Ranking Member Stefanik and I introduced the National Security Innovation Pathway Act.

The U.S. attracts many of the world's best minds to our universities and innovative companies which develop their expertise. These talented people fortify our national security, protect our citizens, critical infrastructure, and interests, and they improve our economy.

Today, much of that talent leaves the U.S. because there are few pathways to remain. We must retain and leverage these scientists and technologists who boost the innovation that fuels our economic and defense competitive edge.

So I would be remiss, of course, not to mention that our challenges over the horizon are rapidly changing. While the Department has historically focused on producing new hardware, we know that biothreats and pandemics can cripple economies and dock carriers, and that the wars of the future will probably be fought via software platforms with the challenge of who can push better improvements and new capability the fastest.

So the Department, I believe, must pivot quickly to preparing us for this software-centric future and to treating the acquisition of the Joint Strike Fighter, just by way of example, and the sixth-generation fighters not as hardware platforms, but as flying computers wrapped in an airplane.

So the Department leaders must drag data and software from back office responsibilities and afterthoughts onto the Department's center stage. So they must enable the innovators and change agents across the enterprise, change the way the enterprise—the Department buys and delivers software, and attract the necessary scientific and technical talent to get us there.

We will not maintain our technological edge if we refuse to empower the Department to take risks, push scientific boundaries, challenge the red tape, attract a talented technical workforce, and protect its innovators.

We must empower those who lean forward on innovation, wherever they are, and to enable the technological leaps that will ensure our warfighters never enter a fair fight.

So with that, I look forward to this discussion, and 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 39.]

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

Ms. STEFANIK. Thank you, Chairman Langevin.

I appreciate you holding this important hearing today, and thank you to each of our witnesses for being here.

As the chairman noted, this is the subcommittee's inaugural hearing and the topic could not be more important. We have a vital mission here on this subcommittee that in many ways will shape the future of the Department of Defense and how battles are fought and won.

One of those missions we have is encouraging innovation within the defense enterprise. Too often legacy programs and platforms are prioritized past their usefulness and consume resources for new technologies that will help protect the United States from future threats instead of those from the past.

There are many reasons for this issue, from the Department's culture to congressional influence. However, we cannot afford to lose our quantitative or our qualitative edge over our near-peer adversaries, especially China, because of bureaucratic inertia or simply red tape.

While we struggle to quickly accomplish our innovation goals, the CCP [Chinese Communist Party] leverages all of its resources through its military-civilian fusion to rush new technologies to the PLA [People's Liberation Army] and upend the current global balance of power.

Make no mistake, we are in a competition to innovate and the side that innovates most effectively and efficiently will hold the strategic advantage that the U.S. has held since the end of World War II.

To maintain a decisive edge over China, the Department of Defense must be willing to take bolder risks, develop new programs, and invest in new technologies. Congress, for its part, must encourage and support these actions.

Thus far, Congress has given the Department some authorities to enable the acquisition of new technologies. Yet, we often hear from innovators about the, quote, valley of death.

Taking an idea from a prototype to contract with the Department often takes years, and many small companies and innovators are unable to navigate and survive this process.

The Department's short-term decision making impacts the long-term outlook for new technologies. But it doesn't need to be that way. We need to find ways to cultivate new ideas that don't fit neatly into strict programmatic timelines.

Innovation also requires a talented workforce and we should focus on growing innovators within the Department. With all the exciting work going on, from AI [artificial intelligence] to bioengineering, the Department should be able to recruit personnel to work on transformational projects. Hubs like DARPA [Defense Advanced Research Projects Agency], the JAIC [Joint Artificial Intelligence Center], and SOFWERX offer talented people the opportunity to use their technical skills to solve the problems of the present and the problems of the future.

We need to ensure the private sector is not the only driver of innovation. One issue that we keep running into is that commercially developed technologies become available to the U.S. after their active time. So we cannot maintain our edge if we are using the same products concurrently.

One of the key questions I hope we touch on today and we continue to try to answer is how do we make the environment for transformational technologies and innovations more efficient and sustainable?

I look forward to hearing from our witnesses today.

And thank you again, Mr. Chairman. I yield back.

Mr. LANGEVIN. Thank you, Ranking Member Stefanik, for your remarks. We now turn to the witnesses, then move into the question and answer session.

Let me introduce each of the witnesses reading their bios and then we'll go to our witnesses for their statements.

First, the Honorable Christine Fox. Ms. Fox was the Acting Deputy Secretary of Defense from 2013 to 2014, and until Deputy Secretary Hicks was confirmed this month, she was the highest ranking woman ever to work in the Pentagon.

She also served as the director of Cost Assessment and Program Evaluation in the Office of the Secretary of Defense and was the president of the Center for Naval Analyses.

She is currently the assistant director for Policy and Analysis at the Johns Hopkins University Applied Physics Laboratory, a university affiliated research center that has supported Department of Defense research for over 75 years.

Welcome, Ms. Fox.

Dr. Victoria Coleman. Dr. Coleman was recently the director of the Defense Advanced Research Projects Agency and a member of the Defense Science Board. She's a senior policy advisor on microelectronics technology at the Center for Information Technology Research in the Interest of Society at the University of California, Berkeley.

She was previously the CEO [chief executive officer] of Atlas AI and the CTO [chief technology officer] of the Wikimedia Foundation. Welcome, Dr. Coleman.

And, finally, Mr. Klon Kitchen. Mr. Kitchen is a resident fellow at the American Enterprise Institute where he focuses on the intersection of national security, defense technologies, and innovation.

He was previously the director of the Heritage Foundation Center for Technology Policy, and while working as a Senate staffer, he helped create the Cyberspace Solarium Commission, which I had the pleasure of serving as a commissioner.

So thank you for that, Klon, and welcome to you as well.

So, again, I want to thank all of our witnesses for being willing to appear today. We're looking forward to your testimony.

And with that, let me turn now to the Honorable Christine Fox for 5 minutes for your remarks.

STATEMENT OF HON. CHRISTINE FOX, FORMER ACTING DEPUTY SECRETARY OF DEFENSE, ASSISTANT DIRECTOR FOR POLICY AND ANALYSIS, JOHNS HOPKINS UNIVERSITY APPLIED PHYSICS LABORATORY

Ms. FOX. Thank you so much.

Chairman Langevin, Representative Stefanik—Ranking Member Stefanik, and distinguished members of this committee, thank you for the opportunity to speak with you today in my personal capacity about innovation opportunities and a vision for the S&T enterprise.

During my tenure in DOD [Department of Defense] and through my current position at the Johns Hopkins Applied Physics Lab [APL], I have had the pleasure of working closely with scientists and engineers who are innovating with new technologies.

It is clear to me that incorporating innovation into DOD programs is more important than ever. In my view, the principal challenge DOD faces is not a lack of innovation. Thanks to investments that must be sustained, new technologies are plentiful.

A sampling of APL's government-sponsored work includes brain-computer interface, biotechnology-based sensors, first dogfight between an AI-driven combat aircraft and a human pilot, and much, much more.

Then there is commercially developed technology. Recently, we have seen a greater engagement by DOD with commercial developers. So innovation abounds today. In fact, my colleagues call it a technology explosion.

The tougher task is how to adopt all this new innovation more rapidly into DOD programs. In my view, the principal challenge to adoption is less about supply and more about priorities.

Some argue that DOD must shed much of the existing military force structure to leap ahead. While some divestiture of outdated systems would be desirable, the reality is that there is a near-insatiable demand for ready U.S. forces to defend vital American interests.

We will need manned ships, tactical aircraft, ground units, and more for the foreseeable future, all of which require considerable resources for training, equipping, and sustainment.

We should not underestimate the enormity of this task. Yet, the technology explosion is here. But even if the U.S. may find it hard to adopt new capabilities, our potential adversaries are not standing still.

So this brings us back to the question of not whether to move forward, but how to do it. To make progress despite intense demands and limited resources requires a clear vision for what a future force should look like and a path to get there.

Developing this vision of the future force will define the priorities for new technology adoption and reveal the capability gaps that should drive S&T investment. My colleagues and I call this process "here to there."

When it comes to future military forces, visions abound inside and outside the Pentagon. Many current visions fall into what I would call the near here—concepts of operations, such as distributed warfare, that are designed to maximize the utility of the existing force structure while incorporating new technologies.

These shifts are significant and needed, but they don't take full advantage of new and envisioned technologies. They don't get us to "there." The more futuristic visions suggest changes like replacing entire categories of military platforms with massive swarms of expendable robots.

These kinds of visions are exciting and potentially transformational. Too often, however, they are not grounded in operational realities.

Take expendable robots or drones, for example. Time and again, I find myself coming back to questions like, how did the drones get to the fight, say, from a warehouse in California to the Western Pacific?

What are they supposed to do when they get there? Drop ordnance? Or will they provide intelligence and communications links, and in that case, what does in fact project combat power?

Are these drones really disposable? For the advanced missions, you would need a highly capable, even exquisite platform, one that is likely quite costly. And how will the drones be controlled, or will they operate autonomously?

These questions raise a host of other practical and ethical considerations. The point here is not to drop a wet blanket on drones or any other transformative technology. These kinds of questions can be answered and, in many cases, answers are in the works.

The point is to ask them. It is imperative, then, for the S&T community to marry up more closely with operational forces. Innovation that is not grounded in operational realities will not, ultimately, make a difference.

New concepts of operation developed without an understanding of new technologies will fail to make revolutionary change, the kind of change America needs to sustain our military preeminence.

We need to evolve our military force more rapidly and purposefully than we do today. Innovation is not the limiting factor, only our vision and wisdom in determining where and how to use it.

Thank you again, and I look forward to your questions.

[The prepared statement of Ms. Fox can be found in the Appendix on page 42.]

Mr. LANGEVIN. Thank you, Secretary Fox, and I appreciate you being here again with your testimony.

I now recognize Dr. Coleman for 5 minutes.

STATEMENT OF DR. VICTORIA COLEMAN, FORMER DIRECTOR OF DEFENSE ADVANCED RESEARCH PROJECTS AGENCY, SENIOR ADVISOR TO THE DIRECTOR, CENTER FOR INFORMATION TECHNOLOGY RESEARCH IN THE INTEREST OF SOCIETY, UNIVERSITY OF CALIFORNIA, BERKELEY

Dr. COLEMAN. Thank you. Can you hear me, first of all?

Mr. LANGEVIN. Yes, we can hear you fine.

Dr. COLEMAN. Wonderful.

Chairman Langevin, Ranking Member Stefanik, distinguished members of the House Subcommittee on Cyber, Innovative Technologies, and Information Systems, it is truly an honor to testify before you today, as well as nerve-racking.

Throughout the Cold War and the turn of the 21st century, the U.S. military enjoyed significant technological advantage. However, this advantage has been steadily eroding.

America's adversaries have made asymmetric strides in building their own technological advantage. This is not a result of reduced U.S. investment in national security S&T. It is a result of the technology investments outside the defense sector surpassing those within it.

The fruit of this commercial innovation are equally available to U.S. competitors and adversaries. But the DOD struggles with accessing technology and talent outside the defense perimeter.

Coupled with inefficiencies in the U.S. defense technology pipeline and China's aggressive national strategy of military-civil fusion, the technology advantage of the U.S. military is being stressed to breaking point.

Private sector companies like Intel, Microsoft, IBM, used to dominate the ecosystem from which the DOD now draws many core technologies essential to its mission.

But in the past 20 years or so, consumer technology has emerged as the driving force. The technology landscape today is defined by companies that bring technology to consumers: a phone maker, a retailer, an advertising company, and a company that keeps your personal address book.

Commercial and consumer markets matter to securing the technology advantage of our military because they drive technology evolution. And our peer competitor, China, also happens to be the world's single biggest consumer market.

China's military-civil fusion is overseen personally by President Xi Jinping, and aims to enable the PRC [People's Republic of China] to develop the most technologically advanced military in the world by eliminating the barriers between China's civilian research and commercial sectors, and its military and defense industrial sectors.

In contrast, the United States struggles to bridge the gap between commercial innovation and military technology needs in key areas such as semiconductors, 5G, AI, and aerospace technology.

We must break down the barriers between the U.S. defense industrial base and the commercial sector. In the world of technology, speed matters. The only way to get ahead and stay ahead is to be faster than our competitors.

As our predecessors envisioned force multiplication as the key strategy for defeating the Soviet threat in Europe in the aftermath of the Second World War, we should aspire to time compression as our key strategy.

To achieve time compression on our platforms, we need to evolve our platforms from the monoliths they are today to agile mosaic systems so that we're able to rapidly swap out components and always have the latest innovations deployed in our platforms.

How can we get there? It has been said that bits beat the atoms. It's all about the software. If we start thinking of the F–35 as an

information appliance versus an airplane, the whole way we approach designing, building, and maintaining it changes.

A lot has been said about supply chains. Innovation can create new businesses here at home to re-shore critical industries such as microelectronics. Scalable domestic manufacturing reduces our dependence on potentially adversarial supply chains. It creates good jobs here at home and maintains vital know-how in the United States that is essential for innovation.

To sustain a technology advantage, we must act to rebuild our industrial complex. Everything starts with people. We need to grow the DOD's workforce by expanding programs such as the SMART [Science, Mathematics, and Research for Transformation] Scholarship Program.

We also need to increase the diversity of the STEM workforce by broadening the recruitment pool in terms of expertise, background, and location, and we need to create a diverse and inclusive environment where everyone is welcome and everyone can succeed.

We need to make innovation matter. Innovation in transition is also critical but often overlooked. DARPA's Embedded Entrepreneur Initiative and National Security Seed Fund are great examples of what can be accomplished within existing authorities.

Finally, we need to broaden knowledge into the nontraditional innovation community by establishing a national security open innovation framework.

Thank you.

[The prepared statement of Dr. Coleman can be found in the Appendix on page 52.]

Mr. LANGEVIN. Thank you, Dr. Coleman.

Mr. Kitchen, you are now recognized for 5 minutes.

STATEMENT OF KLON KITCHEN, RESIDENT FELLOW, AMERICAN ENTERPRISE INSTITUTE

Mr. KITCHEN. Good afternoon, Chairman Langevin, Ranking Member Stefanik, and members of the subcommittee. Thank you for this opportunity to testify.

Our technology and innovation industries remain the envy of the world and the foundation of our national prosperity and security. These advantages, however, are not foreordained and they must continually be secured, and it's in light of this that I would like to make two points.

First, we must understand how and why the technology sector of our economy is growing in influence and importance within national security decision making.

The technologies that will determine the United States ability to secure its people and interest are overwhelmingly being developed for commercial purposes in the private sector.

This leaves the national defense more dependent on the private sector perhaps than ever before precisely as China, who blends its public and private sectors in a strategy of military-civil fusion, is emerging as a true peer competitor and rival, economically, technologically, and militarily.

With this in mind, it follows that new partnerships between the government and industry are essential, and this leads to my second point. We must have a more agile and secure technology acquisi-

tion system. But there are serious challenges to realizing this system.

The National Defense Industrial Association, or NDIA, gives the U.S. defense industrial base a barely passing C grade, and says it's getting worse.

Specifically, in a report last year the NDIA noted that scores for three dimensions—production inputs, industrial security, and supply chain—all fell below a passing grade of 70 out of 100 points, with industrial security bottoming out with an F at just 63 points.

The U.S. cannot settle for an industrial base with a passing grade and we certainly cannot accept a failure in industrial security. We have to do better.

Our current defense contractors are essential for key capabilities, especially more key platforms. But they are not typically the source of leading-edge developments in artificial intelligence, advanced robotics, or quantum computing.

These are overwhelmingly developed by companies who do not regularly work with the Department of Defense and who are not currently trying to solve defense challenges.

Now, this is not due to a lack of patriotism. It's the result of poor incentives and bureaucratic hurdles, and we can clear the way with three changes.

First, we need to recognize and employ new incentives. The current system does not prioritize the best available technology. Instead, it favors cost accounting, regulatory compliance, and administrative ease.

Budgets are programmed years in advance with little ability for companies to realize profits in current fiscal years. And, perhaps most significantly, research and development are often spread across many small contracts, instead of investing deeply in key or in promising capabilities.

Put simply, technology companies don't need government investment. They need government contracts, and they need to know that these contracts can then be scaled into real programs of record.

We must also get rid of regulatory burdens that dissuade or block these new partners. These burdens are all well documented and I'll not itemize them all here. Suffice to say this. We need to work with companies who have more engineers and coders than lawyers and contract officers.

Finally, the U.S. should prioritize the security of our domestic, technological, and manufacturing capabilities. Don't forget it was industrial security that was the lowest scoring dimension on the NDIA report.

This is not a call for economic protectionism. It's a call for commonsense security. In a world where securing nations means securing networks and supply chains, it is unavoidably true that the loyalties and the security practices of those creating and building our defense innovations matter.

In the final analysis, American policymakers and citizens should be encouraged, but also feel a sense of urgency. Our technology and innovation industries are creative, capable, and patriotic.

But if the United States is going to secure its people and its interests going forward, we must do better in leveraging and securing this new defense industrial base.

Thank you, and I look forward to your questions.

[The prepared statement of Mr. Kitchen can be found in the Appendix on page 63.]

Mr. LANGEVIN. Thank you, Mr. Kitchen. I want to thank all of our witnesses for their exceptional testimony today. Your insights have been very helpful.

We're now going to go to the question and answer session, recognizing members for 5 minutes. I'll begin with questions and then turn to Ranking Member Stefanik.

If I could, Ms. Fox and also Dr. Coleman, Congress' goal for the breakup of the Under Secretary of Defense for Acquisition, Technology, and Logistics [AT&L] was to create an Under Secretary for Research and Engineering.

That would be the Department's science and technology visionary, the one with the time and ability to look past the horizon into the future.

Do you think that we are achieving this goal, and if not, why not?

Ms. FOX. Thank you, Mr. Chairman. I think that the emphasis on S&T that has been brought about by the separation of AT&L into the two components is good.

But I think that there's a challenge in that it perhaps has exacerbated the key problem that many of us have talked about this morning, which is adoption of technology.

I think that you need to have them hand in hand. We need to figure out how to get the new technologies into the programs, and I worry that the separation has instituted some barriers to that.

Not that it's easy, nor has it ever been easy. But by having two peer leaders with different responsibilities have to find a way to work together to accelerate adoption can exacerbate one of our biggest challenges, and that does concern me.

Dr. COLEMAN. If I were to echo my friend the Honorable Fox—Christine Fox on this, as already has been said, innovation has to be executable by the entire enterprise. It's no good if we can do it at the beginning but not the end of the process.

And, unfortunately, I think the split has created almost a fracture in this continuum of innovation. While the focus on the front end on the S&T, I think, has been very welcome and we see that, for example, in the various modernization priorities that the Under Secretary for R&E [Research and Engineering] has put forward these past 4 years that has created the similarity of focus.

At the same time also we see that innovative pipeline further down the line to absorb these things. I'm a big believer in learning from our organizational structures. No organizational structure is ever perfect.

I think with the benefit now of almost 4 years of working in this—in this structure, it's probably time that we should review, evaluate, and see how we should go forward, whether we should tweak aspects of it.

I would say that one thing that resonates with me is that acquisition of large programs seems to be a fundamentally different exercise than creating technologies and figuring out the framework with which that technology can be deployed and explored, and transitioning that technology to the warfighter.

So it may be a halfway house, if you like, where acquisition of large programs stays with the services. They know what they need to train and equip. They should be able to buy those things.

And perhaps the other two aspects, the policy aspects as well as innovation aspects, come together.

And just one quick example, software. We all know that software needs to be developed in natural ways. But it's no good if we develop it in sprints but we buy it in decades.

It's clear that different pieces need to come together and fit much better than they do already.

Mr. LANGEVIN. Thank you. If I could expand on that, Dr. Coleman. As you mentioned in your testimony, it's all about the software. Of the Department's 11 modernization priorities, 5 are software-defined technologies, while the others will require complementary software platforms to maximize their potential.

Both the Defense Science Board and the Defense Innovation Board put out major reports in recent years about the need to change the way the Department buys software.

So if you could expand upon this, how must the Department adapt to support the acquisition of world-class software platforms and tools to better leverage capability for the warfighter and affordability for the taxpayer?

Dr. COLEMAN. Thank you. This is a topic near and dear to my heart, as you can imagine. We need to adopt the best known methods from the private sector. When we develop software step by step, the reason why agile development is so successful is because we've given up on this notion that at the start of a large project we can imagine what we want the software to do.

Instead, we do it step by step, and as we do that, we discover if we are going down the right path or the wrong path, and we change.

In order for us to do that, though, how do we do it? Well, we do it through this new discipline that has emerged called product management. Everybody comes together every 2 weeks, every month, and everybody looks at what we've done and they decide, is this still the right thing? Should we be adding something? Removing something?

It's all a team exercise. And if you do that, you bring the acquisition executives in the same place as those people who are responsible for developing the software. So they're making every decision together step by step.

And I just want to, I guess, to emphasize that when we look at one or more ways of developing software, we can't bring just one part of that into, you know, Department's practices.

For example, we all understand the JAIC is important, and as you pointed out, both the Defense Innovation Board and the Defense Science Board pointed this out. We have wonderful examples like Kessel Run.

What we don't have today, however, is this concept of product management in the Department. When I ask—when I look at our innovation pipeline, which is a component in the Department of Defense that plays the role of product management, that doesn't exist today.

And I think we need to adopt these practices but we need to bring in the whole picture, you know, not just parts of it because that cannot work as well.

Mr. LANGEVIN. Very helpful insights, and I'm going to want to flesh that idea out more and how we bring that into the practice within the Pentagon and we institutionalize it. So thank you, Dr. Coleman.

With that, I'll now turn to Ranking Member Stefanik for questions.

Ms. STEFANIK. Thank you, Chairman Langevin. Thank you. Can you hear me, Jim?

Mr. Kitchen, in your written testimony, you mentioned multiple times that the private sector's ability to help the Defense Department is hampered by the need to spend resources on contract specialists and lawyers instead of engineers.

Can you give me policy recommendations about how we can improve this outdated and onerous acquisition process that, of course, disproportionately benefits larger technologies, and is more difficult for the smaller, sometimes more innovative, companies?

Mr. KITCHEN. Yes, ma'am. Thank you for the question.

I think my top-line answer is it's less about authorities than it once was, and now it's about changing the culture of those in the acquisition system, which is understandably set.

A couple of very practical things, just to be responsive to your question. Always leverage private sector and use commercially available off-the-shelf technology whenever possible. Leverage nontraditional acquisition authority such as the Small Business Innovation Research program.

Compete new systems frequently and fairly, and then ensure that winners receive meaningful contracts with clear timelines and dollar amounts.

As has been already discussed about software, software is critical and increasingly a center of focus. Well, recognizing that and showing the type of progress that we're discussing here today would mean allocating large sums to software-specific contracts, and perhaps even designating software companies as the primes and hardware companies as subordinates when appropriate.

And then, finally, the Pentagon is going to have to reconsider its one-size-fits-all approach to software and data rights when engaging private sector companies whose intellectual property and the way that they do business is bound up in the software itself and the data and insight that that software then produces.

The current approach is simply unsustainable and waves off a number of the key companies that we want to be attracting.

Ms. STEFANIK. Thank you very much. I'll yield back, Jim, to get to others.

Mr. LANGEVIN. Thank you very much. Next, Mr. Crow is recognized for 5 minutes.

Mr. CROW. Thank you, Mr. Chairman. I wanted to start with Mr. Kitchen, because you mentioned in your remarks the issue of industrial security, which has been an interest of mine for quite a while because you can't fill a bucket if you have holes in that bucket.

We can make all sorts of investments and promote, you know, innovative technologies in, particularly, our small and medium-sized businesses, as my colleague, Ms. Stefanik, just mentioned, which is a lot of where the innovation is happening.

But those companies are also the most vulnerable as well because they oftentimes don't have the same cyber protections and defenses.

So wondering what you think, starting with you and getting the thoughts of the others as well, what would be the biggest thing we could do through, like, SBIR [Small Business Innovation Research] programs or Small Business Administration to help bolster some of those fences around those smaller, more innovative companies?

Mr. KITCHEN. Yes, sir. So the fundamental truth that we're discussing is the fact, as I mentioned in my testimony, that securing nations means securing networks and supply chains.

The first thing we have to recognize is that that is an inescapable reality for the foreseeable future. That is going to define how we think about securing innovation technology.

Relatedly, I think it's also important that the Federal Government recognize that it is now a stakeholder on this issue and not the stakeholder on this issue, and what I mean by that is you're right, smaller companies up and down the supply chain do not have the requisite level of security in the supply chain that is required.

But I think an honest assessment of what's recently happened in the SolarWinds hack demonstrates that neither does the government and, in fact, it was the private sector who identified this hack and then shared that information with the government, despite our efforts of indications and warning and similar capabilities.

And so the reality is, is that if we're going to be supplying or, excuse me, securing the supply chain, this is going to take a level of integration and collaboration between the public and private sector that is perhaps unprecedented.

And to put an even finer point on it, I do not believe that there is a category in which we are able to secure our people and our interest absent a deep integration of the public and private sector at the level of strategy and policy on this issue.

Mr. CROW. Thank you. Ms. Fox, can I actually go to you next? Sorry. Because I wanted to pick up on that last point that Mr. Kitchen just mentioned, that collaboration, which really seems key here right now.

And, Ms. Fox, since you were formerly in the DOD, you know, you're acutely aware of the challenges of actually breaking down those silos. What would be the best way to actually achieve greater integration between the DOD and those smaller companies?

Ms. FOX. Yes. Thank you for the question. I think that this is a vital point, and it's all related to what we have been talking about already this morning.

I think we need to recognize that we need to more rapidly be able to upgrade, innovate, and make our systems much more modern much more rapidly.

Software has been mentioned many times. It's, obviously, key. That's going to require a different approach to our big programs.

We're going to have to start from the beginning to plan them to be modular so that they can rapidly upgrade.

Then we're going to have to create an environment that these small companies that have these innovations can plug in to these upgrades so they can provide these new capabilities.

I love the phrase of a JSF [Joint Strike Fighter] as a wrapper of software. I think that's going to be true for ships and ground vehicles, many of our large systems, in the future.

That means we have to plan from the beginning to have a collaborative relationship with these small companies.

And back to security, there is nothing more important than giving them a mechanism to plug in securely to defense innovation and acquisition, which means establishing some kind of a secure cloud architecture that they can plug into so that they don't have to try to lift that cost on their own.

If we put it all on them, we'll never get them into the—into the plan—into the program. We need to find a way to do that, and that's going to take clever new designs, more owning of the system baseline, the program baselines, by the Department of Defense, which means more expertise in both how to design and oversee the development of a program, but also more expertise in innovation and new technology.

So it's a lift, but I think it's possible if we all just kind of work for it.

Mr. CROW. Thank you, and Ms. Coleman?

Dr. COLEMAN. Very briefly. I agree with my colleagues.

One—you know, one thing that we normally don't think about when we think about security in the small businesses, there is—who has access to their technology.

So when I think about security I also think about technology protection and, you know, starting with creating technology protection programs for each one of these little companies, the first thing that you come across is that there's predatory capital, venture capital out there, that in many ways co-opts these technologies, even before the Department knew that they existed.

So in some ways, you know, we lose, you know, right out of the gate. So making sure, for example, that we have capital that is not predatory, that is available, and is not foreign, that it's available to these small businesses, I think is going to be fundamental to our success.

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

Mr. LANGEVIN. Thank you, Mr. Crow.

Before I go to Mr. Brooks, if I could just remind all members that under the committee rules, when they're on—when you're on for the hearing, your video has to be visible at all times and, you know, you can—if you're going to be stepping away for a minute you can just leave it going.

If you're going to be leaving for extended period of time or if you're going to be jumping on another hearing, you should exit the platform completely. But while you're on the platform, the video has to be on at all times.

With that, we'll go to Mr. Brooks for 5 minutes.

Mr. BROOKS. Thank you, Mr. Chairman.

Ms. Fox and Dr. Coleman, both of you allude in your written testimonies that overcoming the so-called valley of death remains a significant challenge for the Department of Defense.

For those watching this hearing unfamiliar with the term, it refers to the reality that many promising science and technology research projects ultimately fail to be delivered to warfighters because they're never transitioned into acquisition programs once the technology has been successfully demonstrated.

During my tenure in Congress, I have seen the incredible work done by private industry and by scientists within the Department of Defense, like those of the United States Army Combat Capabilities Development Command Aviation Missile Center, formerly known as the U.S. Army Aviation Missile Research Development and Engineering Center, or AMRDEC.

Unfortunately, although our science and technology enterprise consistently produces astonishing innovations in basic research, applied research, and advanced technology development, translating those innovations into programs of record that result in weapons systems being fielded has proven to be difficult.

I'm impressed by the work being done by the services to overcome this, especially by the Army's Rapid Capabilities and Critical Technologies Office with respect to hypersonic weapons and directed energy. But more needs to be done.

Can each of you offer concrete examples of current Department of Defense efforts to successfully bridge the valley of death and how those can be emulated across the Department of Defense?

Ms. FOX. Well, thank you for the question. I'm not sure that I have an exemplary current example to offer you. I do have, however, a lot of examples of activities that are aimed to try to solve this problem.

I think you have a lot of work, as you pointed out, in the Army, but also in the Air Force and the Navy, to do more rapid prototyping and to try to learn from the rapid prototyping and then select the technology and move it across.

I think, though, that it fails when we actually try to go across that valley of death. We have lots of prototypes but what we need are sustainable programs, and getting to sustainable programs means that we have to cross over.

But you don't want the innovation to die once it becomes a big program, and that's the problem. Once it's in a big program, it starts to get locked up in the system that produces something sustainable and important, but not necessarily easily innovated and upgraded.

So what do you do? Well, I think, again, you go back to the very beginning and we try to design for this from the start by working with small businesses but also, again, as I said in my testimony, with the operating forces to understand exactly where we're trying to go, what we need, and design these programs from the very beginning to be modular by nature and to allow the new capabilities to come in and be rapidly upgraded so that they are innovative from the start.

There are a few small examples of this from our history, but nothing that I can at least point to right now. Perhaps my colleagues have a current example.

Dr. COLEMAN. So if I may offer one, at DARPA the agency is working on hypersonics and it's working actually in very close collaboration with the Air Force.

DARPA is building out the air-breathing category of hypersonic systems which, you know, hopefully, are successful, will be transitions leading to the ARRW [Air-Launched Rapid Response Weapon] program in the Air Force. So it does happen, but I would agree with, you know, all the previous statements that it doesn't happen nearly as often as it should.

But one of the things that I want to highlight is that this is not a problem that is specific to the Department of Defense. You know, working in a research lab for many years, for example, at Intel, we had lots and lots of innovative ideas that, you know, we have been able to build out in the lab. Not many of them made it into a product.

There's a big, big road to be—long road to be traveled between an innovation and actually building something that somebody can use and I think, again, we can learn a great deal from looking at the private sector to see how they do this, how they get the years of innovation and the years of production to come together in a way that allows—maximizes the transfer of ideas.

I think the private sector has built up expertise in this over many years that I think we can leverage in the Department.

Mr. BROOKS. Thank you, Mr. Chairman. I yield back the balance of my time.

Mr. LANGEVIN. Thank you, Mr. Brooks.

Ms. Slotkin is now recognized for 5 minutes.

Ms. SLOTKIN. Great. Thanks for being here and for doing this. I think what you're hearing from us, we're sort of—both sides of the aisle, frankly, asking different versions of the same question, which is, we have all heard testimony in the last Congress.

We have read the books. We have read the papers. We have heard from the experts that technology is not being incorporated fast enough and we're losing that edge to China.

And so I guess—I'm just going to push a little bit on my friend, Christine Fox, who is the witness who has lived this from the inside.

If you were named, you know, in Kath Hick's position in Deputy Secretary of Defense again right now and you had to figure out what you were going to do in the next 2 weeks to try and address this problem specifically—either from programs within the Defense Department or coming back to Congress and saying, I don't have the flexibility I need from you all, here are the three things I need—what are the concrete things that Kath or that the Deputy Secretary Hicks should be doing right now and how can we help from Congress?

Ms. FOX. Thank you. It's very nice to see you, Congresswoman Slotkin.

So, yes, of course. As always, you ask the very hard questions, don't you? So 2 weeks. Well, I think in 2 weeks, I would go through the services and the acquisition community in this side of the Department and I would handpick a very small number of people who have great experience.

I would combine them with some people from industry, commercial partners, but also from our UARC [university affiliated research centers] and FFRDC [federally funded research and development centers] culture that understand how to actually develop these technologies and get them into government programs, and I would give them the task of figuring out how to start designing these programs from the beginning to be upgradable, rapidly upgradable, so that we don't get these systems that stay sort of stuck, if you will, in time for a very long time, able to accept the software.

And then I would task them to identify any systems that are at the very beginning that we could start to apply this to right now.

And then I would start to work with Congress to understand if there are any new legislation capabilities that we would need to implement those plans. I'm not sure there are. There is actually a fair amount of flexibility now.

It's a question of figuring out how to put this together with this forward-looking vision from the very beginning. Hopefully, that would give you a 2-week start.

Ms. SLOTKIN. That's helpful. Thank you. I'll yield back my time. I just will say, Mr. Chairman and Leader Stefanik, you know, I think it would be useful if we got together with the new leadership at the Pentagon and offered our help if there's anything we can do from a congressional perspective to ease some of the restraints that might be on them at the Pentagon, to moving quicker and incorporating.

I don't know that there is, but, certainly, we could do our part to try and ease that through our mantle here on the committee.

And I yield back.

Mr. LANGEVIN. A great suggestion. We want to make sure that they know that they have our support and that we would support those kinds of changes.

So, with that, Mr. Gallagher is recognized now for 5 minutes.

Mr. GALLAGHER. Thank you, Mr. Chairman.

Mr. Kitchen, you're familiar with the Bloomberg reports about Super Micro and the potential CCP compromises of its supply chain, correct?

Mr. KITCHEN. I am, sir. Yes.

Mr. GALLAGHER. I know that elements of those reports are somewhat controversial. So how, in your opinion, should we on this committee view them? Or put differently, it seems to me that these reports are a big warning sign, a giant sort of neon flashing sign that hardware manufactured in China, even under the auspices of an American company, could be subject to compromise. Do you agree with that assessment?

Mr. KITCHEN. Absolutely.

Mr. GALLAGHER. And should the Department of Defense or, really, any entity whose product stores or transmits information that is sensitive in nature be sourcing electronic components of its supply chain from China?

Mr. KITCHEN. If they choose to do so they're assuming a significantly high level of risk, and that level of risk seems to be escalating.

Mr. GALLAGHER. So I guess if we zoom out, I mean, what do you think are some of the lessons of this Super Micro story and how would you sort of encourage the committee to view it?

Mr. KITCHEN. So, thank you, sir. As you said, there are some missing pieces in the Bloomberg reporting, but it gained the traction that it did precisely because the threat is real.

So whether the specific instances described are correct or not, the threat of supply chain interdiction and the use of software and hardware to then gain access to critical systems is absolutely the case.

It's the thing that individuals in the information security environment know is out there and it's particularly—the Bloomberg article highlights hardware.

But I think things like SolarWinds and other recent activity demonstrate that it's actually software that is the most critical issue. Hardware, certainly, is important and cannot be ignored.

But hardware is the kind of thing where you can identify changes in manufacturing and physical changes and things like that. But when it comes to software, you know, a major platform's gonna have millions of lines of code, and keeping a regular assessment and awareness of any changes going on in that code is a Herculean effort.

And so the bottom-line answer to your question is, is supply chain security is a critical factor that we're only really beginning to acknowledge, let alone address.

Mr. GALLAGHER. I thank you for that. I'd also like to draw attention to a recent report that seems to indicate that Oracle has been marketing its products to Chinese security services, including, remarkably, authorities in Xinjiang and the PLA.

I guess to put a fine point on this, Mr. Kitchen, should any—in your opinion, should any American defense contractors be pursuing business with the Chinese government, let alone the Chinese military?

Mr. KITCHEN. So I have no special insight into Oracle's activities in China. I will say, however, that any company offering data and analytic services to the Chinese Communist Party and its regime of oppression deserves to be publicly shamed and should be thoroughly reviewed before receiving any contracts with U.S. Government.

Companies that provide these services are enabling human oppression at scale and with a type of ruthless efficiency, and I, frankly, don't trust anyone who prioritizes those kinds of profits over human dignity.

Mr. GALLAGHER. Thank you for your candor. And I yield back the balance of my time.

Mr. LANGEVIN. Thank you, Mr. Gallagher.

The chair now recognizes Ms. Escobar for 5 minutes.

Ms. ESCOBAR. Thank you, Mr. Chairman, and thank you, Ranking Member. And many thanks to our witnesses. This has been a really great hearing, an important one for us to begin our work with.

I found many of the comments and the statements in your testimony really fascinating. But one of the ones that I most appreciate

is Mr. Kitchen's statement that we need more engineers and coders than we need lawyers.

And no offense to any lawyers in the room. But, you know, I represent a district that has a university that is creating lots of these engineers and coders and with a special focus on additive manufacturing and 3DI printing, an area that I think is completely underutilized by the DOD.

And so I'd like to hear from our witnesses what their thoughts are on linking up—where we could do a better job of linking up with universities and that talent in those engineering departments.

And, Mr. Kitchen, maybe you can go first.

Mr. KITCHEN. I suspect my fellow witnesses will have deeper insight into that. I'll simply say that, as I mentioned previously, that deep connection between the private and public sectors on how to go forward absolutely includes private sector research and universities.

It's often discussed, but not often in detail, the critical gap in terms of our national needs for engineering expertise and other relevant technological expertise and what we're producing domestically.

And our ability to attract and retain global talent is going to be critical, and often that pipeline flows through the university systems.

Ms. ESCOBAR. I agree.

Ms. Fox and Ms. Coleman, would love your thoughts.

Ms. FOX. Thank you. Thank you for that question. I think university research is key and I completely would agree with what my colleague, Mr. Kitchen, has just said. We don't have enough great minds in this country able to meet all of these fabulous technology innovation opportunities and challenges, for that matter.

The more that we can work with universities, the more that we can tap the expertise and encourage more and more U.S. investment in STEM education to build more and more of this capability and capacity, the better.

But we do definitely—from the DOD perspective, there needs to be strong partnership with academic research at the very beginning of what we have been talking about this morning leading to this innovation.

Ms. ESCOBAR. Thank you. Ms. Coleman.

Dr. COLEMAN. Thank you. So I don't know where to start. You know, I live here in Silicon Valley right next door to Stanford. I work at Berkeley. You know, these universities are creating entire industries, entire communities.

I think building stronger links between the defense mission and both the research that is done at the schools as well as the graduates that work for 2 to 3 years is absolutely essential.

I don't think, honestly, that we pay enough attention to this. I don't think we pay enough attention to it even from an investment perspective.

I mentioned briefly the STEM program that the Department has been running for some years. It's approximately maybe 3,000 students a year, Ph.D. students a year. We should be doing 10 times that.

You know, you only have to look at the backgrounds and, you know, countries that students come to our shores in these high-tech domains to see that others are making much greater investments in supporting the growth of a domestic workforce that is essential and can help us, you know, not only building the technology but also transition them.

And it goes, really, hand in hand with this notion of building, rebuilding, supply chains here at home. You know, what will it take one day for us to be able to make an iPhone here in the United States?

Lots of things must take—need to take place including, for example, manufacturing—obviously, manufacturing technologies. Where is that going to come from? It is going to come from the labs in our universities.

The other thing, of course, we need to be careful about is that there is the "valley of death." This was mentioned today already.

So as we support our universities to create innovation, we also need to support them to scale that innovation to show that it can succeed, to give them the tools to enable the transit of that innovation from the lab to production to products of record.

It doesn't happen if we don't plan for it, if we don't resource it, if we don't work on it. Thank you.

Ms. ESCOBAR. Thank you so much. I couldn't agree more. I hope this committee changes that, Mr. Chairman. I yield back.

Mr. LANGEVIN. Thank you, Ms. Escobar. The chair now recognizes Mr. Gaetz for 5 minutes. Is Mr. Gaetz still there?

Mr. GAETZ. Sure. There we go. Thanks for unmuting me, Mr. Chairman, and grateful to be on the subcommittee with you and the ranking member. I'm admirers—I'm an admirer of both of yours.

I had questions for Dr. Coleman. But Mr. Kitchen's response to Mr. Gallagher's question was so sweeping and inspirational I have a bit of a follow-up.

Mr. Gallagher was asking you about Oracle. But I have to ask if those same statements you had about it being, you know, essentially unpatriotic for these U.S. companies to be supporting this regime, have you followed the collaboration that Google is doing in China and does that trouble you to the same degree?

Mr. KITCHEN. Thank you, Congressman. In my answer to Congressman Gallagher, I mentioned that I had no special insight into Oracle but that I would reiterate that any company who provides material support to the CCP is enabling human oppression at scale.

And so I would say any company who's materially doing that would stand under the same condemnation. The only thing ——

Mr. GAETZ. Have you followed Google? Have you followed Google's collaborations in China?

Mr. KITCHEN. So far as I understand, number one, I'm not—I don't represent Google or anyone else. I'll simply say that what I understand Google to be doing in China exists primarily in terms of research.

I know that they have an artificial intelligence research center there. I believe part of the controversy that they've ensued over the

last several years is because they were considering going back into business there, which I don't understand them to be currently.

Mr. GAETZ. So, Microsoft, similarly, has one of those AI collaboration innovation centers, just like Google does, in China. Does that give you concern for the resiliency of those companies?

Because one of the overall themes of all the opening statements today was that we are relying increasingly on the commercial enterprises within America to fuel innovation. But if they are driving that innovation, in part, from centers in China, you know, should that give us some concern?

Mr. KITCHEN. I think companies who are doing a large portion of their innovation and R&D in China, obviously, are assuming a high level of risk.

I believe that that level of risk is reaching a point to where the United States Government now has to consider the implications of that as they think about how they're going to work with any company.

Mr. GAETZ. Yeah. No, I appreciate that, and I know Mr. Gallagher and many others, Mr. Banks, you know, on the committee who see China for the threat they are will likely take that testimony to heart.

Dr. Coleman, your opening statement struck me because it seemed that what you were saying is that, you know, when the greatest minds in America at our greatest companies were working with military, we have the greatest technological edge on the world.

But, increasingly, today, the greatest minds in America are working on likes and clicks and video views and consumer activity, and that has coincided with an erosion of the technical edge that we have on the world.

At the same time, Mr. Kitchen is telling us that these very companies that are driving the likes and the type of commercial activity are now creating innovation centers in China.

Have I understood your testimony correctly? Because it seems to me that that is, you know, a far broader problem for the country.

Dr. COLEMAN. I completely agree with you, sir. I remain concerned about both overt and not so overt activity by the CCP in many of the high-tech areas that are of interest to us, both commercially as well as in terms of national security.

One thing that my colleague on here is very familiar with is the co-opting that often takes place. If you are going to do business in China, there are certain preconditions for admission to that market, and that is artificially constraining growth and markets for our companies.

It is a conundrum, especially in companies that require very, very significant capital in order to operate. If you take the semiconductor business, for example, they need to have access to those markets in order for them to create enough profit to continue doing the R&D that is needed to develop high-end products.

I think we need, as a nation, to find a solution to this, to stop these predatory practices by China so that companies can deliver their products in those markets without at the same time co-opting their technology.

I will also take the opportunity of your comment to speak about my great concern around digital authoritarianism and the export of it by the Chinese government.

They are masters at blocking sites. They are masters at filtering what information arrives at what person. They are masters at flooding the network with misinformation, and they are also masters of co-opting social media.

It is a significant concern. I don't believe it's a concern that we in the national security community have addressed so far, and it's something that I would really like us to spend a lot more time and thinking on so that we can figure ways of countering it. Thank you, sir.

Mr. GAETZ. Thank you. I believe it was former President Clinton who said saying that the Chinese could control the internet would be like saying that they could nail Jell-O to the wall.

So it appears, based on your testimony, they figured out how to do that. I appreciate the chair's indulgence and I yield back.

Mr. LANGEVIN. Thank you, Mr. Gaetz.

Ms. Houlahan is now recognized for 5 minutes.

Ms. HOULAHAN. Thank you, Mr. Chair. Thank you to all of you all for joining us today.

I have a question for Dr. Coleman that has to do with some of the comments you were talking about, about the importance of expanding the STEM workforce and the SMART Scholarship Program. And you did, you know, kind of go into some depth about that.

But I'm still trying to figure out how do we actually do what you're asking us to do. One of the recommendations of a recent study was that we create a sort of a STEM Academy, an equivalent of the Air Force Academy, Naval Academy, for people with degrees, rather, in STEM and STEAM [science, technology, engineering, the arts, and mathematics].

Is that something that you're talking about? Is that—can you give me some concrete ideas of how we can increase the pipeline of STEM talent in this country?

Dr. COLEMAN. Thank you. I would love to speak on this. First and foremost, I think we see the number—increasing the financial supports that we offer to, you know, to domestic students. You know, people, frankly, down the line could actually obtain a security clearance so that we could bring them in to the Department in the roles that we so critically need to have filled.

It is—you know, doing a Ph.D. in a high-end institution, and I should know, my son graduated just before Christmas with a Ph.D.—it is a very significant commitment, both financial and time commitment.

So two things need to happen. One is that money needs to be available, and why is it that we are only sponsoring 3,000 students a year?

I don't have the numbers for China, but I can guarantee it would be in the hundreds of thousands, as opposed to 3,000.

The other piece of that, though, is once someone has made the investment and the choice to go and spend 5 years getting a Ph.D. in a topic, they will have an expectation to get a good job here at home.

Today, for many of these technologies, microelectronics and semiconductors, which is something that I have worked on for quite a while, those good jobs today are in Taiwan. They are not here domestically.

So there is a vicious cycle. People who don't go into these disciplines because they can't get good jobs here at home.

So as well as growing the STEM workforce, at the same time, as I was saying earlier, we need to start an effort to rebuild our industrial commerce, and we can do so. We can do so, you know, by bringing back, you know, businesses or products that somehow we thought was okay to outsource.

Well, you know, it's not okay to outsource them because eventually you lose the know-how that is needed in order to innovate because people, students, families will not choose to go and study these topics that are essential if you're going to innovate, say, in semiconductors. So it all comes in a big circle.

Ms. HOULAHAN. Thank you. I have only a couple more minutes of my time. Another thing that we didn't really touch on yet in this conversation is how we can integrate our friendly international partners and allies into all of these conversations.

Mr. Kitchen, you're nodding your head. Is there some kind of conversation that we should pull in all of those allies of ours across the—across the globe as well into this?

Mr. KITCHEN. Yes, ma'am. I couldn't agree more. The United States simply just can't—it's not a turnkey thing where we turn on, you know, an entire ecosystem of innovation that covers every emerging technology.

And more to the point, even if we did, we need our partners and allies to be able to come alongside us, concurrently, for their own security. We have international agreements and partnerships like NATO [North Atlantic Treaty Organization].

The 5G conversation illustrated this very clearly. And our response to 5G now within our group of partners and allies, particularly in Europe, I think is also illustrating the way forward.

So as we have prevailed upon our friends in the United Kingdom, in Germany, I hope in France, I hope—and I hope in the broader European Union, we're going to see both the need and, I think, the reality of deeper, more sustained cooperation where we are mutually encouraging and supporting one another's technological development, not only to include and facilitate interoperability but our own individual and corporate security.

Ms. HOULAHAN. Thanks. And with the last half minute or so, several of you have made a comment which kind of says, effectively, well, there really isn't anything standing in our way of creating, you know, these awesome pipelines of technology and talent legislatively. We just need to culturally change.

Is that—is that fair? Like, several—at least two of you-all have said that during this discussion, and I was struck by it. Is that something that I should be taking away from this conversation or did I mishear?

Ms. FOX. You didn't mishear me. I do think that we need to constantly be looking for obstacles in our way. So I wouldn't ever assert there's nothing.

But there's been a lot of positive change and I do think we need different approaches, different conversations. Those are cultural, in large part.

There are lots of important reasons. We should recognize that the culture makes it difficult. They're doing important things now, but we also have to change.

Ms. HOULAHAN. And I'm afraid I've run out of time and I have to yield back, and I appreciate your time.

Mr. LANGEVIN. Thank you. I just recognized the vice chair of the subcommittee. Thank you for your line of questions.

Ms. Bice is now recognized for 5 minutes.

Mrs. BICE. Thank you, Mr. Chairman, and thank you to the witnesses for being here today. This is such an important topic we are discussing because the conflicts of tomorrow will truly be won or lost by the investments that we make today.

Dr. Coleman, you mentioned earlier the role of venture capital in this space. What approach do you think Congress should take to protect predatory venture capital firms from overtaking these smaller firms who may be working on classified programs that they may not be able to fully divulge or disclose?

Dr. COLEMAN. Thank you. I love that question. Thank you so much for asking it.

As the CEO of a new startup that is trying to, well, raise capital for my company, I experienced that very personally.

You know, one of the things that we did right was the passing of FIRRMA [Foreign Investment Risk Review Modernization Act of 2018], the rejigging of CFIUS [Committee on Foreign Investment in the United States] to also include investment within the purview, and this is what's really worth hearing about.

Entire companies, venture companies that used to pump Chinese money into small startups have gone away. They've chosen to go away. Not all of them. The problem is we didn't replace them with trusted domestic capital.

So you now have a situation where a company that would have access to Chinese money, they no longer have access. What happens to them?

I have been worrying about this now for years because I experienced it personally, and luckily for me and my company, we were able to raise a good Series A and move forward.

I think that we should be thinking very seriously about reforming SBIR or creating additional programs to make trusted capital available to small businesses. At DARPA, you know, we started pushing a little bit down this path by creating the National Security Seed Fund.

So we took a little bit of money away from SBIR allocation and we said, we'll turn this into the seed fund. So, first of all, it would be—it's available to companies to bid at any time on any topic, and then the funding that they would—they would take from that would be used to build products, to hire salespeople, to build out the business pretty much the same way as venture capital is being used.

So we do that. It was $35 million. It's a drop in the bucket. I think the only reason why we did it, really, is to show what is possible within existing authorities.

I couldn't—I couldn't say—I couldn't put it in even stronger terms. We have a "Houston, we have a problem." We need to do something to replenish the Chinese capital that left town. Thank God they're dead. I'm very glad. They should go somewhere else. But we should be doing something to replenish it.

Mrs. BICE. And Dr. Fox or Mr. Kitchen, do you have any comments on that?

Ms. FOX. So I think that Dr. Coleman—and I'm just Ms. Fox. I'm sorry.

But Dr. Coleman makes a very important point. We need to be very aware of what China is doing and take actions to bolster security, and kicking out the Chinese money for venture capital is a step in that direction.

But the most important thing I believe that we can do is invest in ourselves and we need to really look hard at where those investments are needed, and I think those investments are needed in things we've talked about today: STEM education and in investing in our small businesses and in our own innovative culture, and, frankly, in our government innovation and our government-funded work.

If we invest in ourselves, I truly believe that we can make a lot of progress here, and we have kind of gotten out of the habit of looking at that.

Mrs. BICE. Well, Ms. Fox, thank you for that comment because that leads me into the second question, which is really about the education piece of this. I'm concerned that we aren't doing enough focus on an emphasis on STEM programs for young people in the country.

I actually met with the dean of engineering at one of the colleges in my State, Oklahoma State University, and was shocked to find out that a very small fraction of students that are graduating from some of the largest high schools right around Tinker Air Force Base were actually entering STEM programs after high school.

What do you think we should be doing either through Congress or what the—what should the DOD be doing to sort of foster those relationships and make sure that kids are exposed to STEM and that they're looking at STEM certifications or degrees that will help us down the road?

So to Dr. Coleman's comment earlier, we don't have enough of those folks. We need to foster it at an earlier age. How do we do that?

Ms. FOX. So I can take a stab at that. I believe that if—there's not a silver bullet here, obviously. I think that this needs to be something that we understand and there should be incentives put in place for everything, every company, every organization, every government-funded lab, like APL, to be engaged in reaching out to the STEM education community and get kids as early as possible.

Just one tour of our lab that I've seen over and over and over has turned young girls around into going into STEM education. It's so rewarding.

We have many programs but we don't have enough. I mean, there's just—again, investing in ourselves, investing explicitly in programs that engage kids early and from all walks of life and all economic levels.

We really can't afford to leave a great mind behind. This is—this is a race and we have all been talking about the importance of it. We have got to tap our talent.

Mrs. BICE. Well, my time is expired. I want to thank you for the questioning and I will add that I am the mother of a daughter who's in an engineering program in college. So I agree with what you're saying there.

So, thank you. I yield back, Mr. Chairman.

Mr. LANGEVIN. Thank you, Ms. Bice.

Mr. Morelle is now recognized for 5 minutes.

Mr. MORELLE. Thank you, Mr. Chairman. This is a really critically important subject so I appreciate you very much starting our efforts focused on it.

And I want to thank the witnesses. This has been a fascinating conversation. I'll admit most of my work on innovation policies at the State level involved commercial innovation.

For instance, the "valley of death" that we talk about in that space is really a company, usually a small company, perhaps not capitalized, that has innovations but can't get to the marketplace fast enough and get to a revenue positive position.

So learning about it from a national security perspective in this context is new to me.

I was very interested in the comments about stem cell, or STEM education—stem cell—STEM education, something I worked on as well as workforce and supply chain disruptions.

One of the other things I've worked on in the State level is orphan technologies where innovators would be working on advances, but because it wasn't central to their mission they would often put things to the side.

And we did some interesting work in New York trying to take those innovations and use them in places, perhaps with other companies, that could make a connection. I don't know whether that's something that is done in this space.

But I think for now, as I'm a new member, and, clearly, I'm just beginning the journey on how all this relates in terms of innovation policy to national security, I think I'm going to submit questions for the record.

And with that, I, again, appreciate the witnesses, appreciate the subject very much, and I will yield back the balance of my time.

Mr. LANGEVIN. Okay. Thank you, Mr. Morelle.

The chair now recognizes Mr. Franklin for 5 minutes.

Mr. FRANKLIN. Thank you, Mr. Chairman, and our panelists today. I really appreciate your time. It was a very, very important topic. We spent a lot of our time today talking about the acquisition process and the need for change there.

As a former operator, retired Navy pilot, I experienced that on the end of the whip a lot of times, just anecdotally, frustrations I had as an operator. We just never being able to seem to get technology that was readily available on the civilian side quickly enough on the military side.

As an example, in the early 1990s, we were patrolling no-fly zones in Iraq. We were actually having to go to Bass Pro Shops to buy Garmins to use for GPS [Global Positioning System], even

though it was readily available in the outside but wasn't available in any of our aircraft.

Then later on after I retired, started flying on the general aviation side and realized that we had technology in civilian airplanes that anyone could go out and buy that we still didn't have in our most advanced fighters.

So we have always had that lag. It's a cultural challenge that we have known has always existed and, to me, I think some of that is we know that the DOD doesn't typically reward risk taking and innovation. It's a system that kind of gravitates towards inertia and that tends to be rewarded a lot of times. So I think we do need to make changes there.

And then now, as a civilian on the outside working with a lot of companies that—entrepreneurs that work in the defense space, the idea that—the concept I hear over and over from them is that we have great ideas that we would love to share with DOD but that's where good ideas go to die, and that they can monetize those, get them to market, and do things more productive in working with the civilian sector.

But Ms. Fox, I was very encouraged to hear your commentary about the progress that we have made culturally. Actually, for you and for the others, I would love to hear what we can do to continue to foster within DOD the type of mindset that we're going to need to bring these technologies to market faster.

Ms. FOX. Yes. Thank you, sir, for the question.

I believe that we have made progress in the recognition that we need to move faster, that innovation is key, the rapid prototyping, the demonstrations. There's so much activity here.

What I think we need to now do is to translate the activity into programs that are sustainable but also rapidly upgradable. As you're talking about, the frustration of having to go out and buy a GPS, I remember when that happened.

It's almost—it's appalling to think about it. Yet, when you recognize that it has to be integrated into a program, it's under, you know, a prime contractor, there's rules, it has to be checked out and tested and so forth, you can start to see how that would happen.

That's what has to change. We have to plan for that at the very beginning. And so I think that the culture is recognizing the need for change. I think the Hill is recognizing the need for change. The need to take more risk is being recognized.

Now what we need to do is figure out how to do that and with purpose. So we need to have priorities. We need to do design from the very beginning. We need to lay out this plan, but we need it not to be a plan that goes for 50 years, but much more rapid term.

I think those are steps that need to be taken. I think there's awareness they need to be taken. It's just—it's hard. I mean, let's not underestimate; this is hard stuff to change. But we do need to keep pushing on everyone to make those changes, as this hearing is doing today.

Mr. FRANKLIN. Well, it does seem that the special operations forces have been able to do a better job over time of getting things that they need, whether it's off-the-shelf technology and out into the field more quickly.

We have made some special dispensations for them to do that. Are there areas that we can extend that across other parts of the Department of Defense?

Ms. FOX. You know, there are other aspects of DOD that are looking at the special ops, as I understand it. The cyber area is one that's, obviously, considering these kinds of rapid acquisition authorities.

But we ought to keep in mind that the special ops community leverages the acquisitions of the services and then they upgrade from there.

We can certainly learn lessons from the special ops experience into how they've been able to do that and what they look for in the platforms that are being procured by the services that lend themselves to that kind of rapid upgrade capability.

So I think there are lessons to be learned there. I'm a little hesitant to say that we should just use that model for all of our acquisition because we do need to keep in mind these things have to go out to lots of forces, as you experienced, and be sustainable and be trainable.

And so it's a big lift. Again, I don't think we should understate the value of the acquisition system that has produced some of the absolutely, I think, unquestionably finest warfighting equipment ever. We just need it to move more expeditiously with some changes to the model.

Mr. FRANKLIN. All right. Thank you.

Mr. Chairman, I yield back.

Mr. LANGEVIN. Okay. Thank you very much, Mr. Franklin.

Are there any members that have not been present or online that have not been recognized for a first question? Okay. Hearing none, we're going to go to a second round of questions. And Dr. Coleman, if I could start with you.

With your experience in Silicon Valley, where many companies struggle with diversity and inclusion, aspects that are vital to producing novelty and innovation, can you tell us your perspective of how the Department is doing in nurturing a diverse S&T workforce, and what must the Department do to strengthen its workforce so that it can face the challenges coming over the horizon?

Dr. COLEMAN. Thank you, sir. I appreciate that question, and in many ways, it speaks to my own experience as an individual in the S&T enterprise.

I want to reflect a little bit in this situation. In my previous agency, you know, at DARPA, we were 85 percent white, 70 percent male, 30 percent female. And we know—we know that companies that favor diversity in the ranks are much more likely to have above average profitability.

I don't think, you know, DARPA or the DOD in general is any exception—any exception to that.

How do you change it? I think, first of all, it is extraordinarily difficult, and it's extraordinarily difficult not because people don't want to change it, but because we, you know, culturally, will we hire—you know, there is this adage "like hires like."

We are comfortable with people that look like us, that sound like us, that have done the same things as us.

We have to work against that impulse. We have to be mindful. We have to create pathways and we have to create metrics that support the change. Otherwise, sir, we will never have change.

I will tell you, in my own personal, you know, life now as a private citizen, what do I do? I do mentoring. I go out of my way to help people that want to be part of the S&T community for national defense but for one reason or another are not able to.

And I open up doors, I work with them, because it's not just about getting through the door. So it's also about giving them the tools that they need in order to succeed once they are—they are inside the organization.

Understanding what makes somebody succeed as well as somebody getting hired is really important. I have not seen a ton of emphasis on this. I would like to see a great deal more.

I do know that it can really pay dividends. At the Wikimedia Foundation, after many years of effort, we got to a place where we really have much more balance. It took a ton of work. It is—you know, it's aspirational but it's also something that we have to realize we have to work at. It just doesn't happen because we desire it. It happens because we work on it. Thank you.

Mr. LANGEVIN. Thank you, Dr. Coleman.

Last question I have is of Ms. Fox or Dr. Coleman.

There is currently a pause in the Defense Federal Advisory Committee Act, FACA, boards, including the Defense Science Board and Defense Innovation Board during a 6-month review.

Understanding the importance of these boards, what would you—what would your recommendation be for the vision of these two boards, going forward? Again, just briefly.

Ms. FOX. Yes. Thank you for the opportunity.

I think these advisory boards are potentially very important, and I think they have played important roles in the past. I think that the opportunity to kind of rethink them and stand them up again gives us a chance to refocus the membership on some of the very issues we're talking about this morning.

I think that for the Defense Science Board, for example, there are some notable experts that have been on the Defense Science Board that should, hopefully, have the opportunity to come back.

We need experience. But we also need new voices, voices that understand Silicon Valley, voices that understand the challenges of defense acquisition today, voices that understand diversity and STEM education and many of these challenges.

And so I would look at this as an opportunity to think about what are the challenges the Department is most struggling with, like the ones we are talking about, and how do we tailor the representation to get us the best advice going forward.

Mr. LANGEVIN. Thank you.

Dr. COLEMAN. I had the privilege of serving on the Defense Science Board for about 5 years. I have to say that it has been, professionally, just a remarkable run. These boards are full of brilliant people.

Honestly, I would look around and I would think to myself, how come they let me in here. Just incredible individuals, and I know that even in the 5 years I have been associated with them, a great deal of contribution has been made.

Providing the kind of independence, that deep expertise that otherwise might not be available to the Department, I think, is fundamental. I do agree with my colleague that we—there's nothing that is so good that could not be made better.

This is a great opportunity to take stock, to make sure that the goals are right, that they—the number of members that each board has is sufficient to support the needs that the Department has and also making sure that we have the right composition in terms of all these challenges that we spoke about today.

I think it's a unique opportunity to reconstitute them to be even better than they were in the past, and they were pretty good in the past.

Mr. LANGEVIN. Very good. Thank you.

I'm going to now—I understand that the ranking member did not have any other further questions. So in that case, I'll go to Ms. Bice for 5 minutes.

Mrs. BICE. Thank you, Mr. Chairman.

Dr. Coleman, you mentioned earlier that China works with the commercial sector to advance their initiatives. What can we do to remove barriers between DOD and commercial innovation?

Dr. COLEMAN. Thank you. This is—this is what—you know, this is the single biggest, you know, question and maybe I can relate some of my own kind of experiences.

You know, first of all, you know, these worlds, honestly, kind of the west coast world and the east coast world are very, very separate. It's very rarely the case that there is cross talk.

But that has implications. If you want to be—to be effective in the national security enterprise, for example, requires a security clearance. There are many, many people here in the west coast community that would not qualify or they would not care to qualify. So that's one piece.

The other piece is what forums do we share. How do we—how do we speak to each other in such a way that we can leverage the best from each side?

You know, I served on the Defense Science Board for 5 years. I had this little company I was trying to get funded. I did not know where I could go to ask for support for this company in the DOD.

If I don't—if I didn't know that, what chance does the average CEO or startup founder from Stanford or Berkeley have? You know, where is the door? Where is the entrance that people can come and knock and say, I have this incredible idea that I think could change a number of things in the DOD enterprise.

I was—you know, one of the initiatives that I started at DARPA was to create, first of all, a base right here in the Bay Area where DARPA PMs [program managers] could come and do their work, which would be great because then they could form the relationships with local universities, with a lot of the entrepreneurship community, and then things flow.

But also, honestly, creating a visible door. Our notion was, and I hope that, you know, DARPA will pursue this, was to create a physical point of presence in a high foot traffic area like downtown Palo Alto, maybe in San Francisco, maybe in Berkeley, a little bit like the Apple store.

You can walk in and you can see incredible displays showing you the latest and the greatest and the needs. And, you know, you can book an appointment with Genius Bar to go and talk to somebody from the DOD to say, hey, I've discovered this thing.

Is there something that I could do in order to enhance your mission with this and, if so, who do I talk to? What programs would I have access to? How do we work together?

You know, let's not underestimate the value and the importance of physical presence in relationships and networks. It's all about building that—you know, that human kind of network that would allow us to flow innovation and people from one side to the other.

Mrs. BICE. Thank you for that.

Mr. Chairman, I yield back.

Mr. LANGEVIN. Thank you, Ms. Bice.

Next is—I understand that Mr. Khanna is there and has not yet asked a question. So I'm going to yield to Mr. Khanna. Is Mr. Khanna there and unmuted? Okay.

If not, then we will go to Mr. Morelle for 5 minutes.

Mr. MORELLE. Well, thank you, Mr. Chairman. I passed earlier. But since I'm getting a free shot, I'm going to ask questions of these witnesses, if I might.

I was talking earlier about sort of my experience in the commercial world and, you know, there among innovators it was often hard to get people to collaborate because they were stymied by the need to make their innovations profit-making so they'd keep things in a proprietary way in sharing information.

I mentioned my work on orphan technologies. At one point, we did something in New York. We went to a number of large companies. Eastman Kodak, for instance, had done some work with light spectrum because that's, obviously, light and optics and imaging is their specialty.

But they had technology that they didn't use. Anyway, another company came along, observing that there was a database with this technology in it as part of our orphan technology initiative.

They used it, put it into a product, but they haven't been very successful with it.

On the national security side, and I apologize, I'm brand new so this will probably be an ignorant question. But how do you encourage innovation among companies that would perhaps accelerate the development of their work when you still have the need to make sure that you're protecting national security?

Obviously, that's the—you know, the most important thing. But is that ever a problem or does this not present itself, and if it is a problem, are there ways that you've thought of that we could resolve it to continue to maintain national security but accelerate the development of promising technologies?

And I would ask any of the witnesses.

Mr. KITCHEN. Sir, I'll briefly respond and then I'll defer to my colleagues.

The point you raise is real and it is persistent. It is a persistent challenge, and it's reflected in the—in the government sphere as much as it is in the private sphere.

However, I think one of the key points that I would encourage everyone to take away is that that's not one of the decisive problems.

We are having a hard time ingesting the technology innovation that we have, and that we're actually being flooded with new technologies, whether they be completely new or even just recombinant innovations.

And so the key barrier to entry is our ability to, again, ingest that information. Our private sector does a phenomenal job of building a diverse innovation ecosystem and working together collaboratively when everybody understands that it's in their respective interests.

The only other thing I'll say specific to your question is that to the degree that we can bolster intellectual property protections in the private sector, we will enable and enliven that type of sharing when people feel safer to do so.

Mr. MORELLE. This problem—yeah, I'm sorry, Mr. Chairman. I just wanted to follow up.

So in a sense, you don't—there's no concern that the integration of different innovations might allow us to essentially make—to leapfrog in terms of time the development of new technologies? That would not be a concern and that's not something that I should be thinking about in this space?

Mr. KITCHEN. Well, sir, I wouldn't say it's not a concern, and I wouldn't presume to tell you what you should—what you should be spending your time on.

I'll simply say that as we talk about innovating in the defense space, that is a secondary concern relative to our general difficulty ingesting innovation that we already have.

Mr. MORELLE. And I'd just be curious, in the remaining moments, whether or not Ms. Fox or Dr. Coleman might have any comments on that.

Dr. COLEMAN. I think, just, you know, reflecting, I agree with my colleague. But I will also say that, you know, the biggest—the biggest problems that we have as a society, as a Department, oftentimes can be solved by very determined innovators from the private sector.

Ms. FOX. If I could pile on to ——

Dr. COLEMAN. Goodbye, Christine.

Mr. LANGEVIN. I think she froze. Yeah.

Dr. COLEMAN. I would just like to bring up the example of Steve Jobs. He changed the world. He wouldn't take no for an answer.

So I think, you know, if you see orphan technologies, you know, what I would say is encourage people to find new ways of using them, licensing.

You know, if it doesn't make sense within the portfolio of one company, maybe there's another company that can—that can make use of them. There are many ways that you can take things, dust them off the shelf, and put them to good use, and I would highly encourage that.

Christine, you're back.

Mr. LANGEVIN. Yeah. Ms. Fox, you were—you were—you froze up so we didn't hear what you had to say. Did you want to add to the discussion?

Mr. MORELLE. I suspect she's frozen again, Mr. Chair.

Ms. FOX. You know, I can ——

Mr. LANGEVIN. Yeah, go ahead. Oh. I think we're having technical difficulties there.

Mr. MORELLE. Very good. Thank you, Mr. Chairman. I yield back.

Mr. LANGEVIN. Okay. Thank you all very much.

Before we close out the hearing, are there any other members that didn't get a chance to ask a question? Okay. Very good.

Well, with that, I just want to thank our witnesses, Ms. Fox, Dr. Coleman, and Mr. Kitchen. Thank you for what you had to say today. Very helpful insights. We appreciate——

Ms. FOX. I'm sorry. Can you hear me?

Mr. LANGEVIN. Oh, go ahead. Ms. Fox, did you want to try again? Ms. Fox, did you have something to add? Okay. Somebody was just speaking. I'm not sure who that was.

Ms. FOX. Mr. Chairman, can you hear me? I'm sorry.

Mr. LANGEVIN. Yes. Go ahead. Go ahead.

Ms. FOX. Thank you.

Mr. LANGEVIN. Yeah. Unfortunately, I think you're having technical difficulties on your end and it keeps freezing up.

Yeah, it keeps freezing up. Do you want to try one more time? Ms. Fox, if you want to try. You seem to be on now but you need to unmute.

Okay. I think we'll end there. But I want to—again, I want to thank our three witnesses. It's been a very informative hearing. We're going to probably have some follow-up to do and I know there is some—I have a couple of questions that I'd like to submit for the record, and perhaps we could follow up with your input there. But you've given us some things to look at, to work on, and have been very helpful.

So. with that, I want to thank our witnesses for their testimony today, and the hearing now stands adjourned.

[Whereupon, at 12:48 p.m., the committee was adjourned.]

A P P E N D I X

FEBRUARY 23, 2021

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

FEBRUARY 23, 2021

Opening Statement
Chairman James R. Langevin
Cyber, Innovative Technologies, and Information Systems Subcommittee
"Innovation Opportunities and Vision for the Science and Technology Enterprise"
February 23, 2021

The subcommittee will come to order.

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

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

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

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.

I am pleased to welcome everyone to the first hearing of our newly established Subcommittee on Cyber, Innovative Technologies, and Information Systems (CITI). I am proud to be Chairing this committee again with my distinguished colleague, Ranking Member Elise Stefanik, and look forward to our continued record of bipartisan collaboration. We welcome back our returning Intelligence, Emerging Threats and Capabilities Subcommittee members from the 116th Congress, Representatives Rick Larsen, Ro Khanna, William Keating, Andy Kim, Chrissy Houlahan, Jason Crow, and Elissa Slotkin; and Representatives Mo Brooks, and Mike Gallagher. And we welcome our new members, Representatives Seth Moulton, Veronica Escobar, and Joe Morelle; and Representatives Matt Gaetz, Mike Johnson, Stephanie Bice, Scott Franklin, Blake Moore, and Pat Fallon to our new CITI subcommittee.

As we enter the 117th Congress and a new administration, we are pleased to launch our oversight activities by welcoming our first witnesses to frame the Department of Defense's current innovation landscape, and what the Department should be doing to invest in, harness, scale, and transition the innovation, science, and technology required to ensure the U.S. military's future edge. Today we welcome in their personal capacities:

- The Honorable Christine Fox
- Dr. Victoria Coleman, and
- Mr. Klon Kitchen

Thank you all for joining us today.

In a time when our national defense planning has shifted focus to great power competition, addressing the challenge from rising science powers requires an ambitious strategy of national investment and aggressive development in science and technology (S&T). Funding for basic research, applied research, and advanced technology development in our universities, laboratories, small businesses, and tech sector, seeds the necessary science to grow the advanced technological capabilities required for our next generation military engagements. Yet even with bipartisan support for a drastic increase in investment in our national security innovation base in this era of strategic competition, somehow growth in the science and technology budget is almost always sacrificed to field the mature technologies of today.

If the U.S. is to remain a global leader in technology, we cannot simply play defense, we must also play offense. We must invest in STEM education; university research; programs that develop junior talent into future tech leaders; and actively endeavor to diversify our S&T workforce. Indeed, a strong diversity of background and perspectives is vital for any organization that aims to foster novelty and innovation.

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

Indeed, great power competition is also a race for talent. And we must do better. That is why last year Ranking Member Stefanik and I introduced the National Security Innovation Pathway Act. The United States attracts many of the world's best minds to our universities and innovative companies and develops their

expertise. These talented people fortify our national security, protect our citizens, critical infrastructure, and interests, and improve our economy. Today much of that talent leaves because there are few pathways to remain. It is critical to retain and leverage these scientists and technologists who boost the innovation that backs our economic and national defense competitiveness.

And I would be remiss to not include in my opening remarks of this Cyber, Innovative Technologies, and Information Systems Subcommittee, that our challenges of the future are rapidly changing. While the Department has historically focused on producing new hardware, we know that biothreats and pandemics can cripple economies and dock carriers, and that the wars of the future will probably be fought via software platforms with the challenge of who can push better improvements and new capability fastest. The Department must pivot quickly to preparing us for this non-hardware only future; drag data and software from back office responsibilities and afterthoughts onto the Department's center stage; enable the innovators and the change agents across the enterprise; and attract the necessary scientific and technical talent to get us there.

We will not attain the technological edge we need if we refuse to empower the Department to take risks, push scientific boundaries, challenge the red tape, attract the technical workforce it needs, and protect its innovators. We must empower those who lean forward on innovation – whether it be in our laboratories, small businesses, universities, research offices, tech sector, or contracting offices – to enable the technological leaps that will ensure our warfighters never enter a fair fight. I look forward to this discussion.

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

42

PREPARED STATEMENT

OF

THE HONORABLE CHRISTINE H. FOX

ASSISTANT DIRECTOR, JOHNS HOPKINS UNIVERSITY APPLIED PHYSICS LABORATORY

BEFORE THE

HOUSE ARMED SERVICES SUBCOMMITTEE on

CYBER, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS

23 February 2021

Chairman Langevin, Ranking Member Stefanik, and distinguished members of this Committee:

I appreciate the opportunity to speak with you today in my personal capacity about innovation opportunities and a vision for the S&T enterprise. During my tenure in the Department of Defense and through my current position at the Johns Hopkins University Applied Physics Lab, I have had the pleasure of working closely with scientists and engineers who are innovating with new technologies. It is clear to me that incorporating innovation into DoD programs and harnessing the creativity of the S&T enterprise are more important than ever. Thank you for the opportunity to share my personal observations and current thinking on these issues.

I would start with the observation that the principal challenge DoD faces is NOT a lack of innovation. New technologies — and potential military applications of those technologies — are plentiful. The traditional government-funded sources which gave us the internet, satellite navigation, and stealth are as robust and productive as ever. These include DARPA, the Office of Naval Research, government-run labs, and federally funded and university affiliated research centers. A sampling of APL's work funded by our military sponsors includes brain-computer interfaces, additive manufacturing, biotechnology-based naval sensors, the first dogfight between an AI-driven combat aircraft and a human pilot, and much more. Then there is commercially developed technology. With the help of farsighted leadership — in the Pentagon and in Congress — under the past two administrations, we have seen a greater engagement with commercially derived innovation in areas like C4ISR, artificial intelligence (AI), space, and more. So, innovation abounds today — in fact, my colleagues call it a technology explosion.

As the members of this Committee know better than most, the tougher task is how to adopt all this new innovation more rapidly and productively into DoD programs. At this point, the conversation usually turns to the shortcomings of the defense acquisition system — the bureaucratic hurdles faced by nontraditional vendors, or the proverbial "valley of death" preventing new technology from receiving funding or adoption in a program of record. In recent years, these barriers have been lowered a bit with new acquisition authorities and the stand-up of organizations like the Defense Innovation Unit or the Strategic Capabilities Office. But, while the barrier is a little lower, it is certainly not gone. Many are appropriately focused on this challenge; however, it is not my focus today.

In my view, the principal S&T challenge facing defense leaders today is less about supply and more about priorities. There is broad agreement that America is engaged in great power competition. DoD's highest priority is deterring and, if necessary, defeating China or Russia in a major conflict. Many argue that DoD must shed much of the existing military force structure and related platforms and "leap ahead" to a highly autonomous force optimized for the highest-tech combat. While some divestiture of outdated systems would be desirable, the reality is that there is a near-insatiable demand for ready U.S. forces to defend vital American interests at home and abroad. We don't have the option of taking a break to reequip the entire U.S. military. We will need manned ships, tactical aircraft, ground units, and more for the foreseeable future — all of which require considerable resources for training, equipping, and sustainment and an integrated concept of operations for their employment. We should not

underestimate the enormity of this task. It is all-consuming and, too often, is given short shrift in discussions about military innovation.

Yet the "technology explosion" is here and, even if the U.S. may find it hard to adopt new capabilities, our potential adversaries are not standing still. So, this brings us back to the question of not *whether* to move forward but *how* to do it.

To make progress despite intense demands and limited resources requires a vision for what a future force should look like — for all the things it must be able to do — and, as important, for a path to get there. A big part of that journey will entail incorporating innovations such as cognitive communications, cyber, AI, zoomorphic robots, and more into new concepts of operation. Developing this vision of the future force will define the priorities for new technology adoption and reveal the capability gaps that should drive future S&T investment. Some of my colleagues at APL and I are working through this process — we call it "here to there."

When it comes to future military forces, visions abound inside and outside the Pentagon. So, you might ask, what are we suggesting that is different? Many visions fall into what I would call the "near here" — concepts of operations, such as distributed warfare, that are designed to maximize the utility of the existing force structure while incorporating new technologies. This "near here" force will operate much as it does today — think of multidomain brigades in the Army, manned-unmanned teaming in the Air Force, and autonomous surface vessels in the Navy.

These shifts are significant — and needed — but they don't take full advantage of new and envisioned technologies to fundamentally alter the character of warfare. Here is where the more futuristic visions come in, for example, replacing entire categories of military platforms with massive swarms of expendable robots. These kinds of visions are exciting and inspiring — and potentially transformational. Too often, however, they are not grounded in operational realities.

Unmanned aerial systems — to simplify things I'll refer to them as drones — provide a case in point. At the Lab, we are taking a comprehensive look at all the drone-related innovations underway and how they may add up to a new vision of warfare. The technologies being developed are very impressive — mind-blowing in some cases. However, time and again, I find myself coming back to questions like these:

- How do the drones get to the fight, say from a warehouse in California to the South China Sea?
- What are they supposed to do when they get there? Drop ordinance? Carry supplies? Shoot down other aircraft? Sink ships in blue water? Or are they intended to provide intelligence and communications links? In that case, what *does* in fact project combat power?

- Are these drones really disposable? For the advanced missions, you would need a highly capable, even exquisite platform — one that is quite costly as well.

- How will the drones be controlled? Or will they operate autonomously? These questions raise a host of other practical and ethical questions.

The point here is not to drop a wet blanket on unmanned aerial systems or any other transformative technology. These kinds of questions can be answered and, in many cases, answers are in the works. The point is to ask them.

It is imperative, then, for the S&T community to marry up more closely with operational forces — the same people who may have to take these innovations to war and trust them. Innovation that is not grounded in operational realities will not ultimately make a difference. Likewise, new concepts of operation developed without an understanding of new technologies will fail to make revolutionary change — the kind of change America needs to sustain our military preeminence.

As mentioned before, we don't have the luxury of standing down the existing force to start over according to a new vision — and likely we never will. But we can certainly evolve more rapidly and purposefully than we do today. Innovation is no longer a limiting factor; only our vision and wisdom in determining where and how to use it.

Thank you.

###

The Honorable Christine H. Fox
Assistant Director for Policy and Analysis at the Johns Hopkins Applied Physics Laboratory
Board of Directors

The Honorable Christine Fox is Assistant Director for Policy and Analysis at the Johns Hopkins Applied Physics Laboratory, a position she has held since 2014. Previously, she served as Acting Deputy Secretary of Defense from 2013 to 2014. In her role as acting deputy, she became the highest-ranking woman ever to work in the Pentagon. She officially retired from the Pentagon in May 2014. She also has served as Director of Cost Assessment and Program Evaluation in the Department of Defense from 2009 to 2013 and as president of the Center for Naval Analyses from 2005 to 2009, after working there as a research analyst and manager since 1981. Ms. Fox holds a bachelor and master of science degree from George Mason University.

DISCLOSURE FORM FOR WITNESSES
COMMITTEE ON ARMED SERVICES
U.S. HOUSE OF REPRESENTATIVES

INSTRUCTION TO WITNESSES: Rule 11, clause 2(g)(5), of the Rules of the House of Representatives for the 117th Congress requires nongovernmental witnesses appearing before House committees to include in their written statements a curriculum vitae and a disclosure of the amount and source of any federal contracts or grants (including subcontracts and subgrants), and contracts or grants (including subcontracts and subgrants), or payments originating with a foreign government, received during the past 36 months either by the witness or by an entity represented by the witness and related to the subject matter of the hearing. Rule 11, clause 2(g)(5) also requires nongovernmental witnesses to disclose whether they are a fiduciary (including, but not limited to, a director, officer, advisor, or resident agent) of any organization or entity that has an interest in the subject matter of the hearing. As a matter of committee policy, the House Committee on Armed Services further requires nongovernmental witnesses to disclose the amount and source of any contracts or grants (including subcontracts and subgrants), or payments originating with any organization or entity, whether public or private, that has a material interest in the subject matter of the hearing, received during the past 36 months either by the witness or by an entity represented by the witness. Please note that a copy of these statements, with appropriate redactions to protect the witness's personal privacy (including home address and phone number), will be made publicly available in electronic form 24 hours before the witness appears to the extent practicable, but not later than one day after the witness's appearance before the committee. Witnesses may list additional grants, contracts, or payments on additional sheets, if necessary. Please complete this form electronically.

Hearing Date: February 23, 2021

Hearing Subject:

Innovation Opportunities and Vision for the Science & Technology Enterprise

Witness name: Christine Fox

Position/Title: Appearing in a personal capacity

Capacity in which appearing: (check one)

● Individual ○ Representative

If appearing in a representative capacity, name of the organization or entity represented:

appearing in a personal capacity

Federal Contract or Grant Information: If you or the entity you represent before the Committee on Armed Services has contracts (including subcontracts) or grants (including subgrants) with the federal government, received during the past 36 months and related to the subject matter of the hearing, please provide the following information:

2021

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
N/A			

2020

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
N/A			

2019

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
N/A			

2018

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
N/A			

Foreign Government Contract, Grant, or Payment Information: If you or the entity you represent before the Committee on Armed Services has contracts or grants (including subcontracts or subgrants), or payments originating from a foreign government, received during the past 36 months and related to the subject matter of the hearing, please provide the following information:

2021

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment
N/A			

2020

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment
N/A			

2019

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment
N/A			

2018

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment
N/A			

Fiduciary Relationships: If you are a fiduciary of any organization or entity that has an interest in the subject matter of the hearing, please provide the following information:

Organization or entity	Brief description of the fiduciary relationship
JHU/APL	Officer - Assistant Director for Policy
Woods Hole	Board Member
US Naval Institute	Board Member-Finance Committee Chair
National Academies	Member Div. Eng. and Phy. Sciences (DEPS)

Organization or Entity Contract, Grant or Payment Information: If you or the entity you represent before the Committee on Armed Services has contracts or grants (including subcontracts or subgrants) or payments originating from an organization or entity, whether public or private, that has a material interest in the subject matter of the hearing, received during the past 36 months, please provide the following information:

2021

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
General overhead charge on JHU/APL's contracts	JHU/APL		Annual compensation

2020

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
General overhead charge on JHU/APL's contracts	JHU/APL		Annual compensation

2019

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
General overhead charge on JHU/APL's contracts	JHU/APL		Annual compensation

2018

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
General overhead charge on JHU/APL's contracts	JHU/APL		Annual compensation

Testimony before the House Committee on Armed Services subcommittee on Cyber, Innovative Technologies, and Information Systems

Hearing on Innovation Opportunities and Vision for the Science & Technology Enterprise.

Victoria Coleman, former Director of DARPA
February 23, 2021

Chairman Langevin, Ranking Member Stefanik, distinguished members of the House Committee on Armed Services subcommittee on Cyber, Innovative Technologies, and Information Systems, it is truly an honor to testify before you today on the innovation opportunities and vision for the S&T enterprise.

Context

Throughout the Cold War and the turn of the 21st century, the U.S. military enjoyed significant technological advantage over its adversaries. But this advantage has been steadily eroding over the past three decades. During that time, America's adversaries have made asymmetric strides in building their own technological advantage. This is not the result of reduced U.S. investment in national security science and technology. It is the result of the technology investments outside the defense sector surpassing those within it. The fruits of this commercial innovation are available equally to U.S. competitors and adversaries without any significant investment on their part. Conversely, the DoD struggles with accessing technology and talent outside the defense perimeter. Coupled with inefficiencies in the U.S. defense technology pipeline and China's aggressive national strategy of Military-Civil Fusion, the technology advantage of the U.S. military is being stressed to breaking point.

It is worth remembering how we got here. In the decades since the Sputnik experiment in the 1950s, and right up to the Cold War, technology innovation was driven by defense investments, and priorities were executed by a broad and vibrant defense R&D industry. With the end of the Cold War, as the U.S. started drawing on the peace dividend and defense investments began to shrink, commercial technology innovation and globalization took over. Frequently enabled by DoD investments, such as the Arpanet and microelectronics, companies like Intel, Microsoft, IBM, Hewlett-Packard, and others begun to dominate the technology landscape that defined the ecosystem from which the DoD now draws many core technologies essential to its mission. But in the past 20 years or so, as these technologies spread beyond enterprise uses, consumer technology emerged as the driving force. The technology landscape today is not defined by the traditional powerhouses of the 1980s and 1990s, but by companies that bring these technologies to consumers. A phone maker—Apple—who put a computer in everyone's pocket; a retailer—Amazon—who invented cloud computing; an advertising company—Google—that made searching the Web child's play; and a company that keeps your personal address book— Facebook—that built social media as we know it. We know that these innovations have offered critical capabilities to foreign state and non state actors. Armed with commercial satellite imagery, GPS, and a Facebook account, an adversary can track highly sensitive military operations not only with accuracy, but also with zero technology investment. But this is just a manifestation of something far more insidious. *Commercial and consumer markets matter* because they drive change and technology evolution. And our peer competitor, China, also happens to be the world's single biggest consumer market.

Principal challenges

China's military-civil fusion (MCF) is an aggressive national strategy of the Chinese Communist Party. Overseen personally by President Xi Jinping it aims to enable the PRC to develop the most technologically advanced military in the world by eliminating the barriers between China's civilian research and commercial sectors and its military and defense industrial sectors. Under MCF, the CCP is systematically reorganizing the Chinese S&T enterprise to ensure that new innovations simultaneously advance economic and military development. In contrast, *the United States struggles to bridge the gap between commercial innovation and military technology needs* in key areas such as semiconductors, 5G, AI and aerospace technology.

Assuming that we are able to break down the barriers between the U.S. Defense Industrial Base and access technology and innovation originating outside, our next challenge is being able to rapidly and systematically transition the technology into deployed systems – enterprise or mission. Technology transition even within the same company or organization is a challenging business. It is especially so in the large, complex innovation network that our military depends on. Cornerstone technologies like AI and 5G are just the beginning. The world is full of good ideas. But, as Steve Jobs used to say, the idea accounts for, at most, 10 percent. The remaining 90 percent is execution, and it differentiates those who win and those who fail. Taking an idea from concept to deployment is a fiercely challenging process that requires unrelenting focus, exquisite execution, and precise alignment throughout the organization. *Innovation needs to be executable by the entire organization.*

Finally, in the coming years, devoting resources to priorities such as righting our country after the Covid-19 pandemic, rebuilding the middle class or meeting the challenges of climate change will mean that we will have to do more with less as we rebuild America's military technology advantage. Picking our priorities through the lens of a *clearly articulated Defense S&T strategy* will be more important than ever.

Areas of opportunity

In the world of technology speed matters. As we strive to build technology advantage, we also have to strive to keep it. All technology advantage is temporary and comes to little unless fielded and leveraged at the speed of the next technology evolution. As new technology emerges, tactics are developed that use it. Then counter tactics are developed and technological parity is reached. And the cycle starts over again. The only way to get ahead and stay ahead is to be faster than our competitors. As our predecessors envisioned force multiplication as the key strategy for defeating the Soviet threat in Europe in the aftermath of WW II, we should aspire *to time compression as the key strategy of our generation*. Time compression means we can win the fight in a fraction of the time it would take to achieve the same objective otherwise. It means we control the time domain. We can speed up time when it suits us and we can slow down time when we need more time to achieve our objectives. And this certainly applies to imagining, creating and deploying innovation to secure the technological edge for our military.

In the struggle to achieve time compression and speed up time, our platforms matter. We need to *evolve our platforms from the monoliths they are today to agile, mosaic systems.* If we are successful we will be able to rapidly swap out components and always have the latest innovations deployed in our platforms. A lot has been said about doing over the air updates to the F-35. It may sound like science fiction but this is what happens every time your mobile phone gets an upgrade – so that you always have the latest and the greatest. Imagine a world where we can change the functionality of our platforms at such a dizzying rate that every morning our adversaries wake up and they are confronted with a brand new system and

capability against which they have 24 hrs to develop counter tactics. We just succeeded in slowing down time for them.

How could we get there? It has been said that bits eat atoms. *It's all about the software.* If we start thinking of the F-35 as an information appliance vs an airplane, the whole way we approach designing, building and maintaining it changes. We design it from the start to be software centric, modular and composable. In others words a mosaic vs a monolith. Increasing the software competency of our Defense S&T Enterprise and technology acquisition workforce is therefore at the heart of time compression.

A lot has been said about supply chains. In the Department of Defense we have worried for some time now about the trustworthiness of the supply chain for microelectronics for example. And as the Covid-19 pandemic has demonstrated our dependency on many other overseas supply chains is also a vulnerability. Building transparent, resilient and diverse supply chains is critical for our economy and our national security. But it also highlights the opportunity to not only innovate here at home but also to help create new businesses that translate the innovation into scalable domestic manufacturing. First because doing so reduces our dependency on potentially adversarial supply chains. Second because it creates good jobs here at home. Third, and perhaps most importantly, because unless we build and manufacture products right here in the United States, we will eventually lose our ability to innovate all together. A recent New York Times article by Noam Scheiber said it all:

"A 2012 book by the Harvard business professors Gary Pisano and Willy Shih made the case that when it comes to manufacturing, strength yields strength, and weakness yields weakness. They showed that the offshoring to Asia of the consumer-electronics industry, which executives believed was becoming too commoditized to be worth keeping entirely in the U.S., had weakened America's so-called industrial commons — the ecosystem of research, engineering and manufacturing know-how that creates innovative products. In effect, getting out of the business of making stereos and TVs in the 1960s and '70s made it harder for American manufacturers to produce more sophisticated technologies like advanced batteries. The Chinese, of course, took the other side of the bet — gaining know-how by starting with simpler products, which then led to the making of more sophisticated ones. That's partly why the China shock started with exports of products like textiles and steel and eventually included smartphones."

To ensure the future of our technology advantage *we must act to rebuild our industrial commons.*

Recommendations

People first

Everything starts with people. We need to nurture our S&T Enterprise technical community by protecting them from onerous bureaucracy, giving them the tools they need to do their work and offering them opportunities to grow their skills and careers. Hiring the best and the brightest starts early. We need to grow the DoD STEM workforce by investing in the next generation of our technical national security professionals by for example expanding programs such as the SMART scholarship program. We also need to increase the diversity of the DoD STEM workforce by broadening the recruitment pool in terms of expertise, background and location. And we need to create a diverse and inclusive environment where everyone is welcome and can succeed. Empowering the DoD technical community and giving technology a strong voice at the decision making table is key.

What we work on

As Peter Drucker once said, if you don't know where you are going, all roads will take you there. Absent a defense R&D strategy, it is impossible for the Defense Department to focus and prioritize its technology investments. When the Department had a clearly articulated overarching technology strategy in the 1950s and the late 1970s U.S. investments translated to dramatic and lasting superiority. Compiling a list of current technology investments does not constitute a strategy. The 2018 USAF 2030 S&T Strategy provides a good example of S&T strategy making. It starts with articulating a *vision:* an Air Force that dominates time, space, and complexity in future conflict across all operating domains to project power and defend the homeland. It then identifies *5 strategic capabilities*: Global persistent awareness, resilient information sharing, rapid, effective decision making, complexity, unpredictability and mass and speed and reach of disruption and lethality. And then identifies a non exhaustive list of underpinning technologies that may be needed to implement the strategic capabilities: Enabling microelectronics, quantum science, AI and autonomy, hypersonic flight amongst others. Looking beyond the usual suspects, key areas of focus in our R&D strategy making should include R&D for transforming manufacturing to rebuild our industrial commons (starting with microelectronics) and technologies for countering digital authoritarianism that undermines democracy around the world and here at home.

How we work

We need to give our DoD innovation engine a tune up. We can radically enhance the productivity of the S&T Enterprise workforce by killing a paper cut every day, starting by offering them a performant information technology infrastructure: cloud, modern software development and collaboration tools. We can speed up execution and open up the door to non traditional innovators by innovating in contracting and using granted authorities. As mentioned earlier, innovation needs to be executable by the entire organization.

How we have impact

An efficient and responsive defense Tech pipeline is essential in allowing the transition of innovation from the lab to the warfighter. Commercial product development relies on this pipeline and has developed best known methods such product management to bridge the gap between a technology and its consumers. *We need to migrate these best known methods into the way we develop and acquire technology in the DoD.* And we need to innovate in transition. Going beyond the often elusive transition of a technology directly into a program of record by, for example, creating and supporting new startups that can develop, mature and transfer the technology to the warfighter. DARPA's Embedded Entrepreneur Initiative and National Security Seed Fund are great examples of what can be accomplished within existing authorities.

Who we work with

We need to broaden our reach into the non traditional innovation community *by establishing a national security open innovation network*. The companies that came to define the technology context within which the military has to defend the nation today all hail from the West Coast, as do many other disruptors, such as Uber, Tesla, and SpaceX. It is no wonder then that Silicon Valley is teeming with company outposts from all over the world. Their objective: to gain visibility into talent and technologies they can acquire to further their interests. Open innovation is about building a presence in and bridges with innovation hubs, such as Silicon Valley and the Boston Corridor. The

S&T Enterprise (with the notable exception of DIU and In-Q-Tel) is mostly absent from these hotspots. The innovation muscle of the Defense Department lies in the defense vendor base, the defense laboratories, DARPA, and the various other defense R&D agencies. The lack of a physical, substantial, and enduring presence of the S&T Enterprise in Silicon Valley and the other national innovation hotspots means that we do not have eyes and ears on the ground when it comes to emerging technologies and talent in these areas. The consequence is a chronic isolation of the defense technology establishment from the very commercial innovation that U.S. competitors and adversaries exploit to build asymmetric technology advantage against our country.

In closing

It is perhaps fitting to conclude this testimony with the words of Charles Kettering to the U.S. Chamber of Commerce in 1929:

"I am not pleading with you to make changes. I am telling you you have got to make them – not because I say so, but because old Father Time will take care of you if you don't change. Advancing waves of other people's progress sweep over the unchanging man and wash him out. Consequently, you need to organize a department of systematic change-making."

Dr. Victoria Coleman

Dr. Victoria Coleman was the 22nd director of the Defense Advanced Research Projects Agency (DARPA).

Most recently, Coleman was a senior advisor on microelectronics technology policy to the director of the Center for Information Technology Research in the Interest of Society (CITRIS) at the University of California, Berkeley.

Before her time at Berkeley, Coleman was the CEO of Atlas AI P.B.C, a Silicon Valley startup that sought to apply AI solutions to sustainable development initiatives. By combining satellite data with other data sets, Atlas AI's proprietary deep learning models helped create actionable insights for clients across governments, NGOs, and commercial companies.

Prior to joining Atlas AI, Coleman was the CTO at the Wikimedia Foundation, the nonprofit organization that supports Wikipedia. At Wikimedia she oversaw the organization's technology department and technical roadmap, and was responsible for the evolution, development, and delivery of core platforms and architecture. In this role, Coleman worked to ensure an accessible and performant technology infrastructure and anticipate scale and capability challenges for Wikimedia projects.

Throughout Coleman's expansive career she has held a series of senior positions at leading technology companies, including: Technicolor, Harman International, Yahoo!, Nokia, Hewlett Packard, Samsung, Intel, and SRI International.

Coleman joined SRI International in 1998 after serving 10 years as a tenured professor at the University of London. She also completed her undergraduate and graduate work in the United Kingdom, earning her B.Sc and M.Sc degrees at the University of Salford and her Ph.D. in computer science from the University of Manchester.

Coleman is a former member of the Defense Science Board, as well as a member and founding chair of DARPA's Microsystems Exploratory Council. In addition, she served in an advisory capacity to Airbus Industries Starboard, Lockheed Martin's Technology Advisory Group, and Santa Clara University's Advisory Board for the department of Computer Engineering. She also sat on the board of directors of the Public Library of Science.

DISCLOSURE FORM FOR WITNESSES
COMMITTEE ON ARMED SERVICES
U.S. HOUSE OF REPRESENTATIVES

INSTRUCTION TO WITNESSES: Rule 11, clause 2(g)(5), of the Rules of the House of Representatives for the 117th Congress requires nongovernmental witnesses appearing before House committees to include in their written statements a curriculum vitae and a disclosure of the amount and source of any federal contracts or grants (including subcontracts and subgrants), and contracts or grants (including subcontracts and subgrants), or payments originating with a foreign government, received during the past 36 months either by the witness or by an entity represented by the witness and related to the subject matter of the hearing. Rule 11, clause 2(g)(5) also requires nongovernmental witnesses to disclose whether they are a fiduciary (including, but not limited to, a director, officer, advisor, or resident agent) of any organization or entity that has an interest in the subject matter of the hearing. As a matter of committee policy, the House Committee on Armed Services further requires nongovernmental witnesses to disclose the amount and source of any contracts or grants (including subcontracts and subgrants), or payments originating with any organization or entity, whether public or private, that has a material interest in the subject matter of the hearing, received during the past 36 months either by the witness or by an entity represented by the witness. Please note that a copy of these statements, with appropriate redactions to protect the witness's personal privacy (including home address and phone number), will be made publicly available in electronic form 24 hours before the witness appears to the extent practicable, but not later than one day after the witness's appearance before the committee. Witnesses may list additional grants, contracts, or payments on additional sheets, if necessary. Please complete this form electronically.

Hearing Date: 2/23/2021

Hearing Subject:

Innovation Opportunities and Vision for the Science & Technology Enterprise

Witness name: Victoria Coleman

Position/Title: Senior Advisor to the Director at CITRIS & the Banatao Institute, University of California Berkeley; Former Director of DARPA

Capacity in which appearing: (check one)

● Individual ○ Representative

If appearing in a representative capacity, name of the organization or entity represented:

Federal Contract or Grant Information: If you or the entity you represent before the Committee on Armed Services has contracts (including subcontracts) or grants (including subgrants) with the federal government, received during the past 36 months and related to the subject matter of the hearing, please provide the following information:

2021

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant

2020

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
Atlas AI Grant	National Science Foundation	$999,805	SBIR Phase II: Instance Segmentation

2019

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
ATLAS AI Grant	National Science Foundation	$224,943	SBIR Phase I: Instance Segmentation
ATLAS AI Contract	DARPA (Sub to Kimetrica)	$948,956	World Modelers Program

2018

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant

Foreign Government Contract, Grant, or Payment Information: If you or the entity you represent before the Committee on Armed Services has contracts or grants (including subcontracts or subgrants), or payments originating from a foreign government, received during the past 36 months and related to the subject matter of the hearing, please provide the following information:

2021

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment

2020

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment

2019

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment

2018

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment

Fiduciary Relationships: If you are a fiduciary of any organization or entity that has an interest in the subject matter of the hearing, please provide the following information:

Organization or entity	Brief description of the fiduciary relationship
CITRIS, UC Berkeley	Advisor to the Director on Microelectronics
Lockheed Martin	Member of the Technology Advisory Group to the CTO
LookingGlass	Advisor
DARPA	Director
Atlas AI, PBC	CEO

Organization or Entity Contract, Grant or Payment Information: If you or the entity you represent before the Committee on Armed Services has contracts or grants (including subcontracts or subgrants) or payments originating from an organization or entity, whether public or private, that has a material interest in the subject matter of the hearing, received during the past 36 months, please provide the following information:

2021

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
Salary	DARPA	$10,563	Director compensation

2020

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
Salary	DARPA	$30,776	Director compensation
Consulting fees	Lockheed Martin	$161,661	Technology advice
Salary	Atlas AI	$ 296,335	CEO compensation

2019

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
Consulting fees	Lockheed Martin	$29,361	Technology advice
Salary	Atlas AI	$229,166	CEO compensation

2018

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
Consulting fees	Lockheed Martin	$60,915	Technology advice

AMERICAN ENTERPRISE INSTITUTE

Statement before the House Committee on Armed Services
Subcommittee on Cyber, Innovative Technologies, and information Systems
On Innovation Opportunities and Vision for the Science and Technology Enterprise

Creating a More Agile and Secure Defense Innovation Base

Mr. Klon Kitchen
Resident Fellow

February 23, 2021

Introduction
Good afternoon Chairman Langevin, Ranking Member Stefanik, and members of the subcommittee. Thank you for this opportunity to testify.

There is good reason for the United States and its citizens to be optimistic about our future. Our technology and innovation industries remain the envy of the world – pioneering technological discoveries and applications that are the foundation of our national prosperity and security.

These advantages, however, are not inevitable and deliberate action is required for the United States to maintain its leadership and to protect its people and interests. I would like to briefly describe two features that should define our policies going forward.

The Strategic Context

First, we must understand how and why the technology sector of our economy is growing in influence and importance within military and national defense decision making.

National security is a team sport – and not just among America's myriad government departments and agencies. While the United States Constitution makes the federal government responsible for ensuring the "common defense" of the nation, individual citizens, civil society groups and private companies have always helped shoulder this burden. This remains unchanged.

What is changing is the distribution of this burden among these stakeholders – particularly private companies.

The technologies that will determine the United States' ability to secure its people and interests are overwhelmingly being developed for commercial purposes in the private sector. It is highly unlikely the government will create its own, distinct capacity to create and distribute these technologies in the near- to mid-term.

This leaves the national defense more dependent on the private sector than ever before, precisely as China is emerging as a true-peer competitor and rival economically, technologically, and militarily.

China also recognizes this migration of the national security burden into the private sector and is responding with what its leaders call "military-civil fusion." This is a form of governance where the Chinese Communist Party (CCP) co-opts Chinese companies and employs them as an extension of the state's political, economic, military, and intelligence enterprises.

This, for example, is the root of Western concerns with Huawei: the potential for a Chinese telecommunications behemoth that has used government subsidies to dramatically undercut Western competitors to build a monopoly over infrastructure that – under Chinese law – could be used as a global surveillance network for Beijing.

All of this adds up to an unavoidable truth: the ability of the United States to invent, design, build, deploy and secure advanced technologies – and their key components – is as important to national security as the nation's capacity to field traditional military capabilities. With this in mind, it follows that new partnerships between the government and industry are essential.

That's not to say the United States should try to "out China" China. America's model of non-coercive private-public cooperation is agile, productive, and fair. But this model only works when partnerships between the government and the free market are voluntary. Naturally, this requires technology firms to act from a shared sense of responsibility – a shared sense that was understandably undermined by a number of events, most notably the illegal disclosures of NSA contractor Edward Snowden. That was seven years ago. We have to move on and we have to do better.

It's not all bad news. Despite these challenges, the world's largest, most profitable and most innovative technology companies are still American companies. While Chinese tech firms are catching up (and fast), the U.S. still holds the advantage. But it is time to use it or lose it.
This requires two adjustments.

The government, for its part, must accept the reality that it is *a* national security stakeholder and not *the* stakeholder. Many of the world's leading technology companies have global interests and influence on par with many nations – they have a legitimate place at the geopolitical table. This isn't hyperbole. Apple's annual revenue exceeds the GDP of Portugal.

This shift in perspective will be as important as our efforts to devise new applications and tactics for employing new capabilities. As my colleague Kenneth Pollack observes:[i]

> The world is shifting from the industrial age to the information age. That transformation has profound implications for warfighting. In the most obvious fashion, new technologies will have a direct impact on combat operations, transforming what is possible and how best to accomplish military ends. However, major technological shifts also exert an indirect impact on military affairs by transforming other aspects of society that will in turn dictate the organization, resources, goals, abilities, and constraints that nations and other groups bring to warfare. As it always does, technology is reshaping economies, political systems, cultures, and organizations of every kind. Although these indirect effects are often less obvious, they are typically no less important.

More concretely, Washington can best demonstrate its intent to be a true partner with the tech industry in the way it shares information and acquires new capabilities.

For too long, the U.S. government has treated information exchange with industry as a one-way street – demanding "real-time" information sharing from private companies on cybersecurity and other threats while being painfully slow in sharing with industry its own insights about malicious actors, their intentions and their capabilities.

This posture increasingly means that it is the government, not industry, who is being left behind. It was the private sector, after all, who discovered and alerted officials to the massive "Holiday Bear" supply chain attack (aka, the SolarWinds attack) that compromised hundreds of public and private networks – the impact of which we still no not fully understand.

There are early signs this might be changing. The NSA's release of its Ghidra tool is a good example of the government proactively treating industry as a partner. This software reverse engineering framework was developed by Fort Meade for the NSA's national security mission, but its release to the public allows private sector security personnel to better defend themselves as well.

Likewise, when Cyber Command publishes fresh malware samples used by U.S. adversaries in public

repositories, it democratizes access to information all network defenders need to protect themselves.

Less progress is being made in government purchasing and procurement, where a rigid and outdated acquisition bureaucracy makes it difficult for new technology companies to help Washington. Tech companies thrive when they spend precious resources on engineers and coders, not on hordes of contract specialists and lawyers.

Organizations like the Pentagon's Defense Innovation Unit and the CIA's In-Q-Tel are good at technology scouting and at strategic investment. But we still struggle to transition these technologies from niche experimental programs into stable, long-term solutions.

None of these very real frustrations with the government excuse tech companies from the responsibilities that come with their growing global influence.

It is precisely because they are amassing this power and influence, and because they are enabled to do so only under the military, legal, and economic protections of the U.S. government, that these companies must also change.

Specifically, American technology companies must acknowledge their growing national security responsibilities. They must also accept the fact that Great Power competition is returning and that this return requires them to choose sides.

While the Chinese market may be lucrative, it is also a moral minefield and ultimately a dead end for Western companies. American companies' submission to Beijing's predatory demands on intellectual property, proprietary information, trade secrets, data, and other assets weakens American economic competitiveness, individual and national cybersecurity, and broader national security to the degree that this capitulation enables China's technological ascendance over the U.S. This participation also gives cover to Beijing's rampant political oppression and human rights violations.

The business risk is extreme, too. China has a proven record of allowing U.S. companies to take part in their market for only as long as is required to pilfer their intellectual property and secrets. Once these are sufficiently harvested, Beijing caps the companies' market presence and prioritizes domestic competitors that have been built with the information stolen from American firms.

Consider the experience of Microsoft: back in 2018, some 90 percent of Chinese firms used the company's operating system, but only 1 percent actually paid for it. This, according to former Microsoft CEO Steve Ballmer, cost the company more than $10 billion in profits.[ii] But, thus far, such losses have been accepted as the cost of doing business in what, until recently, was the world's fastest growing market.

Companies that chase short-term profits in the Chinese market over long-term stability are in for a rude shock.

Ultimately, western technology companies and the U.S. government must recognize that the long-term interests of both are better served through national security partnerships. They should do this out of patriotism, out of economic interest, and because these partnerships enable the expansion of truly free markets and human thriving around the world.

The time for rhetoric has passed. We don't need another study or another commission. Instead, the United States – its government, industry, and civil society – must establish a consensus on, and shared commitment to, our national security. This requires new levels of cooperation and mutual support.

Nowhere is this cooperation needed more than in the arena of defense innovation and acquisition.

Agile and Secure Acquisition

The second defining feature of any successful defense innovation policy, will be a more agile and secure technology acquisition system.

American military superiority is essential, but it is not inevitable. It is the result of strategic planning, deliberate investment, and an industrial base that is able to anticipate and deliver the capabilities needed to fight and win wars. We've made significant progress but a recent report shows that our defense industrial base is falling behind.

The National Defense Industrial Association (NDIA) gives the U.S. defense industrial base a "C" grade and says it is getting worse. "The defense industrial base is increasingly struggling to meet the 'unprecedented' challenges it faces," the NDIA concludes.

In the new report mentioned above, *Vital Signs 2020: The Health and Readiness of the Defense Industrial Base*, nearly 20 experts reviewed eight different dimensions shaping the capabilities of defense contractors and came away with the following judgments[iii]:

- The overall composite score for the industrial base was 77 points, just over the passing grade of 70 points and a decline of two points from 2018;
- Scores for three dimensions – production inputs, industrial security, and supply chain – fell below 70 points;
- Composite scores for four of the eight dimensions declined from 2018 to 2019; and,
- The lowest scoring dimension was industrial security, with a score of 63.

It is clear that national security leaders recognize the new era of great power competition requires significant and sustained investment in military capabilities, but the nation's defense industrial base is not ready to meet these challenges.

A decline in innovation is of particular concern. According to the NDIA report, innovation received a score of 74 for 2019, down two points from the previous year.
In a time where emerging technologies will define the battlefield, the U.S. cannot settle for a "passing grade" in developing, acquiring, and deploying these innovations. We have to dominate.

Such domination requires alternative partners, reduced bureaucracy and regulations, and industrial security.

Our current defense contractors are essential for key capabilities, especially marque platforms like aircraft carriers, fifth-generation jets, and modern fighting vehicles. But they are not typically the source

of bleeding-edge developments in artificial intelligence, advanced robotics, or quantum computing. These advancements are overwhelmingly developed by companies who do not regularly work with the department of defense and who are not currently trying to solve defense challenges.

These companies' lack of involvement is not due to a lack of patriotism. It is the result of poor incentives and massive bureaucratic hurdles. It is time to clear the way for these alternative partners so that our national security can profit from their agility, creativity, and expertise.
We can make dramatic improvements by making three key changes.

First, we need to recognize and employ new incentives. The current system does not prioritize the best available technology. Instead, it favors cost accounting, regulatory compliance, and administrative ease. Budgets are programmed years in advance with little ability for companies to realize profits in current fiscal years. And, perhaps most significantly, research and development are often spread across many small contracts instead of investing deeply in key or promising capabilities.

Encouraging a diverse ecosystem of innovation is wise only if it regularly produces the capabilities you need when you need them. Ours is not.

Generally speaking, innovative companies in the technology sector do not need government "investment," they need government contracts. There is plenty of venture capital in the United States; but those dollars only follow markets where there is a real opportunity for profits. These companies need real contracts, not one-off awards, and they need to know that these contracts can be scaled into real programs of record. Do this, and the defense innovation market place will boom. While some progress is being made using "other transactional authorities," these efforts need to be greatly expanded.

The second critical action is to get rid of the innovation killing regulatory burdens that block the partners we need.

The Federal Acquisition Regulation (FAR) — which governs all federal acquisitions, including those of the Department of Defense — is more than 2,000 pages long and even includes a definition on what constitutes a "copier." Certainly, rules need to be in place to ensure the U.S. government gets its money's worth and that taxpayers are treated fairly. But this bloated framework is a massive hurdle for companies who want to have more programmers and engineers than they have lawyers and contract officers.

There is ongoing effort to update FAR, but it is progressing too slowly, and it must take the nation's innovation needs as a central concern.

Finally, the U.S. should prioritize the security of our domestic technological and manufacturing capabilities. Do not forget, it was industrial security that was the lowest scoring dimension in the NDIA report.

This is not a call for economic protectionism – U.S. companies are very competitive – it is a call for commonsense security.

In a world where securing nations means securing networks and supply chains, it is unavoidably true that the loyalties and security practices of those creating and building our defense innovations matters.

This is part and parcel of developing and maintaining the American defense base in general. As the ongoing European capitulation to China's Huawei telecommunications company demonstrates, the lack of a robust and secure domestic technology industry leaves governments in desperate straits with few good options.

The United States should never accept such outcomes.

In the final analysis, American policymakers and citizens should be encouraged, but also feel a sense of urgency. Our industrial base is still the envy of the world, and U.S. emerging technology innovators are second to none. But, if the United States is going to secure its people and its interests going forward, we must do better in leveraging and securing these engines of innovation.

---

[i] Pollack, K. (2019, November). Society, Technology, and Future Warfare. Retrieved February 18, 2021, from https://www.aei.org/wp-content/uploads/2019/11/Society-technology-and-future-warfare.pdf?x91208

[ii] Limitone, J. (2018, November 01). China is ripping off Microsoft to the tune of $10B. Retrieved February 18, 2021, from https://www.foxbusiness.com/business-leaders/china-is-ripping-off-microsoft-to-the-tune-of-10b

[iii] National Defense Industrial Association, (2020, February 10). Vital Signs 2020: The Health and Readiness of the Defense Industrial Base. Retrieved February 18, 2021, from https://www.ndia.org/-/media/vital-signs/vital-signs_screen_v3.ashx?la=en

Klon Kitchen
Resident Fellow, American Enterprise Institute

Klon Kitchen is a resident fellow at the American Enterprise Institute (AEI), where he focuses on the intersection of national security and defense technologies and innovation. Through his research, he works to understand and explain how emerging technologies are shaping modern statecraft, intelligence, and warfighting, while focusing on cybersecurity, artificial intelligence, robotics, and quantum sciences.

Before joining AEI, Mr. Kitchen was director of the Heritage Foundation's Center for Technology Policy, where he led an enterprise-wide, interdisciplinary effort to understand and shape the nation's most important technology issues.

Before joining Heritage, Mr. Kitchen was national security adviser to Sen. Ben Sasse (R-NE) and worked on the creation of the US Cyberspace Solarium Commission, a blue-ribbon commission tasked with developing an American grand strategy for cyber. While working for Sen. Sasse, Mr. Kitchen served as the staff director of the National Security and International Trade and Finance Subcommittee for the Senate Committee on Banking, Housing, and Urban Affairs.

Mr. Kitchen has also worked on cyber strategy at the National Counterterrorism Center; as a senior program assessment officer at the Office of the Director of National Intelligence in the Office of the Director of Central Intelligence; and as the lead analyst on al Qaeda senior leadership at the Defense Intelligence Agency. He was also the National Counterterrorism Center chair at National Defense University.

A popular speaker, Mr. Kitchen has appeared on "60 Minutes" on CBS News and The New York Times podcast "The Argument." He has also been published in RealClearDefense, The Hill, The National Interest, The Telegraph, Washington Examiner, and National Affairs, among other outlets.

Mr. Kitchen has an MA in strategy and security studies from the College of International Security Affairs and a War College Diploma in security strategy and irregular warfare from the National War College, both from National Defense University. His BA in biblical studies is from Bryan College.

Experience

- The Heritage Foundation: Director, Center for Technology Policy, 2020; Senior Fellow, Technology, National Security, and Science, 2018–20
- United States Senate, Office of Sen. Ben Sasse (R-NE): National Security Adviser; Staff Director, National Security, International Trade, and Finance Subcommittee, Senate Committee on Banking, Housing, and Urban Affairs, 2015–18
- National Counterterrorism Center: Cyber Strategy and Planning, 2013–15; Chief, Extremist Messages and Influence, 2007–10
- National Defense University: Chair, National Counterterrorism Center, 2010–13
- Office of the Director of Central Intelligence: Senior Program Assessment Officer, Office of the Director of National Intelligence, 2005–07
- Defense Intelligence Agency: Lead Analyst, Al Qaeda Senior Leadership, 2002–05

Education

MA, strategic security studies, College of International Security Affairs and War College Diploma, security strategy and irregular warfare, National War College, National Defense University
BA, biblical studies, Bryan College

DISCLOSURE FORM FOR WITNESSES
COMMITTEE ON ARMED SERVICES
U.S. HOUSE OF REPRESENTATIVES

INSTRUCTION TO WITNESSES: Rule 11, clause 2(g)(5), of the Rules of the House of Representatives for the 117th Congress requires nongovernmental witnesses appearing before House committees to include in their written statements a curriculum vitae and a disclosure of the amount and source of any federal contracts or grants (including subcontracts and subgrants), and contracts or grants (including subcontracts and subgrants), or payments originating with a foreign government, received during the past 36 months either by the witness or by an entity represented by the witness and related to the subject matter of the hearing. Rule 11, clause 2(g)(5) also requires nongovernmental witnesses to disclose whether they are a fiduciary (including, but not limited to, a director, officer, advisor, or resident agent) of any organization or entity that has an interest in the subject matter of the hearing. As a matter of committee policy, the House Committee on Armed Services further requires nongovernmental witnesses to disclose the amount and source of any contracts or grants (including subcontracts and subgrants), or payments originating with any organization or entity, whether public or private, that has a material interest in the subject matter of the hearing, received during the past 36 months either by the witness or by an entity represented by the witness. Please note that a copy of these statements, with appropriate redactions to protect the witness's personal privacy (including home address and phone number), will be made publicly available in electronic form 24 hours before the witness appears to the extent practicable, but not later than one day after the witness's appearance before the committee. Witnesses may list additional grants, contracts, or payments on additional sheets, if necessary. Please complete this form electronically.

Hearing Date: February 23, 2021

Hearing Subject:

Innovation Opportunities and Vision for the Science and Technology Enterprise

Witness name: Klon Kitchen

Position/Title: Resident Fellow, American Enterprise Institute

Capacity in which appearing: (check one)

● Individual ○ Representative

If appearing in a representative capacity, name of the organization or entity represented:

NA

Federal Contract or Grant Information: If you or the entity you represent before the Committee on Armed Services has contracts (including subcontracts) or grants (including subgrants) with the federal government, received during the past 36 months and related to the subject matter of the hearing, please provide the following information:

2021

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
NA			

2020

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
NA			

2019

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
NA			

2018

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
NA			

Foreign Government Contract, Grant, or Payment Information: If you or the entity you represent before the Committee on Armed Services has contracts or grants (including subcontracts or subgrants), or payments originating from a foreign government, received during the past 36 months and related to the subject matter of the hearing, please provide the following information:

2021

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment
NA			

2020

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment
NA			

2019

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment
NA			

2018

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment
NA			

Fiduciary Relationships: If you are a fiduciary of any organization or entity that has an interest in the subject matter of the hearing, please provide the following information:

Organization or entity	Brief description of the fiduciary relationship
NA	

Organization or Entity Contract, Grant or Payment Information: If you or the entity you represent before the Committee on Armed Services has contracts or grants (including subcontracts or subgrants) or payments originating from an organization or entity, whether public or private, that has a material interest in the subject matter of the hearing, received during the past 36 months, please provide the following information:

2021

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
NA			

2020

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
NA			

2019

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
NA			

2018

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
NA			

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

FEBRUARY 23, 2021

QUESTIONS SUBMITTED BY MR. LANGEVIN

Mr. LANGEVIN. Can you talk about the role of user feedback in innovation and adoption? How do you think a tighter partnership between the operational military forces and the S&T community can best be achieved?

Ms. FOX. Chairman Langevin, thank you for this important question. Feedback in innovation and adoption is essential, in my view. Innovations that cannot be used in an operational environment are not valuable. Similarly, operators who are blind to the advantages of new technologies will neglect to make game-changing advancements. When the partnership between the operational military forces and the S&T/R&D community has been strong, it has produced game-changing results. A notable example is the adoption of stealth and precision that led to significant operational advantages dating back to Desert Storm. The U.S. Air Force set up an internal organization called "Checkmate," in which dedicated creative operators determined how to best use these emerging technologies. Today, this partnership is more important than ever and needs to be strengthened. The technologies being developed today are not evolutionary upgrades of existing capabilities but, rather, entirely different from anything we have had access to before. We need to educate the operators on the potential power of these new technologies. We need to educate the developers on the operational needs and opportunities the technologies can fulfill.

Liaison assignments might be able to help. Scientists living with operators and operators assigned to S&T/R&D organizations can expand the understanding of what is needed and what is possible. Technical exchange conferences can help as well. For example, once the Strategic Capabilities Office (SCO) began to hold technical exchange meetings with the IndoPacific Command, the resulting partnership helped guide SCO's activities and solidified their value. That is near-term R&D, but the same idea can be used for S&T. These technical exchanges do happen, but not often enough or deeply enough to build tech-infused concepts of operation or to focus tech development in critically important areas. Another approach is to increase the focus of experimentation on the integration of S&T/R&D advancements into operational challenges. Experimentation with new technologies will help operators envision new concepts for their use. Additional resources focused toward fostering a closer partnership between S&T developers and operators would help make this a reality.

QUESTIONS SUBMITTED BY MR. MOULTON

Mr. MOULTON. I appreciated your comments about grounding new technologies in operational reality, and vice versa. It seems that a critical part of that would come from training our forces to leverage new technologies and integrate them into their concepts of operation. Based on your previous experience at DOD, did you get the sense that the Services were adequately integrating new technologies and concepts of operations into their training and education? Do you have the sense of whether they are adequately doing that now?

Ms. FOX. Thank you for this question, Congressman Moulton. The new technologies envisioned today have the potential to completely change the way the military operates. As a result, it is very difficult to integrate new technology into training and education. This is what we call the "here-to-there" problem at the Johns Hopkins Applied Physics Lab. The force must be ready to meet any challenge thrown at it today and, therefore, training and education is rightly focused on today's capabilities and concepts of operation.

A key challenge is that the new technologies envisioned for tomorrow are radically different. To explore the potential of artificial intelligence, autonomous systems, zoomorphic robots, biology-based sensors, brain-controlled drones, and more, we need dedicated events that place operators into a future world with these future capabilities. This is likely to require virtual interactive environments tied to advanced digital engineering and modeling and simulation efforts that are integrated with prototypes as they become available. These dedicated experiments are important if we are to develop concepts of operation that can take advantage of these potentially game-changing technologies.. They could occur on enhanced test ranges or within the government-funded R&D labs or both.

Mr. MOULTON. Last year I co-led the Future of Defense Task Force, which was a bipartisan effort to identify the hard choices and smart investments necessary to secure our future competitive advantage. In our months of interviews and research,

we frequently faced the challenge of investing in the future while managing platforms of the past. We looked at current and future budget constraints and ultimately concluded that it would be necessary to divest of some legacy systems to make room for the next generation of technology. In Dr. Coleman's testimony, she noted that we need to "evolve our platforms from the monoliths they are today to agile, mosaic systems." Do you believe that ALL platforms can and should be carried forward into a new era of warfare? Are all the platforms designed for conflicts of decades past still appropriate to address the threats of the future?

Dr. COLEMAN. The essence of mosaic systems and platforms is that they are modular, compositional and able to be assembled in fit-for-purpose force packages just in time. This then calls for a set of diverse platforms and components to be available. I believe that it is not possible for a single, multi-purpose platform to meet all mission needs. This mixture of platforms will include manned and unmanned aircraft. As we look at the mix of capabilities, and as older platforms are retired, we should be laser focused on replacing them with modular, easily upgradeable capabilities. And at the same time we should be investing to modernize and upgrade our software development and deployment infrastructure to take advantage of these new platforms that would be capable of over the air updates including test ranges to support incrementally developed, tested and fielded capabilities.

Mr. MOULTON. As a veteran who has served overseas and faced some very real threats to our nation, I believe that every person in this country must have a vested interest in national security. But the reality of these threats sometimes aren't clear to everyone—the importance of national security is clear to everyone who took part in this hearing, but it often doesn't seem like a compelling business case for companies considering investments or clients in China. How can we show companies that it is worth thinking about national security implications in their everyday activities, either for investment screening or cybersecurity practices or anything else?

Mr. KITCHEN. The very best thing Congress can do to raise general national security awareness on these issues is to speak clearly and regularly on these issues. Beyond this, increasing coordination and general information sharing between the federal government, state and local governments, and private industry will be essential. Continuing to refine and to expand the prevue and expertise of the Committee on Foreign Investment in the United States (CFIUS) will also be critical. The recent CFIUS reforms were largely well-received; however, it will be necessary to continue this refinement if the organization is to remain relevant and engaged on the most important emerging technologies.

QUESTIONS SUBMITTED BY MR. MOORE

Mr. MOORE. I understand the Air Force has been examining legacy programs and trying to accelerate the retirement of programs that won't contribute significantly in the 2030–2038 timeframe. What are the greatest challenges in expediting the retirement of legacy programs to re-invest in next generation technologies?

Ms. FOX. Congressman Moore, thank you for this question. I experienced two challenges when attempting to expedite the retirement of legacy programs. The first was that many of these capabilities were in constant demand, so the operational need outweighed the benefit of early retirement. There is a significant time delay between initial investment in next-generation technologies and their availability for actual use. As long as there is a great need for deployed military forces, this gap is a deterrent to early retirement of legacy systems.

There are, however, some capabilities that the military services and DOD leadership would like to retire early. Some examples from my time in government include the A–10 and Navy cruisers. While these platforms still provided operational value, there were more modern alternatives that cost much less to operate and maintain. In each case, despite strong evidence that the military could perform its missions without these platforms, Congress, at that time, overruled DOD and forced the Department to retain these platforms. Congressional interests and constituency pressure are factors the Department must face when attempting to retire legacy platforms.

Mr. MOORE. Utah is home to the Utah Test and Training Range, the nation's largest overland restricted airspace. This Major Range and Test Facilities Base provides capabilities critical to support of next generation technologies and the DOD acquisition system. How should the department modernize and invest in this infrastructure that supports the training and integration of next generation technologies?

Ms. FOX. Thank you, Congressman Moore. The Utah Test and Training Range, with its large area and extensive high-altitude restricted airspace, provides a vital ability to test and experiment with current and new technologies. I am not current

on the status of test ranges; however, in the past these ranges have been under constant pressure to reduce operations from nearby communities and civilian airspace control. In my view, it is vitally important to protect these ranges and their capabilities. Beyond protection from encroachment, to adequately test new technologies, I believe we will need some new capabilities and, possibly even new policies. AI-enabled autonomous systems, for example, have the risk of straying out of approved test areas. Technologists are working hard, and are making progress, to effectively control these new technologies, but upgrades to ranges could be necessary to enable them. Additionally, as operational ranges and altitudes continue to expand, we will need to incorporate more detailed modeling and simulation capabilities, to include augmented reality/virtual reality (AR/VR) technologies, in order to fully test and experiment with some of the next-generation technologies.

Mr. MOORE. During your time at DARPA, did special hiring authorities give you the ability to recruit and retain top tier talent? What changes can the department pursue to improve personnel authorities?

Dr. COLEMAN. DARPA hires personnel using two authorities: 1121 and IPA. It is tremendously important that DARPA's hiring authorities are not only preserved but also continually reviewed for enhancement. The hiring authorities are often under attack from those who would prefer a "one size fits all" approach. That would be nothing short of disastrous for the Agency. The authorities must be preserved and expanded so that their benefits don't fall too far behind the private sector.

1121: This is perhaps the most widely used authority at DARPA. It works well for two types of people: those who are already employed by the government and/or those who live in the DC metro area. People that do not work for the government are not eligible for full relocation benefits. So on top of very often asking them to take a pay cut, we also ask them to self finance their move to Washington. This obviously acts as a powerful disincentive for technical talent outside the government and the DC metro area for joining the Agency. Adding a statement to the 1121 language that DARPA employees appointed under the authority will be considered as current government employees for the purposes of the Joint Travel Regulations would be a huge recruiting tool.

IPA: Extending the same relocation benefit as above to those hired under the IPA authority and/or offering full per diem for those who choose not to move for the duration of their service would offer much needed flexibility to those who want to serve so that they can select which option works best for them and their families.

DARPA does not currently have any HQE allocations. When the HQE authority was first created, DARPA had 60 regular allocations. At its inception the authority was delegated from SecDef to the defense agencies. However OSD/WHS rescinded the delegation of the HQE direct hiring authority in September 2012. The significant delays this introduced were of the order of several months and the authority became no longer viable as it resulted in loss of expediency to hire. Legislating the HQE authority directly to the DARPA Director (as is 1121) would offer the Agency an extremely valuable tool to recruit senior talent.

While it is true that nobody joins DARPA for the financial benefits, and it will always offer less than what the private sector can provide, every little bit helps and allows the Agency to target the critical technical talent we need to secure our national security technology advantage

Mr. MOORE. Back in my district, Hill Air Force Base and Utah's defense community consistently rank a highly competitive hiring atmosphere and the ability to find and retain talent as one of their greatest challenges. Do you share any concerns about the health and quality of the DOD STEM workforce and how can government programs better compete with private industry?

Mr. KITCHEN. Congressman Moore, I do share your concerns regarding the nation's STEM workforce—in the Department of Defense and elsewhere in the government. There have been several attempts to "attract and retain" STEM expertise into government service; however, until the U.S. government is able to pay, train, and use this expertise as well as the private sector (or at least close to these standards while providing a sufficiently motivating mission), there is little reason to believe the government will achieve its STEM manpower goals. Even industry is unable to attract the level of American STEM expertise that is demanded by existing commercial needs. Add to this the complications of calcified bureaucracies and a near total lack of agility, the federal government is not well positioned to make meaningful progress on this front in the near- to mid-term.

○