[H.A.S.C. No. 115–111]

MILITARY TECHNOLOGY TRANSFER: THREATS, IMPACTS, AND SOLUTIONS FOR THE DEPARTMENT OF DEFENSE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

HEARING HELD
JUNE 21, 2018

U.S. GOVERNMENT PUBLISHING OFFICE
33–384 WASHINGTON : 2019

COMMITTEE ON ARMED SERVICES

ONE HUNDRED FIFTEENTH CONGRESS

WILLIAM M. "MAC" THORNBERRY, Texas, *Chairman*

WALTER B. JONES, North Carolina
JOE WILSON, South Carolina
FRANK A. LOBIONDO, New Jersey
ROB BISHOP, Utah
MICHAEL R. TURNER, Ohio
MIKE ROGERS, Alabama
BILL SHUSTER, Pennsylvania
K. MICHAEL CONAWAY, Texas
DOUG LAMBORN, Colorado
ROBERT J. WITTMAN, Virginia
DUNCAN HUNTER, California
MIKE COFFMAN, Colorado
VICKY HARTZLER, Missouri
AUSTIN SCOTT, Georgia
MO BROOKS, Alabama
PAUL COOK, California
BRADLEY BYRNE, Alabama
SAM GRAVES, Missouri
ELISE M. STEFANIK, New York
MARTHA MCSALLY, Arizona
STEPHEN KNIGHT, California
STEVE RUSSELL, Oklahoma
SCOTT DESJARLAIS, Tennessee
RALPH LEE ABRAHAM, Louisiana
TRENT KELLY, Mississippi
MIKE GALLAGHER, Wisconsin
MATT GAETZ, Florida
DON BACON, Nebraska
JIM BANKS, Indiana
LIZ CHENEY, Wyoming
JODY B. HICE, Georgia
PAUL MITCHELL, Michigan
(Vacancy)

ADAM SMITH, Washington
ROBERT A. BRADY, Pennsylvania
SUSAN A. DAVIS, California
JAMES R. LANGEVIN, Rhode Island
RICK LARSEN, Washington
JIM COOPER, Tennessee
MADELEINE Z. BORDALLO, Guam
JOE COURTNEY, Connecticut
NIKI TSONGAS, Massachusetts
JOHN GARAMENDI, California
JACKIE SPEIER, California
MARC A. VEASEY, Texas
TULSI GABBARD, Hawaii
BETO O'ROURKE, Texas
DONALD NORCROSS, New Jersey
RUBEN GALLEGO, Arizona
SETH MOULTON, Massachusetts
COLLEEN HANABUSA, Hawaii
CAROL SHEA–PORTER, New Hampshire
JACKY ROSEN, Nevada
A. DONALD MCEACHIN, Virginia
SALUD O. CARBAJAL, California
ANTHONY G. BROWN, Maryland
STEPHANIE N. MURPHY, Florida
RO KHANNA, California
TOM O'HALLERAN, Arizona
THOMAS R. SUOZZI, New York
JIMMY PANETTA, California

JEN STEWART, *Staff Director*
TIM MORRISON, *Counsel*
WILLIAM S. JOHNSON, *Counsel*
JUSTIN LYNCH, *Clerk*

CONTENTS

MILITARY TECHNOLOGY TRANSFER: THREATS, IMPACTS, AND SOLUTIONS FOR THE DEPARTMENT OF DEFENSE

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
Washington, DC, Thursday, June 21, 2018.

The committee met, pursuant to call, at 10:01 a.m., in Room 2118, Rayburn House Office Building, Hon. William M. "Mac" Thornberry (chairman of the committee) presiding.

OPENING STATEMENT OF HON. WILLIAM M. "MAC" THORNBERRY, A REPRESENTATIVE FROM TEXAS, CHAIRMAN, COMMITTEE ON ARMED SERVICES

The CHAIRMAN. The committee will come to order. In his January 19, 2018, remarks on the National Defense Strategy, Secretary Mattis warned that, quote, "our competitive edge has eroded in every domain of warfare, air, land, sea, space, and cyberspace, and it is continuing to erode," end quote.

Now much of that erosion has been caused by things we have done to ourselves; sequestration and continuing resolutions come to mind. But part of the erosion in our competitive edge is the result of adversaries and competitors obtaining American technology and intellectual property by legal and often illegal means.

In its January 2018 report, China's Technology Transfer Strategy, DIUx [Defense Innovation Unit Experimental] found that the People's Republic of China, for example, uses a variety of methods to obtain U.S. technology, including industrial espionage, where China is by far the most aggressive country operating in the United States; cyber theft on a massive scale, deploying hundreds of thousands of Chinese Army professionals; academia, since 25 percent of U.S. STEM [science, technology, engineering, and math] graduate students are Chinese foreign nationals; China's use of open-source information, cataloging foreign innovation on a large scale; Chinese-based technology transfer organizations; U.S.-based associations sponsored by the Chinese government to recruit talent; and technical expertise on how to do deals learned from U.S. firms.

That report noted that the cost of stolen intellectual property has been estimated at $300 billion a year. Most alarming, DIUx found that—again, I will quote—"[t]he U.S. does not have a comprehensive policy or the tools to address this massive technology transfer to China," and "[t]he U.S. government does not have a holistic view of how fast this technology transfer is occurring, the level of Chinese investment in U.S. technology, or what technologies we should be protecting." That is the end of the quote.

Now I understand that the DIUx report is just one report, but based on everything this committee has learned and heard about over the course of this year, those conclusions sound right to me, and it should be alarming. There are several provisions in the upcoming NDAA [National Defense Authorization Act] conference which relate to this issue, including the modernization of CFIUS [Committee on Foreign Investment in the United States] and export control regime. This hearing will better equip us to make important decisions in the days ahead.

Let me yield to the ranking member for any comments he would like to make.

[The prepared statement of Mr. Thornberry can be found in the Appendix on page 39.]

STATEMENT OF HON. ADAM SMITH, A REPRESENTATIVE FROM WASHINGTON, RANKING MEMBER, COMMITTEE ON ARMED SERVICES

Mr. SMITH. Thank you, Mr. Chairman. I think the most important part of your statement was at the end there, is that we do not have a strategy to counter what is happening. I think the chairman is right and the Secretary of Defense is correct. Our advantage in a number of different areas has been eroding.

Now the biggest reason for that, I believe, is that the rest of the world is catching up. I mean, there was a substantial period of time there when it was really just the Soviet Union and us who were building, on a significant level, our military capacity. And we dominated the world economically and militarily post-World War II for a long period of time.

That was never going to last forever. The rest of the world was going to develop ways to grow their economies, grow their technology, and eventually turn towards growing their defense, and that is what has happened. But what has not happened on our end is we have not responded to that. Our strategy still seems to be based on the notion that we are still dominant, so we do not have to worry about these details, and I think that is dangerous and that we need to develop.

And I will just mention a couple of key areas, most of which the chairman mentioned. But to begin with, the CFIUS process of protecting our technology has long needed reform. Items that were not thought of as being national security are. Technology; how do we protect that? How do we make sure that adversaries are not purchasing those companies and taking away our technology?

I think what the Senate added to the defense bill is a great opportunity for us to update that process to help protect our technologies through the CFIUS process. And we have to get that right, and we are going to try to do that in the next 5, 6 weeks, so we definitely want to be in touch, make sure the language is right, make sure what we are doing in that part is correct.

The second piece of this is on the cyber piece, and we had a briefing yesterday on a cyber breach, and it was shocking how disorganized, unprepared, and quite frankly, utterly clueless the branch of the military was that had been breached. Even in this day and age, we still have not figured out how to put together a cyber policy to protect our assets. In particular, with our defense contractors, who

we work with, who store our data, but do not have adequate protection. But even within the DOD [Department of Defense], we do not have a clear, cohesive policy to put in place.

And the third area of policy we do not have is we do not have an industrial policy. And again, I think this is a legacy of our dominance. We did not have an industrial policy because we were dominant. In fact, an example from my own neck of the woods, Boeing. Why is Airbus able to be subsidized and competitive? Well because decades ago, we agreed to allow them, in many instances, to do that. And we did that because at the time, we had like 85 percent of the global aircraft manufacturing market, and we thought, well, is it not cute? Airbus wants to compete, whatever, it does not really matter to us. Well, here we are with that flipped. They have stepped up and competed.

And now, we have not come through with a sensible idea of what technologies, what industries do we need to protect for our own national security. As the chairman will relate, I do not think it is flatware, but that seems to be the one thing that we wind up debating in the NDAA every year. While, meanwhile—no offense to those in the part of the world who consider that important—but, you know, meanwhile, we are losing core technologies that are critical to defense and no one really understands exactly why.

The last piece of it, I will say, that I think is important, is trade. Now, we have a somewhat—I do not know what the word would be—unfocused approach right now to how we combat a competitive trade environment. The one thing we definitely should be doing is figuring out how to get on a more level playing field with China.

It is not just our trade deficit with China, but it is the strategies that they have put in place to capture core technologies, to steal them in some instances. But, a lot of it, they are doing within the WTO [World Trade Organization] framework. Some of it, they are doing outside of the WTO framework. But, we have not put together a comprehensive strategy for changing that equation, whether it is bringing trade actions against them, whether it is trying to get them to change their policies. It is sort of a reactionary approach right now. So, we need a strategy on this.

And, I think this hearing is incredibly important. I look forward to the testimony of witnesses. And I thank the chairman for convening it. I yield back.

[The prepared statement of Mr. Smith can be found in the Appendix on page 40.]

The CHAIRMAN. I thank the gentleman. I am pleased to welcome our witnesses today: the Honorable Michael Griffin, Under Secretary of Defense for Research and Engineering; Honorable Kari Bingen, Deputy Under Secretary of Defense for Intelligence; Mr. Eric Chewning, Deputy Assistant Secretary of Defense for Manufacturing and Industrial Base Policy; and Mr. Anthony Schinella, National Intelligence Officer for Military Issues. Thank you all for being here.

Without objection, your written statement, it looks like there is just one to me, will be made part of the record. And we will turn it over to you-all for comments you would like to make.

Mr. Schinella, I—or, you are starting first, is that? Oh, you all figure it out.

Secretary GRIFFIN. I——

The CHAIRMAN. Mr. Secretary. Go ahead if you would like.

Secretary GRIFFIN. I believe the earlier agreement was that I would start, sir.

The CHAIRMAN. Great.

STATEMENT OF HON. MICHAEL D. GRIFFIN, UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING, DEPARTMENT OF DEFENSE

Secretary GRIFFIN. So thank you first of all, Chairman Thornberry, Ranking Member Smith, members of this committee. We appear before you to discuss the very real Chinese adversarial behavior to which you have referred. And this is not about the threat of such behavior; this is real behavior.

We are here to underscore the urgency with which all of us must focus our actions to maintain our technological and military dominance. I thank you for the trust you have placed in myself and my fellow witnesses to discuss this topic in this open setting as carefully as we can.

We did—yes, sir, we did submit a single joint statement because we wanted to be together rather than separate. I think we have a common view of this topic. But our conversation today is only a handful of pixels in the entire picture of what we face. It is my and I believe, our deep belief that we must act now. But, at the same time, it is my duty to limit my comments to those of a strictly unclassified nature. So, as we go forward, I welcome, expect, and encourage more detailed discussions in a more restricted environment. I believe this will be necessary in the months and years ahead. This is not a problem with a short-term fix, sir.

We are here, in part, to recognize that this is a whole of government, indeed, a whole of society problem. And we are here, in part, to recognize and draw distinctions between adversaries and allies according to the behavior of the actor. No one believes more strongly than I, in the value of international partnerships and alliances, and in the value of international commerce and fair exchange.

But the Chinese theft of technology and intellectual property through the exfiltration of the work of others is not unlike the Chinese construction of islands to encroach upon the geographic domains of international waters and those of other sovereign nations. It circumvents the autonomy of nations in a departure from a rules-based global order. It is adversarial behavior and its perpetrator must be treated as such.

The breadth and depth of Chinese malfeasance with regard not only to our technology but also to our larger economy and our Nation is significant and intentional. As referenced in our written testimony, we are taking steps to counter it.

You, as the Congress, have established my office in particular to regain and maintain the technological dominance that we as a Nation have depended upon in the past. We pledge to you to do that; and, with your help and support, we will.

Thank you and I look forward to your questions. And I yield to my colleagues.

STATEMENT OF ANTHONY M. SCHINELLA, NATIONAL INTELLIGENCE OFFICER FOR MILITARY ISSUES, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Mr. SCHINELLA. Mr. Chairman Thornberry, Ranking Member Smith and all members of this distinguished committee, good morning and thank you for welcoming me here to discuss this important topic.

As the DNI's [Director of National Intelligence's] National Intelligence Officer for Military Issues, I am regularly tasked with reporting on threats to the U.S. military. There are, of course, the visible threats from foreign military forces and weapons systems. But the U.S. intelligence community also sees a less visible but dual threat from adversaries and competitors that are deliberately working to acquire U.S. research, technologies, and talent, to improve their own military programs and erode the effectiveness of ours.

More broadly, the IC [intelligence community] assesses that foreign countries' acquisition of U.S. technology through licit and illicit means, as well as cheating on trade agreements, joint ventures, and exploiting scientific collaborations, have the potential to erode the U.S. competitive edge. Foreign countries, most notably China, are able to acquire and transfer critical U.S. technology through their intelligence services, foreign direct investments, joint ventures, open-source science and technology acquisition programs, use of insiders, front companies, and scientific and business collaborations.

This has potentially far-reaching consequences. As we have highlighted in the DNI's annual threat testimony, persistent trade imbalances, trade barriers, and a lack of market-friendly policies in some countries probably will continue to challenge U.S. economic security. Some countries almost certainly will continue to acquire U.S. intellectual property and proprietary information illicitly to advance their own economic and national security objectives.

China, for example, has acquired proprietary technology and early-stage ideas through cyber-enabled means. At the same time, some actors use largely legitimate legal transfers and relationships to gain access to research fields, experts, and key enabling industrial processes that could, over time, erode America's long-term competitive advantages.

Foreign actors, notably China and Russia, recognize that investing in and acquiring technology is absolutely essential to achieve their strategic goals. They want to develop weapons systems that strike farther, faster, harder, and more precisely as a means to erode the traditional pillars of U.S. military strength and challenge the United States in all warfare domains.

This pursuit of advanced weapons systems could lead to new means of warfare, especially robotic and autonomous systems operating across land, sea, air, and space domains. In this capacity, the U.S. intelligence community has long monitored foreign countries' acquisition of technology outside of their own indigenous development programs.

Analysis of technology transfer most intuitively includes tracking a country's acquisition of a key technology or component, openly or illicitly, but also includes understanding of how actors assess tech-

nical specifications, design or engineering skills, and manufacturing and production techniques. These kinds of technology transfers can allow a country to speed up or lower the cost of development projects because they can bypass or trim the costly research and development stages. These acquisitions can not only improve foreign military capabilities, but can also accrue to them economic benefits.

In this course, China is the embodiment of the military technology transfer challenge. The Chinese government has a comprehensive strategy for technology and modernization to bolster China's international image, foster its national economic growth, and improve its military modernization.

And technology acquisition from the United States is definitely part of that comprehensive strategy. For some time, Beijing has articulated industrial policies and long-term objectives contained in a number of comprehensive national development plans, such as its well-known 5-year plans and its Made in China 2025 initiative.

In these plans, Beijing has shown that it is interested in acquiring technology and expertise that is of critical economic or national security importance to the United States. In its most recent 5-year plan, Beijing identified its most critical technology priorities, including clean energy, aerospace and deep sea research, computer and information technology, and manufacturing.

China is therefore prioritizing investment in and acquisition of critical future technologies that will be foundations for future innovations, both for commercial and military innovations like artificial intelligence, robotics, autonomous vehicles, augmented and virtual reality, financial technology, and gene editing. These technologies are inherently dual use, making it difficult to draw a line between commercial versus military applications. These technologies are also likely to be foundational to future innovations and essential to the next wave of competitive high-technology products.

China's development strategy is multifaceted and its supporting infrastructure is robust. China uses multiple vectors to acquire the skills and know-how it seeks, and I would like to highlight a few of these for you.

One is joint ventures, mergers, and acquisitions. Tech transfer to China is occurring in part through increased levels in investment and acquisitions of U.S. companies, which hit a record level in 2016 before dropping somewhat in 2017 and again in the first half of 2018. China's aggregate investment in U.S. technology over the past decade, from 2007 to 2017, totaled approximately $40 billion and was about $5.3 billion last year. And because the Chinese Communist Party is intimately involved in planning economic activity and supporting companies, there is a great deal of coordinated investment, along with other vehicles of technology transfer, to accomplish China's larger stated goals.

Another vehicle are research partnerships and academic collaborations. Foreign governments often use every means at their disposal to secure an advantage in technological areas, and their exploitation of academics and researchers at U.S. colleges, the National Laboratories, and other institutions is one of those means. China actively seeks partnerships with government laboratories to learn about and acquire specific technology and the soft skills nec-

essary to run such facilities. China also uses collaborations and relationships with universities to acquire specific research and access to high-end research equipment.

Another vector are science and technology investments. Beijing has made sustained, long-term state investments in its S&T [science and technology] infrastructure, and China leverages international collaborations with key pieces of this S&T infrastructure to gain technology and know-how. In 2017, China's spending on research and development was estimated at $279 billion, up more than 70 percent from 2010.

Another mechanism are talent recruitment programs. Beijing runs multiple talent recruitment programs specifically focused on recruiting global experts who can facilitate the transfer of foreign technology, intellectual property, and know-how to advance China's science, technology, and military modernization goals. China uses these programs, such as its Thousand Talents Program, to recruit Western-trained experts to work in China on key strategic programs.

Beijing also has employed Western-trained returnees to implement important changes in its science, engineering, and math curricula that foster greater creativity and applied skills at China's top-tier universities.

Another mechanism that it exploits is the legal and regulatory environment. China consciously uses its laws and regulations in ways that can disadvantage U.S. companies and advantage its own companies. The Chinese government uses foreign ownership restrictions, such as formal and informal restrictions, to require or pressure technology transfer from U.S. companies to Chinese entities.

The Chinese government also uses its administrative licensing and approvals process to force technology transfer in exchange for the numerous administrative approvals needed to establish and operate a business in China.

We also assess China will use cyber espionage and bolster its cyberattack capabilities to support national security priorities, which include technology acquisition. The IC and private sector experts continue to identify ongoing cyber activity from China. Most detected cyber operations against U.S. private industry are focused on cleared defense contractors or IT [information technology] and communications firms whose products and services support government and private sector networks worldwide.

And China's technology transfer mechanisms are paired with Beijing's parallel strategy of military-civilian fusion that expands civil-military integration of defense and industrial bases to facilitate the construction of a national infrastructure connecting the PLA [People's Liberation Army], state-owned defense research, development, and manufacturing enterprises, and government agencies under the state council, universities, and private sector firms. We assess that these collaborative partnerships have well supported Beijing's rapid military modernization.

What are the possible long-term consequences? Well, while the most immediate and visible effects may be related to particular military technologies, the long-term consequences could be much broader.

A decline of the United States advantage in key technology could affect our ability to set global norms and regulations for technology, control access to technology for military purposes, and reap the economic benefits we derive from commercialization. If the United States were to lose its technological edge, the associated loss of influence would have far-reaching implications beyond scientific disciplines to include economic, social, political, and security dynamics.

Within the ODNI [Office of the Director of National Intelligence] we are facilitating the information exchange among the organizations responsible for the analysis of technology transfer because this issue is global and multifunctional in reach and nature. We collaborate closely across the intelligence, counterintelligence, and law enforcement communities, as well as other national agencies in multiple ad hoc groups and formal groups working on specific technology transfer issues. We regularly develop collection requirements and provide warning in the form of intelligence products of threats associated with technology transfer.

This concludes my overview of the threats posed by military technology transfers. And, I will now turn to my colleagues to continue with remarks on the impacts of these foreign activities on the United States and measures we are taking to thwart and deter them. Thank you very much.

STATEMENT OF HON. KARI A. BINGEN, DEPUTY UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE, DEPARTMENT OF DEFENSE

Ms. BINGEN. Thank you. Chairman Thornberry, Ranking Member Smith, and members of the committee, it is a privilege to be back although it is a bit of a different viewpoint from down here. I was really honored to support you in all the vital national security work you do, and was fortunate to see firsthand the bipartisan approach that you took to national security and providing for our military. So, thank you.

In my new role, I support the Under Secretary of Defense for Intelligence [USDI] as he carries out his lead responsibilities within the Department on behalf of the Secretary for both intelligence and security, executing the National Defense Strategy, including its direction to protect the National Security Innovation Base. As you heard from my ODNI colleague, the Department of Defense is facing unprecedented threats to its technological and industrial base, putting at risk the capabilities critical to maintaining our military advantage.

China, in particular, has made it a national goal to acquire foreign technologies to advance its economy and to modernize its military. It is comprehensively targeting advanced U.S. technologies and the people, the information, businesses, and research institutions that underpin them. It is playing the long game, using a variety of different methods to steal our information, circumvent our processes, and exploit our seams.

Across the defense intelligence and security enterprise that the USDI oversees, we are making significant changes in our approach to industrial and to information security, as well as to counterintelligence. I welcome the opportunity to follow up with you in classi-

fied session to discuss additional initiatives we are undertaking that will provide you with a more holistic picture.

In our unclassified forum today, I will touch briefly on four key lines of effort. First, we are elevating the private sector's focus on security, through an initiative called Deliver Uncompromised. We must have confidence that industry is delivering capabilities, technologies, and weapon systems that are uncompromised by our adversaries, secure from cradle to grave.

It is no longer sufficient to only consider cost, schedule, and performance when acquiring defense capabilities. We must establish security as a fourth pillar in defense acquisition and also create incentives for industry to embrace security not as a cost burden, but as a major factor in their competitiveness for U.S. government business.

Second, through the Defense Security Service, we are implementing a more comprehensive approach to industrial and information security. We are transitioning from a compliance checklist-based national industrial security program to a risk-based approach, informed by the threat and the Department's technology protection priorities.

However, safeguarding our cleared defense contractors only protects part of our defense industrial base. The increasing ease of access to large amounts of unclassified and nongovernment data in the defense industrial base offers opportunities for exploitation which, in aggregation, can be as damaging as a breach of classified information. To narrow this gap between protecting classified information and that unprotected unclassified information, we are developing a program protection plan to cover controlled unclassified information, including identifying the policy and resources necessary to do this.

Third, using authorities provided by this committee, including section 806 of the fiscal year 2011 NDAA and section 1696 of last year's NDAA, we are strengthening the integrity of the supply chain as well as establishing a pilot program to enhance information sharing with cleared defense contractors.

And, fourth, we are enhancing our counterintelligence capabilities to better address the nontraditional collection methods being employed by our adversaries. We are adding security and counterintelligence personnel resources to the Defense Security Service, NCIS [Naval Criminal Investigative Service], Air Force Office of Special Investigations, and the Army CI [Counterintelligence]. Our defense intelligence components are augmenting their collection and analysis capabilities to gain a more comprehensive understanding of threats to our technologies, which will improve our intelligence support to export control reviews and CFIUS transactions.

Lastly, we are increasingly relying on our partnerships with FBI [Federal Bureau of Investigation]—not just increasingly, but we must rely on our partnerships with the FBI, Homeland Security, and other departments to actively leverage both our individual and our collective authorities to protect the Nation's critical technologies. Through these four lines of effort, we can help mitigate the threats to our technology and information critical to our military

advantage. And, by doing so, deliver uncompromised capabilities to our warfighters.

We recognize that strong relationships with industry across the interagency, with our allies and partners and with Congress are essential to that success. We thank you for your continued focus on the threat, your understanding of the impacts to our warfighters and their capabilities, and your commitment to support our policies, programs, and the resources necessary to maintain our advantage. I look forward to your questions.

STATEMENT OF ERIC CHEWNING, DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR MANUFACTURING AND INDUSTRIAL BASE POLICY, DEPARTMENT OF DEFENSE

Mr. CHEWNING. Mr. Chairman, Ranking Member Smith, and members of the committee, thank you for the opportunity to speak with you all this morning. I serve as the principal adviser to the Under Secretary of Defense for Acquisition and Sustainment on DOD policies for the maintenance of the U.S. defense industrial base. This includes assessing the national security impact of foreign investments.

Our National Defense Strategy outlines a handful of critical technologies necessary for maintaining U.S. military dominance in an era of great power competition. For those capabilities with unique military applications, like missile defense and nuclear forces, the Department of Defense will continue to act as our Nation's sole developer and technological first mover.

But, for those emerging technologies with both military and commercial uses, like artificial intelligence, we will also need to be a fast follower and adapter of commercial sector innovation. Therefore, force structure modernization requires support from both our heritage and legacy, and commercial defense industrial base.

Chinese industrial policies of economic aggression, such as investment-driven technology transfer and illegal intellectual property theft, pose a multifaceted threat to our entire national security innovation base, a threat with the potential to create both long- and short-term impacts. In the short term, their attempts to steal intellectual property, compromise our defense supply chain, and create economic dependence within the sub-tier of our industrial base chips away our relative military technological advantage.

Over the longer term, spurred on by strategic initiatives like One Belt, One Road, Civil-Military Fusion, and Made in China 2025, this potential for China to erode our underlying innovation and industrial advantage. The engine of our national defense has always been the strength of our economy.

Chinese policies seek to extract technologies from Western institutions, leverage our educational system to develop its own workforce, and use subsidies and nontariff barriers to prevent competition and to enable the creation of national champions. These national champions enjoy a protected domestic market, which they will use to their relative advantage and enable them to grow at speed and scale. And then, use all the elements of the communist state to place their national commercial champions at the top of critical markets and industries globally.

These commercial national actors are then directed to compete globally against United States and Western firms, while being given every subsidy and benefit the authoritarian communist government can devise, with the goal of marginalizing U.S. companies. Combating these predatory economics require a whole of nation approach to both protect and promote American industry, as well as our like-minded allies and partners.

From a defense industrial policy perspective, this includes modernization of the complementary protection measures of CFIUS and export controls, as well as increasing the private sector's focus on cybersecurity. On the promote side of the ledger, we need to make sure the Department is a customer of choice for emerging technology providers. This will require acquisition processes that operate at the speed of relevance, as well as budget stability so we can send a clear demand signal to industry.

Thank you very much for the opportunity to testify on this important topic, and I look forward to answering your questions.

[The joint prepared statement of Secretary Griffin, Mr. Schinella, Ms. Bingen, and Mr. Chewning can be found in the Appendix on page 42.]

The CHAIRMAN. Let me just ask, as I mentioned at the beginning, one of the issues with which we will deal in conference is a modernization of the CFIUS process. That has been added to the Senate Defense Authorization Bill. There is an effort in the House to not only update CFIUS, but also the export control regime, which may be considered fairly soon in the House floor.

But, regardless, this issue is before us. And, what guidance can you, any of you, give us as far as the updating of CFIUS and export controls?

Mr. CHEWNING. I am happy to take that first, Mr. Chairman, and I am sure my colleagues would also like to add on. But we think of CFIUS and export controls as complementary tools for protecting national security.

The Secretary has identified three gaps in the current regime, specifically around tech transfer through joint ventures, access to technology through non-controlling investments, and expanded review of leases and real estate purchases so we can protect investments near sensitive military sites. What I would suggest to you is that recognizing that both CFIUS and export controls need to work in concert to address these three gaps.

Secretary GRIFFIN. The comment that I would like to make, sir, is that in the CFIUS process historically, we look at one deal at a time. We do not look at the overarching pattern of such purchases or investments. I think it is the broader pattern which is actually of greater concern.

We also do not look at CFIUS investments or investment candidates from the perspective of, let me just say, the intelligence gathering opportunities it offers. For example, every firm today, which even if it is not in a technology-critical sector—so, let me go to that extreme, but yet such firms all have highly networked software systems controlled by commercial operating systems.

Every time that there is a software update to such an operating system, it affords another intrusion path into domestic networks. We do not look at Chinese investments from the perspective of the

mischief that might be made simply by having foreign ownership and, in some cases, control of such avenues. So I will leave it that. I believe that is as far as I would want to go at this point.

The CHAIRMAN. So my conclusion from that is, we need to update CFIUS and export controls but it does not fix all the problems?

Secretary GRIFFIN. It does not remotely stop there, sir, in my opinion.

The CHAIRMAN. Okay. Mr. Smith.

Mr. SMITH. Thank you. I mentioned in my opening remarks, the idea of, you know, having an industrial policy as to what key technologies we should protect. That is very easy to say; it is incredibly complicated to implement in terms of how you would do that.

But, just what ideas would you have in terms of what an industrial policy would look like if we basically geared our trade policy and our internal investments to make sure that we were protecting certain core technologies? I realize you could write a book in answer to this question; please do not.

But, if you could, just give us a little bit of a framework of what an intelligent industrial policy would look like. Because I do not think the President has the vague idea of the problem, and then it is just like all over the place in terms of how to solve it. What would a more coherent approach look like?

Secretary GRIFFIN. Well, I am not going to address any of the back-and-forth chatter in the current environment because we are talking about a long-term strategy here. We need to recognize that whether they are specific defense products or not, many things underlie our industrial base.

I might, from a large list, as you said, sir, I might pick out, for example, microelectronics. We worry about that from the point of view of having a trusted supply. Kari mentioned that in her comments. We want to know that we have an end-to-end supply of defense equipment, and I would also say commercial equipment, that we can trust.

The difficulty in the microelectronics arena is that, an area in which the United States once reigned supreme, thanks to now 20-some years of Chinese investment, domestic U.S. manufacturers no longer, in all cases, make the best microelectronics. So we should be unsurprised when others elsewhere or anywhere in the world no longer seek to buy from us, but seek to buy the best.

Mr. SMITH. Can I shift focus on my question a little bit——

Secretary GRIFFIN. Yes, sir.

Mr. SMITH [continuing]. To help with that. As I mentioned early on, some of this is inevitable. I mean, the rest of the world was going to catch up.

I think a lot of people underestimate the impact that World War II had on, you know, several decades of us—the entire industrialized world got blown off the face of the map and we were the last ones standing, basically. If you are going to fight a war, it is always good to win; it is even better to win on the road. And, that left us in a very, very strong position for several decades.

But that was highly unusual. So even if China was not doing all this nefarious stuff—and I agree with the chairman, we have got to go after the CFIUS possibly, we are going to have to compete. And we are also—I think, part of our industrial policy is some of

what we are going to need, we are going to have to get from someplace else.

So would you say that—in my conclusion, that is we need allies. We need people who have—the—I do not think there is anything built in America anymore that is entirely made of American parts, or anything built anywhere, for that matter, that does not rely on some sort of supply chain. What could we do better to make that aspect of it work? To have part—you know, countries that we can trust and work with?

Secretary GRIFFIN. Well then I will get off that previous path and refer to my opening remarks, where we are today not drawing distinctions in our industrial policies between friends and allies and partners, and people who behave in an adversarial manner.

Mr. SMITH. Yes.

Secretary GRIFFIN. It is in our interest to make it easy for our allies and partners to cooperate and collaborate with us as opposed to making it easy for them to collaborate with China, and it is in our interest, in my opinion, for us to make it more difficult for the Chinese to work with us.

During the Cold War, there was a whole of nation policy, such that the idea of doing a commercial deal with the Soviet Union were words that did not fit in one sentence. We do not have such policies today.

Mr. SMITH. Yes, I will stop there, because—well, keep it quickly, I have gone on too long. Go ahead.

Mr. CHEWNING. Well—just very quickly, just to maybe give a tactical example of where that collaboration is taking place. You know, the NDAA enshrined the NTIB, the National Technical Industrial Base, which is a partnership between the United States, Australia, Canada, and the United Kingdom.

We are using that to do a couple of things. One, collectively, how can we work together to create a foreign direct investment screen so we can work in concert against predatory economics from unallied nations? But then also to identify areas where we can do industrial-based collaboration to benefit us more broadly.

Mr. SMITH. Okay. Thank you. Sorry, Ms. Bingen.

Ms. BINGEN. Mr. Smith, if I can also tackle that, is from the foxhole where I sit, I see it as my job to not make it easy for China to get this technology. And so in my remarks, I hit on four key pieces. Security has got to be a fourth pillar in acquisition, in addition to cost, schedule, performance. And it is not right now. And it will be incredibly complex to do. We have got to put it into the regulations, into the contract mechanisms, et cetera.

Second, DSS [Defense Security Service] in transition—and I will hit on that in a moment, integrity of the supply chain, and increasing our CI resources. DSS in transition: it was amazing to me to see the approach we take to industrial security today is very much checklist-based. You go into a cleared defense contractor, "Do you have the alarms, the locks, the safe?" It was not looking holistically at what is the technology or capabilities that you are providing to the government? What is the threat? What are your vulnerabilities?

And so they are now, based off of DOD's critical technology priority list, going into these companies that work in these areas to

look more holistically at all those different pieces; it is probably going to be uncomfortable for industry, but we need them as a partner to do this if we are going to be able to deliver on compromise.

Mr. SMITH. Okay. Thank you very much, Mr. Chairman, I yield back.

The CHAIRMAN. Mr. Wilson.

Mr. WILSON. Thank you, Chairman Mac Thornberry, for holding this hearing on such an important topic. Establishing and maintaining our military's technological edge is imperative in order to increase their effectiveness and lethality on the battlefield while protecting our troops.

The Department must encourage and protect research and innovation from being stolen by state and non-state actors. I am concerned by the assessments provided today, but hopeful by the attention being provided by Chairman Thornberry and the House Armed Services Committee.

First I would like to welcome back Secretary Kari Bingen as an alumna of this committee, and we appreciate your service and wish you the best. And so appropriately the first question begins with you. And the question is, is additional legislation needed to protect particular technologies and associated intellectual properties with military applications? If so, what technologies are in the greatest need of protection, why would legislation be necessary to protect them, and how should such legislation provide such protections?

Ms. BINGEN. Thank you, Mr. Wilson. Good to be back here. A couple areas I would highlight, there—there is section 806 this year on extending the authority for us to strengthen the supply chain. We think that is a very good measure, and we are implementing those processes now to be able to do that and excise out of supply chain vulnerabilities.

On the resource front—and we will have to work with the committee on the specifics of this, but on the counterintelligence areas that I talked about, the greater analysis that we will have to do with our industry partners to understand where their threats and vulnerabilities are, that will require additional resources.

With these CFIUS reforms, whatever final legislation comes out of that, that will place an increasing demand signal on our intelligence capabilities, so that will require additional resources. But then also, as we go through this delivering uncompromised and DSS in transition, as we look at how we implement control—how we implement protections on controlled, unclassified information, we may need to come back to you with specific legislative proposals, and we will work with you on that.

Mr. WILSON. Thank you. And if anyone else would like to respond?

If not, a general question for everybody again. Is this primarily a nation-state problem? What about transnational criminal organizations, multinational corporations, or terrorist groups? What risk do non-state actors pose in transfers of U.S. intellectual property and technology?

Secretary GRIFFIN. Well sir, those are important issues as well, but the bulk of all the information we have gathered is that China is the big problem. And I think we need to focus our efforts on first

taking care of the big problems and then absolutely we cannot afford to neglect other areas, such as you suggest. But we have to prioritize.

Mr. WILSON. And then in particular, identified in China, the Confucius Institutes that are located at 103 colleges and universities across the United States. Many of these are located adjacent to research facilities. Is anyone familiar with the Confucius Institutes, which has been identified by a member of the—of the Central Committee of the Communist Party of China as a very important propaganda arm? Is anybody familiar with what is being done to try to identify these institutes as to their motives?

Mr. SCHINELLA. Speaking to your original and second question generally, I would agree with colleagues that this is predominantly a state actor problem, or at least that is certainly the largest and most looming problem. Within that, China is the most pressing threat.

With the slight additional amplification that in the case of a country like China, you asked about multinational corporations. When you have state-owned enterprises, you know, our framework does not necessarily capture the—that blurred line between a multinational corporation and state actor itself.

I—we are familiar with the Confucius Institutes as one more visible representation of China's global presence, including in the United States, and consistent with my earlier remarks, I would just note that that is just one of many, many footprints that Beijing has in, near, and on our campuses and research institutes that it uses as ways to overtly and less overtly collect on and maintain awareness of what is happening on those campuses and institutions. Thank you, sir.

Mr. WILSON. And thank each of you, and we appreciate your service to our country.

The CHAIRMAN. Mr. Gallego.

Mr. GALLEGO. Thank you, Mr. Chair. And thank you, to our witnesses. Even before getting to Congress, I have been hearing about this, reading about this, and now, even more sitting in Congress, I am dismayed that I am hearing about the diagnosis but not necessarily the way to fix this.

You know, in the Marine Corps, you have a couple options, right? You know, to protect yourself, you have your Kevlar or your body armor, more importantly though, you have your rifle. And the best way to stop somebody from trying to attack you is to look tougher and make sure they know the consequences if they do attack you.

I feel when we are dealing with this issue that we are talking about how to only play defense. But what are, actually, are our offensive options to actually make our quote/unquote enemy understand that if they do these types of actions that it is going to be painful? And, obviously to a certain degree—I, you know, I do not want to trigger a war—but we need to be able to have some level of deterrence.

So, that way, they actually have to make a rational calculation of whether or not they are going to engage in this type of conduct. If not, I feel like this is just going to continue to happen. Every year, I am going to have the same briefing and all we are going

to be talking about is what happened and not what we can do to stop them.

So, I do not know who wants to take the question first, but I would like to hear some ideas. Or, if we have to take this to a classified setting, that is fine, too. But, I would love to hear it. And, welcome back, too.

Ms. BINGEN. Sir, thanks. If I can start, again, from an industrial security perspective and that is what I am here to represent, my focus is on cleared defense contractors. And I outlined the four areas, security fourth pillar, DSS and transition, supply chain integrity, counterintelligence. Two other areas; we are branching out and, as Mr. Schinella highlighted, there is a deep concern with the cyber data exfiltration issue. And it is one that the Chinese in particular are targeting.

So, one of the directions that my boss, the Under Secretary, has given to Defense Security Service is to come up with that program protection plan, come up with the policies for how we control within industry that unclassified information, yet still may potentially have some sensitive technical information or personal information. So that is one of the areas that we are hitting.

The other one is I absolutely agree with you on we are playing defense right now, particularly in the cyber domain. And we need to be playing more offense. We need to be working with the FBI, leveraging their authorities on the law enforcement front. But that will require a further conversation with you, largely at the classified level, on some of the authorities and resources that we might need to do that.

Secretary GRIFFIN. At the unclassified level, I will say that it is through CFIUS, and possibly FIRRMA [Foreign Investment Risk Review Modernization Act] in the future and other mechanisms, it is our choice as a nation as a matter of national policy as to whether or not we allow investments of any magnitude and scope by China in this country. It is our——

Mr. GALLEGO. And I apologize, not to cut you off, but my point—the point that I guess I have made is that you are all describing defensive protocols and methods, right? And it does not really matter to the Chinese or to our foreign adversary if they know that, you know, they can get around our defenses and there is no consequences.

So, what are we actually doing to change the rationale, the calculations that they are going to actually do these types of things that ostensibly are illegal? What is our pushback?

Mr. CHEWNING. Well, I mean, obviously the administration's Section 301 investigation into Chinese intellectual property theft would be an example of that. I think more broadly, if we think about the offensive measures we can take from an industrial base perspective, what are we doing to promote our own industrial base capabilities, right?

I think that, from a DOD perspective, starts with the recognition that going forward we are going to have to not only remain the sole developer for certain bespoke military applications, but reform our acquisition processes in a way we can leverage the benefit of our entire broader economy, right? And, become a customer that is able

to attract the best of both the heritage defense industrial base as well as emerging commercial technology providers.

Mr. GALLEGO. Thank you, I yield back.

The CHAIRMAN. Mr. Lamborn.

Mr. LAMBORN. Thank you, Mr. Chair, and thank you for having this important hearing. Thank you all for being here.

This is an occasion where I am going to agree with Mr. Gallego 100 percent, which is not a typical, not a daily occurrence necessarily. But, something on this important issue I wanted to point out. And I was going to ask, and will ask the same exact question. What are we doing offensively?

You have talked a lot about some great defensive measures, and where we are buttoning up, and then making airtight the secure and vital research and technology that our defense contractors, our government has. And I applaud you 100 percent for doing that. But I would like to see more in the way of consequences to the Chinese when they do this adverse behavior.

I will just make an editorial comment here. I think for too long, administrations of both parties have been rather passive in light of what is going on. I want to applaud the Trump administration that, at least in the area of trade, that there is pushback going on now with talk of tariffs. I do not know how that is all going to play out; but I am glad that that is being discussed and made a serious issue in Washington. I think that is an example of pushback that needs to happen.

Let me throw out an idea, if you want to comment on this, you can. You do not have to if you do not want to. I think it might be interesting to have a widespread and concerted policy in our defense to put out wrong information, pretend like it is great information, great technology, and they steal it and it will not work for them. Or they go down a dead end and they waste money, or it actually backfires somehow.

I think it would be an interesting thing to pursue, where we start poisoning some of the technology that is ostensibly vital, and healthy, and good, but it messes them up when they start to pursue it. Any thoughts on that?

Mr. CHEWNING. Maybe I could answer the first part of the question, then defer to my colleagues around that particular issue specifically. But, just to elaborate, so the Section 301 investigation the USTR [Office of the United States Trade Representative] led into Chinese theft of U.S. intellectual property does have some offensive measures to it. And as was publicly articulated in a memo from the White House on the 29th of May, there is obviously the tariff action that has been associated with that. There is potential for investment restrictions into the U.S. economy. And then, there is the WTO case that we have taken forward, specifically to dispute——

Mr. LAMBORN. Okay, good.

Mr. CHEWNING [continuing]. What the Chinese are doing. So——

Mr. LAMBORN. Good.

Mr. CHEWNING [continuing]. Just to be clear, there are offensive measures that are being done in response to Chinese economic aggression. I will defer about——

Mr. LAMBORN. Thank you, I am glad to hear that.

Mr. CHEWNING [continuing]. About the second question.

Mr. LAMBORN. I am glad to hear that.

Ms. BINGEN. And, Mr. Lamborn, I would love to follow up with you in a classified session to talk more holistically, at the classified level, about all the different things that we are doing or looking to do.

Mr. LAMBORN. Okay. Okay, good. And lastly, I will finish up, there was an article in The Wall Street Journal today or yesterday about some detected Chinese hacking on our space operations. And it was on not research and development, but on the operations side, which indicates that there is an intent in the future perhaps to use that information to disrupt—to be disruptive, to disrupt operations in an offensive way, possibly in a time of conflict. Does that concern you?

Secretary GRIFFIN. Sir, that is a topic that I really do not want to discuss in a public setting. Broadly speaking, your comment, taken on its face, is very concerning. It is, for me, very concerning to have read about it in the papers. I would—as my colleague, Kari Bingen, just said, I would welcome the opportunity to discuss this stuff in a more closed setting.

Mr. LAMBORN. Thank you. Well, with that, Mr. Chairman, I will yield back the balance of my time. Thank you for being here.

The CHAIRMAN. Ms. Davis.

Mrs. DAVIS. Thank you, Mr. Chairman. Thank you all for being here. While we have raised the issue of trade policies, I am wondering if you could comment and you know, I am not trying to make this into a debate here in terms of trade, but we mentioned a number of areas, particularly related to China. So was it a real missed opportunity to have not moved forward on the Trans-Pacific Partnership when it comes to national security?

Secretary GRIFFIN. I am unable to offer you an opinion on that, ma'am. I am sorry, I am not familiar—I just do not have the expertise to comment on the Trans-Pacific Partnership versus national security.

Mrs. DAVIS. Okay, because in many ways—maybe you would like to comment, I think we lost that opportunity to have China be more disruptive when it comes to that. Go ahead, did you want to comment?

Mr. CHEWNING. I agree with the Under Secretary. That is not an issue we have looked at specifically yet, so I do not have any further comments.

Mrs. DAVIS. Really. Okay, maybe that is one of the problems. I mean, I think that we were aware that national security was an issue in this regard, and it is I guess sort of surprising to me that there was not that kind of weigh-in when it came to those issues.

So I wanted to ask you further, we talk about a whole of government approach, we are often doing that, and yet when it comes to the concerns that you are raising here, how important is it, and are you monitoring that? Are we engaging those elements of governance and government that historically or traditionally we do not think of in this area of intellectual property or endeavors?

Where do you think that is, I mean, and how do the Department of State, Treasury, Justice, Homeland Security contribute to technology protections, and are there other roles that the Department

of Education, Health and Human Services could be playing in this regard?

I mean, it is a complex issue and I am just looking to see—to what extent do you think that that is important?

Secretary GRIFFIN. Well, I will start. I do think it is important. I have said publicly, actually I believe in an earlier hearing before this committee, that we somehow in the years since the Berlin Wall came down and the Soviet Union dissolved, we believed that great power competition was behind us. The National Defense Strategy released this past January makes a very clear set of points that we have returned to an era of great power competition and we must treat it as such.

When we believed, throughout the, you know, several decades of the Cold War, when we believed we were in a great power competition for not only the hearts and minds of the world, but possibly our very existence, we treated such all the matters that you are talking about, State, Education, Commerce, the Treasury, we treated all of that as if it were of existential importance, which it was.

Today, we treat these individual matters as if they were individual matters, and I think what you are hearing from us is that they are not isolated issues, that they need to be treated in the large.

As I was starting to answer to Mr. Gallego's question earlier, we as a nation have choices. Do we wish to admit, as we have today, 30,000 Chinese PhD students in STEM areas? Do we wish to do that? Do we think the benefits outweigh the gains? There is not a national decision in that regard as there was when we were competing against the Soviet Union. We did not do those things.

It us not for me to say whether we should or should not. I am trying to put on the table that these apparently isolated decisions in fact when taken together comprise a whole of government strategy that we do not have.

Mrs. DAVIS. Yes, I do not know if anyone wants to comment [inaudible]. Is there one particular example that you think creates best practices in a more non-traditional way of working together that we ought to be looking at more seriously?

Guess not. Thank you. Thank you.

Ms. BINGEN. I would be happy to follow up, ma'am.

The CHAIRMAN. Dr. Abraham.

Dr. ABRAHAM. Thank you, Mr. Chairman. A huge problem, national security issue, and the mentality of, why build it when you can steal it? So we get that, and I was listening to—Ms. Bingen, you had your four pillars, and one of those was a program called "delivery uncompromised," I think was what it says.

And my question is, for these contractors and subcontractors, is there an MBO, a management by objectives policy, that if they do not meet objectives they are penalized or punished, or if they do not reach that security level they are kicked out of the system? Is there any accountability today?

Ms. BINGEN. Well sir, you have actually hit on the challenge and why we are taking this different approach. When a contract is awarded to a company, it is based on cost, schedule, performance. It is not based on security.

And so part of this delivery uncompromised initiative is working through all the details of what would that look like, what are the standards, is there an independent verifier that does the—you know, the good housekeeping seal of approval on it, how do we work with our acquisition colleagues on infusing security into acquisition policies, into the regulations, into the actual—in the COTRs [Contracting Officer's Technical Representatives], the contracting officials that help drive those decisions?

So those are all the details that we are working through now. But then also, industry cannot look at it the way they do today, which is, this is a cost center and it is a loss to my bottom line. They have to be incentivized to look at security as, this is actually going to help me make more profit.

Dr. ABRAHAM. But are they held to that standard now?

Ms. BINGEN. They are not.

Dr. ABRAHAM. Okay, and I will just go to a quick second question. Classified versus unclassified, we understand that today's classified data is yesterday's outdated data, or vice versa, but it—this data evolves so quickly and this technology evolves so quickly that it is hard to keep up with. And that, if you take two unclassified pieces of data and perhaps marry them together, then it becomes a classified document.

My question, just for my understanding, who actually has the authority to make the call as to whether a piece of data or a piece of technology is classified. Is it the project managers? Is it somebody in DOD? Is it somebody—what wheelhouse makes that decision on a daily basis?

Ms. BINGEN. The Under Secretary for Intelligence has the policy responsibilities. So, we set the framework and the basic standards for what those differentials are.

Dr. ABRAHAM. So you have the responsibility. And you have the authority. But do others under you also have the authority? I understand the responsibility, and that is where the bullet does stop there. But the authority can be delegated out to other people. Is that a lot of fingers going out, or is it two or three people, how does that work?

Secretary GRIFFIN. Well, in the technology arena, for example, I have original classification authority, should I make a determination that a particular set of technologies upon which we're working needs to be protected. And many others do as well. Those authorities can be delegated and are delegated downward. I know there have been breaches, we had reference to that earlier on today, of actual classified information.

But I will go on record, sir, as saying that I believe this hearing, and our witness statements and responses to questions, are more about the amalgamated effect of the industrial base and technology levels as a whole, not whether or not a particular exfiltration attempt by the Chinese was successful in a particular case. But rather, the whole pattern of Chinese investment in our industrial base, extraction of data, predatory joint ventures, predatory trade practices, the whole spectrum of Chinese adversarial behavior with respect to our economic and industrial base, I believe that is—actually the larger concern, sir.

Dr. ABRAHAM. Oh, I understand the 30,000-foot view. But, I also understand the ground-level view, that if we have that one breach on a national security issue, it can certainly parlay into something much bigger, so.

Secretary GRIFFIN. Absolutely, sir.

Dr. ABRAHAM. I yield back, Mr. Chairman. Thank you.

The CHAIRMAN. Mr. Larsen.

Mr. LARSEN. Thank you, Mr. Chairman. So, on the debate about whole-of-government approach, I am just concerned that you throw the term around like it is candy at a parade. Because at the same time, you have testified that—someone, one of you did—that the Belt Road Initiative is problematic for U.S. policy.

At the same time, you testify that our Department of Commerce is holding bimonthly meetings with U.S. companies and the U.S. embassy in China to figure out ways for those U.S. companies to access projects in the Belt Road Initiative, at the same time you talk about whole of government approach.

I am not asking you to be experts on trade or TPP, but to have some concept of how—what the argument was on Trans-Pacific Partnership, how it fit into leveraging U.S. economic policy and strength in Asia vis-a-vis China. Just that basic understanding would be helpful for you all.

And so, I do not think you are talking about a whole of government approach. I think you are talking about—you may be talking about a whole of Pentagon approach. So, if there is a whole of government approach, I would like to know—and not from you today.

But, just another example, if we are in an era of great power competition, you talk about the last one we had and we are not doing those things we—today that we did in the last one. Well, in the last one we had, we fought for open markets. We put human rights near the top of the list when we talked to North Korea. And we are not doing that today, so does that not apply to this era of great power competition?

So, again, I think you are throwing the term around to try to make it sound like you are doing it. But I do not think you are. And you need to get on it. If you have—you need to have a, you know, a mechanism. If we only had a National Security Council mechanism that could develop the whole of government approach that is used by the White House, then we might have one.

So that is—I usually do not give speeches. I usually ask questions in my 5 minutes. But, it has just been—frustrating to hear this term being thrown around, again, like candy at a 4th of July parade; and I do not think you are living up to it.

So, Ms. Bingen, I wanted to ask you about a couple questions on your five—you made four points on what you are doing. Specifically on, I think it was your third or second point, about section 806 and 1696 authorities and strengthening supply chain security in the Defense Department. That is great, that might favor larger contractors. And so, because they have the capacity to, you know, absorb the costs, if you will.

How are you going to ensure that smaller companies, smaller businesses that maybe have more innovative ideas, can bring more flexibility to the table at the Pentagon, how are you going to ensure that they do not get tossed aside because they do not have that ca-

pacity to do the kinds of things perhaps on supply chain security that you might be asking them to do?

Ms. BINGEN. Yes, Mr. Larsen, that is a great question and that is something that we will have to work through. We are really just at the front end of that. And on 1696, we are putting together the plan for right now. I think it was—it is—the pilot has to be established by next—I think early next year, 2019. So, that is something that we absolutely will have to consider. I do not know that I have a good answer for you today. But, it is something that we are looking into and I would be happy to follow up with you.

Mr. LARSEN. Yes, if you could. Your staff and the committee when we did a tour around the country with small businesses, Chairman Schuster, at the time, and I went around the country and tried to find ways that we could bring small business more into Pentagon contracting. So, I just would ask you to watch that.

Ms. BINGEN. And then, we will also have to work with them as we do the delivering uncompromised pieces. They do not—you are right, they do not have the capacity that a lot of these large folks do. So, it is, how do we incentivize them, and, also, how do we work the liability issues to encourage them to report and to make these fixes, when they just do not have that big capital that the large folks do.

Mr. LARSEN. Yes, and, again, for me, the crux of it is that this is where some of that innovation that we need to have happen, and that Dr. Griffin wants to have happen, a lot of this is going to take place in smaller companies. But we do not need be building hurdles to make it more difficult for them to do that. So I just would ask you guys to watch that. Thank you. And I yield back.

The CHAIRMAN. Mr. Gallagher.

Mr. GALLAGHER. Thank you, Mr. Chairman. This a great hearing to have. I think sometimes we overlook the issue of technology transfer. And just to follow up on what was said about the need to go on offense: as we are considering a few initiatives, obviously the need to strengthen CFIUS, but I would also like to call your attention to section 217 of the Senate NDAA, which provides the USD(R&E) [Under Secretary of Defense for Research and Engineering] with the authority to establish or fund a nonprofit entity to help facilitate research and technology development in critical hardware-based technologies that the private sector has tended to insufficiently support and could help meet emerging security needs.

And I know it is a long bill, but have you all, maybe starting with Mr. Griffin, been able to take a look at this provision? And from your initial read, do you support it?

Secretary GRIFFIN. Yes, sir, I have read that section. I have worked with some of the folks that are promulgating that initiative, and I support it.

Mr. GALLAGHER. And Mr. Chewning, I know we have had discussions on this. I would just be interested in your thoughts on sort of that angle of the need to invest in hardware. I mean, we spent so much time talking about software and not the hardware angle.

Mr. CHEWNING. Yes, sir, it is a great point. And—and to build on it, about 92 percent of our venture capital investment is in software. And as we think about our need for modernization roadmaps, we know hardware and company formation, in particular, hard-

ware technology is going to be critical. And so I think taking that language in addition to exercising the authorities given to us by Congress in section 1711 in last year's NDAA, we can pull together a response.

Mr. GALLAGHER. Great. I appreciate that. I could not agree more. I look forward to helping this provision get over the line. I think one of the biggest challenges we face is that those of us in the room here today may understand the scope of the challenge, but much of the broader society does not.

And in fact, I think our competitive edge in many cases hinges on more people just getting it from—you know, the promising researcher who takes a second look at an attractive offer to join a state-connected Chinese firm, or a graduate student who decides maybe they should not conduct PhD STEM research in China.

And I know this hearing's about solutions for DOD, but I would be fascinated to hear your thoughts on how we can better communicate the story we are hearing today to the broader population. And reading sort of the DIUx report on technology transfer, I mean, one of the key proposals is outreach to the private sector and academia.

And so I guess maybe a question—let us just go down the panel that way. I mean, how can we more effectively conduct that outreach to the private sector, to academia, and to society more broadly? I know it is a big question, but.

Mr. CHEWNING. Well, I think—and it is a great question. I think increasingly through our industry association engagement, and not just with the types of folks who you think we would be talking to, but more broadly, increasingly we are hearing those concerns from the industry associations.

And I think it is the need to begin to separate the need for an incremental revenue opportunity, where you may be going into a new market, to the longer lens necessary, recognizing that you are going to be doing business with someone who eventually wants to put you out of business, and the need to get that message across.

Mr. GALLAGHER. Yes. And can I just put a finer point on it. I mean, we have had these recent stories about certain Silicon Valley companies not wanting to do business with DOD because of sort of the intersecting with lethal drone operations, right? I mean, that is a huge problem, if at the time when we need to be working more closely with the Googles or the Amazons, with the Facebooks of the world, that is sort of the cultural reaction to working with DOD.

I am just wondering if you could just comment on that briefly, and how do we turn that conversation around? If that makes any sense. Yes?

Ms. BINGEN. Absolutely, sir.

Mr. GALLAGHER. Yes?

Ms. BINGEN. We are disappointed in that, but we also know, in particular in artificial intelligence, that is where the talent, that is where the technology is. The government is not leading in this area, so we need to be able to leverage that. You know, when I think about the numbers of transactions, the data sets that they have—some of our problems may be pretty straightforward for them, given what they do in the commercial sector, and we have got to be able to leverage that.

So for us, from an intelligence perspective, you know, we have a clear mission imperative, we have manual, labor-intensive processes that our analysts undertake every day. We have got to make it better for them and use their brainpower more effectively. But Department-wide, there are a lot of other challenges that we have, you know, logistics, business reforms, et cetera, that would benefit from them, and we have got to believe that there are folks there that, you know, bleed red, white, and blue and want to participate in hard national security—well, want to participate and support national security, but also that the engineers like our problems and we have got good ones for them to work on.

Mr. GALLAGHER. Sure. Sure. Well, I have run out of time. I have a bunch of other questions that we will not get to, but thank you for what you are doing. This is an important subject. I yield the balance of my time, Mr. Chairman.

The CHAIRMAN. Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman. And I want to thank our witnesses for your testimony here today. Like many of my colleagues, I believe a comprehensive, whole of government approach is really needed to maintain U.S. technological superiority, as you have heard from many of my colleagues.

And there is the problem we have run into is that less democratic states have no trouble marshalling their collective resources to their advantage. So what are your recommendations to Congress for policies that maintain our technological edge in critical areas by countering activities of other nations while also fostering a culture of innovation in the United States?

Secretary GRIFFIN. Well, I am fond of saying that the best way to get ahead and stay ahead is to work harder, run faster. We believe that our free-market, capitalist system, capitalist-based system, is the seed of innovation to a far greater extent than any command economy can achieve. And indeed, the entire topic of this hearing is about China stealing from us, not about us stealing from China.

So if we can provide the kinds of incentives that my colleagues have been talking about, we just mentioned 217 for new authorities for hardware-based venture companies. If we, in the DOD, can, using the authorities that you have given us, learn to deal with our industrial base on a more commercial basis, on a quicker and more responsive manner that is not so burdensome to our companies, I think those actions will help us stay ahead.

The mere recognition that we are in a competition and that we should not be making it easier for our adversary will help us. My colleague Kari Bingen outlined and our statement outlines four broad areas that we are very serious about.

So other than those and more general statements, I do not know that I have any very specific things to recommend to you.

Mr. LANGEVIN. Okay, thank you. Ms. Bingen, do you have anything to offer?

Ms. BINGEN. I think I would just echo what Dr. Griffin just highlighted.

Mr. LANGEVIN. Okay, let me——

Ms. BINGEN. But my job, sir—I look at my job as slowing the Chinese and others down from getting our stuff. You know, his job

is to push the envelope on that, our own technology investment and our own R&D [research and development].

And my fear right now, or my big concern is what is being taken from us now, the R&D that we are both—and that S&T—we are both competing for, we are both interested in the same things right now; that is what is going to show up on the battlefield 5 to 10 years from now. And that is what we—we need to slow down our adversaries and then speed up our own capabilities.

Secretary GRIFFIN. Let me amplify my comments, sir, with just one short statement. One of the best assets we have is, in fact, the openness of our society and our alliances and partnerships with our Western—with our Western allies. The more that we can find ways to do things jointly with them and binding them to us, that will—that is a positive step we can take, sir. Thank you.

Mr. LANGEVIN. Thank you. So, let me ask you this. There—there are many promising ideas that the Department has invested intellectual equity in, only to see those ideas and programs end up in the valley of death.

So, recognizing the remaining utility, other entities certainly can swoop in and swoop up any gains made at that point and move forward from there. So, I find this troubling. I am sure you do as well.

You know, with programs like hypersonics and directed energy, where we invested but our competitors have taken our ideas and our investments and continue to innovate. So, do you deem it a risk when we worked on and developed a technology but failed to fund the transition? And—or, also, are there policy impediments that slow technology transfer to our own forces?

Secretary GRIFFIN. Well, sir, the National Defense Strategy released in January, frankly, makes a big deal out of the point you have just raised. And has specific modernization—force modernization goals for the future fight that are outlined in that strategy. And we are working today, this week, this month, next month to enshrine these and to codify these in the upcoming budget preparation.

We have done groundwork, important groundwork in directed energy, especially, and hypersonics, especially—that we have, if you will, let lie for a while when we should have been turning it into actual force. We are trying to reverse that trend. We are working with all deliberate speed to do that.

The two areas that you mentioned, hypersonics and directed energy, are our major candidates for re-vectoring. I am working on that as we speak.

Mr. LANGEVIN. Thank you, well the sooner the better. I know my time is expired——

Secretary GRIFFIN. Yes, sir. Thank you.

Mr. LANGEVIN. So I will yield back. Thank you for your testimony.

The CHAIRMAN. Mr. Hice.

Mr. HICE. Thank you, Mr. Chairman. Dr. Griffin, in the written testimony earlier it was discussed and brought up the need to better balance risk with speed when it comes to prototyping. Can you expound on that a little bit and explain why that is so important?

Secretary GRIFFIN. My favorite topic, sir. That is because, in my more useful years, I did that for a living. I now hope to enable others to do it for a living.

I think the key point that I would make is that if we can return to what used to be this country's ace in the hole, our ability to try out new ideas, cobble them together in prototype fashion, take them to the test range, fly them off, see how they work, fix them where they break and plump them up where they are doing good, then, let operators interact with them because designers and operators need to work together.

When we can develop new things in that fashion, that is the best of this country. We have left our processes get in our way; and by that I mean our legal and contracting processes. The Congress has bent over backwards to offer broader permissions by which we might undertake these developments.

And if I have a single mission in life as the new Under Secretary in this area, it is to get our guys in the field working, again, on these new ideas and let nature tell us which ones are good. The key point is, it is important to recognize that a test failure is not a failure. The failure is when we do not stick to the goal and get the product to the finish line.

Mr. HICE. Very good. Well, I am glad to hear that. And, secondly, I would like to kind of follow up on where Dr. Abraham was going a little bit earlier. And I am not sure exactly who this would be addressed to, so maybe even a couple of you have an answer. But, how do we incentivize companies to comply with the Deliver Uncompromised?

Ms. BINGEN. Sir, that is something we are working through right now. We have had actually FFRDC [federally funded research and development centers] come onboard and do a study for us. And we are working through those recommendations.

But, some of this is going to be outside our area, too. Where it comes back to, you know, how do they look at this so it is not a cost, but—but it is a profit for them. How do we get them to—encourage them to self-report, but not think that there is going to be a liability or penalty associated with that?

So, are there tax incentives we can pursue, regulatory incentives, safe harbor ideas? So, we are working through all of those right now. But, we do think that there are some concrete ideas that we can explore to do those incentives.

Mr. HICE. Well, and I think that is extremely important to solidify this, would you agree?

Ms. BINGEN. Absolutely, sir, and the sooner the better.

Mr. HICE. Does anyone else have a comment?

Secretary GRIFFIN. Yes, sir. I mean, we need, through combination of public policy, tax code, selection criteria for our procurements, we need to make it in the interests of our industrial base to protect their own intellectual property from theft. When it is in their interest to do so, when it is a profit center rather than a cost center, when they care about it is much as we do, then that will turn around.

Mr. HICE. Okay, well while you are going on that, how—how well integrated is the executive branch on the whole threat here?

Secretary GRIFFIN. That might be above all of our pay grades put together, sir.

Mr. HICE. I mean, but you all are dealing with this, just from your observation.

Secretary GRIFFIN. Well, it depends upon who you talk to, really. The primary interest of the Commerce Department is to promote commerce. The primary interest of the intelligence community, I will not speak to that, we have intelligence community representatives. But, as Kari has said a couple times, their goal is to protect what we have. Those two interests can be in conflict.

Mr. HICE. So is DOD and the intelligence community cooperating, at least?

Secretary GRIFFIN. We, I think we are, sir.

Ms. BINGEN. Daily, weekly, monthly basis.

Mr. HICE. Okay.

Ms. BINGEN. I go to all those meetings.

Mr. HICE. All right. And thank you, Mr. Chairman, I yield back.

The CHAIRMAN. Ms. Hartzler.

Mrs. HARTZLER. Thank you very much. Thanks for being here on this very, very important topic. There was a recent article in Foreign Policy magazine that discussed how China has created a sophisticated state surveillance system with facial recognition technology, specifically to target minorities and what they call anti-China behavior. And they developed the system with the help of Chinese surveillance firms like Hikvision.

Now, Hikvision is about 42 percent owned by the Chinese government. And, the chairman of Hikvision's board was quoted as saying that the board must ensure the company, quote, creates a state-owned enterprise, and that it remains quote, under direct control of the Communist Party's Central Committee. In fact, Hikvision received a $3 billion line of credit from the state-owned China Development Bank and this is one of the three so-called policy banks whose financing objectives follow political motives.

And I am sure you can imagine that I was alarmed when I learned that Hikvision cameras were operated at a military installation in my district. The cameras have since been removed, but I am disturbed that the Federal Government willingly purchased these cameras knowing that China is actively engaged in espionage against the United States.

So my question is, I am deeply concerned that video surveillance and security equipment sold by Chinese companies exposes the U.S. government to significant vulnerabilities due to potential built-in back doors, creating a video surveillance network for China purchased by the taxpayer and installed courtesy of the U.S. government.

I would like each of you to discuss the security vulnerabilities posed by Chinese surveillance cameras, and whether or not you believe it is a security risk to have them operating at U.S. government facilities.

So Mr. Schinella, you want to start?

Mr. SCHINELLA. Sure, everything you have laid out there is consistent with some of the threats which we tried to point the flashlight at in our opening statement. You have got essentially a state-owned, or a certainly state-invested company, and you have got an

example of the sort of—you could characterize it as an insider threat, if you will, but the Chinese government's relationships with these kinds of companies, which have a worldwide commercial presence, poses exactly the sort of threat you have identified.

And as my colleague articulated, it is also an indication of the different kind of world we had. We were not buying surveillance cameras from the Soviet Union in those days, but when you have got Chinese companies making world-class equipment on a global market, they pose a threat that is different than we faced during the Cold War.

Mrs. HARTZLER. Okay, thank you.

Mr. CHEWNING. And ma'am, if I might. It is obviously a concern, and something that we are actively working. There are other additional examples like that, that we would be happy to take you through in a classified setting to discuss similar vulnerabilities that we have identified and then what we are doing to remediate them.

Mrs. HARTZLER. That would be great.

Ms. BINGEN. And Ms. Hartzler, if I could also just add, going back to the supply chain discussion we had and the policies associated with that and the congressional engagement and the direction that you have all provided us. You know, there are three areas of the supply chain I worry about. It is going through the front door, the cyber exfiltration and us making it easy for them.

It is—two, exactly what you highlighted, it is the backdoor piece. But then third, there is also the counterfeits part piece, and we need to be able to look holistically at all of those and mitigate threats along all three of those vectors, which the authorization you provided us helps us to start doing.

Mrs. HARTZLER. Okay. Mr. Griffin, you have anything to add?

Secretary GRIFFIN. Shockingly for me, I have nothing useful to add. Thank you, ma'am.

Mrs. HARTZLER. You bet. Mr. Schinella, and also Mr. Griffin, you mentioned in your comments concerns about the universities and the Chinese using the universities. That is something I am very concerned as well. The National Intelligence Council, you have provided us with this chart that shows the different programs that China has in talent recruitment, and of the snapshot that is provided here, approximately two-thirds of these individuals worked or studied in the United States and are employed in China in areas such as defense, research, technology, state-owned enterprises, academia, and things.

Now, Mr. Griffin, you said it is not up to me to give a recommendation, so I will ask Mr. Schinella. Do you think we should change our visa system to deny Chinese students being able to participate in PhD programs?

[The chart referred to can be found in the Appendix on page 55.]

Mr. SCHINELLA. Well, as part of the U.S. intelligence community, it is even less my mandate to make policy recommendations, but as the intelligence product you have illustrates, and as my opening remarks indicated, China, through a state-directed policy, absolutely is trying to make the most licit and illicit, but often through absolutely legal mechanisms, exploitation of their ability to take advantage of the U.S. university system.

Mrs. HARTZLER. Thank you.

The CHAIRMAN. Mr. Bacon.

Mr. BACON. Thank you very much. We appreciate your-all's time today. I wanted to ask you a question about some of the areas that we are seeing bigger advances with technology. Of course, we keep seeing advances in stealth, we are seeing higher capacity computing power, which is changing a lot of our weapon systems, hypersonics, robotic type of investments, but also nanotechnology.

So a few of these—I just want to ask you a question—how did we fall behind, in your mind, in the hypersonics side? Because that is what I keep reading. And what can we learn from that? And I just open it up to anybody.

Secretary GRIFFIN. Well, let me take that one first. We fell behind because while this nation was pioneering in that era, we decided some years back that we did not face a significant threat requiring the delivery of force by means of hypersonic weapons.

Mr. BACON. Yes.

Secretary GRIFFIN. So we—as an earlier questioner asked, we did not transition this.

Mr. BACON. Right.

Secretary GRIFFIN. We could have. We just chose not to. Our adversary, China, has gone on to develop a very, very startling capability in that area. We certainly can match and exceed that capability, and we are setting about that task. But we fell behind because we elected to make other choices, sir. I——

Mr. BACON. And it was probably focused on the Middle East I would assume. Afghanistan, Iraq probably preoccupied our bandwidth.

Secretary GRIFFIN. There is always the tyranny of the urgent——

Mr. BACON. Right.

Secretary GRIFFIN [continuing]. Versus the long term, and truly, I lived through all of this.

Mr. BACON. Yes.

Secretary GRIFFIN. Cold War competition and such. One of my political adversaries once labeled me as an unreconstructed cold warrior. It was not offered as a complement, but I took it as such. So we have, for 25 years, believed——

Mr. BACON. Right.

Secretary GRIFFIN [continuing]. That the era of Great Power competition was over, and it is not.

Mr. BACON. Well, let me ask you—I have been reading about robotic technology, and that Russia's investing a lot into that. Would you say that we are—where are we at with that compared to the Russians? If you can elaborate? If anybody wants to?

Secretary GRIFFIN. I do not believe that I know. I can give you an assessment for the record later, sir. I will say that in the area of autonomy, machine learning, robotics generally, that as my colleague said earlier, and quite well, deserves emphasis, the DOD is a small player with regard to where commercial industry is. Now, that is not bad. Our commercial industrial base is the biggest single asset——

Mr. BACON. Right.

Secretary GRIFFIN [continuing]. That we have for national security. But we need to make it attractive for them to continue work

in this area, and we need to make it attractive for them to partner with us so that we can reap those advantages.

Mr. BACON. Right. One last question in this line, unless some—and I will give somebody else a chance to answer any of these, but on nanotechnology. I keep reading of the importance that maybe 23 years from now what miniaturization will be able to do to the battlefield. Can you all talk about that at all? Because it fascinates me that we will be able to maybe have weapons systems that are quite a bit smaller and harder to detect, and perhaps just as lethal as what we have today.

[Laughter.]

Mr. BACON. Yes.

Mr. CHEWNING. I mean, I think the innovations you are describing are exciting on a lot of fronts because of the warfighting applicability that they have. I also think it draws on an important distinction that we have talked a lot about the type of innovation that we are expecting industry to push to us.

There is also a pull effect. And, the innovation of our warfighters to take technologies like you are describing, experiment with them so we can determine how they will impact doctrine going forward, and then providing that feedback to industry. And so, I think this push-pull concept around how we divine this innovation, we take commercial insight, figure out what the military applicability are is an important part of the equation.

Mr. BACON. Anybody else want to jump in on any of those questions?

Ms. BINGEN. Mr. Bacon, I will go outside my line a bit. No, that is probably dangerous. You know, I do want to bring this back to China a bit as well. And when I look at some of the trends out there, and frankly it is less about us protecting ours, but this is really us making it a national priority in some of these technology areas.

They have got 16 megaprojects; these are Manhattan-style projects. Their global share of R&D expenditures, the U.S. dropped 11 percent between 2000 and 2015, China increased 21 percent. STEM degrees, this is 2014 data, but Chinese universities are putting out 1.3 million students with STEM backgrounds; we are 525,000.

So, just when I think of those numbers and what that portends for the future, you know, the onus is on us to really make these challenges and these technologies a national priority.

Mr. BACON. Okay. Well, thank you so much. And, Mr. Chairman, if we have got time at the end, I have got about one more minute of question if you come back around. But I yield.

The CHAIRMAN. Mr. Banks.

Mr. BANKS. Thank you, Mr. Chairman. Dr. Griffin, I, along with 25 Members of Congress, this week sent a bicameral and bipartisan letter to the Secretary of Education on—earlier this week on Tuesday that expressed our concern about Huawei's links to the Chinese government.

Huawei has so-called quote, research partnerships, with over 50 U.S. universities and is likely using these relationships to exploit the open and transparent culture of our schools and communities as well as gain access to critical next-generation technologies. We know that China has used relationships like these for spying, con-

ducting cyber attacks, and committing industrial and economic espionage.

Meanwhile, the DOD policy that governs technology transfer is dated back to 1999. At that point, we had no idea what an iPhone was, we were worried about Y2K, and the USB flash drive was not even invented. The world, as I am sure you would acknowledge, is very different technologically now than it was 19 years ago.

So, Dr. Griffin, considering the emerging nature of strategic competition with China and the increasing need to protect our critical investments in both academic and private partnerships, what is the DOD doing to protect the DOD-funded research from foreign threats and unvetted members with uncertain loyalties? And, what specifically are you doing to assist the Secretary of Education in mitigating risk to universities and other schools, and help the Federal Government to protect and advance the United States technological advantage?

Secretary GRIFFIN. Sir, that is a bigger question than I believe I can answer here for, the record. I think Eric might be more capable than I. I share your concern. I have several times alluded in this hearing to the number and, in fact, the existence of so many Chinese STEM students in the United States.

I completely share your concern. And, it is well documented that this is an avenue of access for the Chinese that we would not want them to have. Beyond that, I do not have any detail for you. Eric——

Mr. BANKS. Aside, before we move to Eric, are you, too, concerned about the dollars that fund academic research on universities in America that, on our behalf, are engaged in classified research for DOD?

Secretary GRIFFIN. I am concerned that we——

Mr. BANKS. That have ties to Huawei and other——

Secretary GRIFFIN. I am concerned that we are not yet as vigilant as we should be about making sure that that research does not go to places that have those ties. Certainly, universities have a very long, multi-decade history of collaboration with the national security community writ large on problems of national interest. It is one of our greatest strengths. But doing so in an environment that can be penetrated by adversaries is not wise. And we are looking more closely at that.

Mr. BANKS. So, Mr. Chewning, you would agree that we are not as vigilant as we should be, as Dr. Griffin said?

Mr. CHEWNING. Yes. No, I agree 100 percent. We are concerned. We are reviewing the contract language associated with those research projects at the universities. And I think more broadly, this hits on the hard issue of we have an open innovation model.

And, we have an adversary that is within that model, and operates a closed model on their own side. And that we need to experiment to find what structural fix is for that without breaking what makes our system work the best in the world.

Mr. BANKS. Are either of you aware, at all, of any interest by the U.S. Department of Education in these ties or this subject at large? Have you had any conversations with any leaders at the Department of Education?

Secretary GRIFFIN. I have not. I would be happy to do so; but I personally have not. And, of course, another difference between now and 1999, which you cited, was that China had not been admitted to the World Trade Organization in 1999. And I might make the point that that was truly a seminal branch point that allows many of the types of intrusions of which you speak.

Mr. BANKS. Thank you very much. I yield back.

The CHAIRMAN. Let me follow up with just one question for Mr. Schinella and probably Ms. Bingen. As a practical matter for our purposes is should we see any distinction between a Chinese company and the Chinese government? So, if a Chinese company is investing in some technology, some business, something going on—for our, as a practical matter, for our purposes is that—should we see that as the Chinese government doing it?

Mr. SCHINELLA. I would say there is a gradation. But whether you have got a wholly owned state-owned company that essentially is an element of the Chinese government, or largely a genuinely private company that the Chinese government still has leverage over back within China, there may be a spectrum of risk. But, I would say, that at no point on that spectrum is the risk zero.

The CHAIRMAN. Okay. Ms. Bingen, do you have anything to add?

Ms. BINGEN. Mr. Chairman, I would just add the China National Intelligence Law from 2017 says that all organizations and citizens shall support, cooperate with, and collaborate in national intelligence work.

The CHAIRMAN. Yes, that is kind of what I thought. Mr. Bacon, you had a quick question?

Mr. BACON. One quick follow-up. I know CFIUS has a very important role, and we need to protect our technology and make sure it is not being, you know, sold or exported, particularly prematurely.

But, I have a concern. I have heard from a couple of companies where they thought there was some—they were unfairly limited. So, when I have asked CFIUS about this, they go, well, "we are our own appeal authority."

I am wondering, from the DOD perspective, should we not have an appeal authority somewhere in the DOD to say—in case CFIUS gets it wrong once or twice on whatever company that they hold back. You got any thoughts on that?

Mr. CHEWNING. Well, Congressman, if there is any specific case, of course, we are always able to provide briefings to members explaining the rationale and the logic behind why a decision occurred the way it did. I will say, as the representative for the Department on—on the interagency committee, companies may not be aware of the full fact-base that we have because——

Mr. BACON. Right.

Mr. CHEWNING [continuing]. We conduct the RBAs [risk-based assessments] as they are informed by the intelligence community. And so, I could see why certain companies may not think we got it right because they do not have the picture that we do, based on the work from the intelligence community.

Mr. BACON. But—and, I got that. I think—and I would say 99 percent of the time, that is probably the case. But, should there not be a one—some kind of recourse, outside of CFIUS, because it is—

because what I am hearing is you are your own appeal authority. And granted, I am sure you get it right 99 percent of the time.

But I still think from a, just a fairness, that there has got to be some kind of board at the DOD-level. Just to—and it gives you a chance to say, this is why we made that case. And people could agree or disagree. But I think some of the companies would say, they do not—there is no other appeal authority other than CFIUS itself.

And I just—it seems to me there needs to be a check and balance there. And I just—I throw that out as a suggestion.

Mr. CHEWNING. Sure, no. Thanks. No, well, I am certainly happy to take that feedback back to the committee and discuss it.

Mr. BACON. Thank you.

The CHAIRMAN. As luck would have it, votes have been called. So this worked out just right. Thank you all for being here, and for your insights. We will obviously continue to have conversations on this topic.

The hearing stands adjourned.

[Whereupon, at 11:45 a.m., the committee was adjourned.]

A P P E N D I X

JUNE 21, 2018

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

JUNE 21, 2018

House Armed Services Committee Chairman William "Mac" Thornberry
Opening Statement
Full Committee Hearing on: "Military Technology Transfer: Threats, Impacts, and Solutions for the Department of Defense"

June 21, 2018

In his January 19, 2018, remarks on the National Defense Strategy, Secretary Mattis warned that "our competitive edge has eroded in every domain of warfare, air, land, sea, space and cyberspace, and it is continuing to erode." Much of that erosion has been caused by things we have done to ourselves – sequestration and continuing resolutions come to mind.

But part of the erosion in our competitive edge is the result of adversaries and competitors obtaining American technology and intellectual property by legal and often illegal means.

In its January 2018 report, "China's Technology Transfer Strategy," DIUX found that the People's Republic of China, for example, uses a variety of methods to obtain U.S. technology, including:

Industrial espionage, where China is by far the most aggressive country operating in the U.S.;

Cyber theft on a massive scale deploying hundreds of thousands of Chinese army professionals;

Academia, since 25% of U.S. STEM graduate students are Chinese foreign nationals;

China's use of open source information cataloguing foreign innovation on a large scale;

Chinese-based technology transfer organizations;

U.S.-based associations sponsored by the Chinese government to recruit talent; and

Technical expertise on how to do deals learned from U.S. firms.

The report noted that the "cost of stolen intellectual property has been estimated at $300 billion per year."

Most alarming, DIUX found that, "[t]he U.S. does not have a comprehensive policy or the tools to address this massive technology transfer to China" and "[t]he U.S. government does not have a holistic view of how fast this technology transfer is occurring, the level of Chinese investment in U.S. technology, or what technologies we should be protecting."

That is just one report but based on everything that the committee has heard this year, it sounds right and it should be alarming.

There are several provisions in the upcoming NDAA conference which relate to this issue, including the modernization of the CIFUS and Export Control regime. This hearing will better equip us to make important decisions in the days ahead.

House Armed Services Committee Ranking Member Adam Smith
Opening Statement
Full Committee Hearing on: "Military Technology Transfer: Threats, Impacts, and Solutions for the Department of Defense"
June 21, 2018

Thank you, Mr. Chairman for holding this timely hearing. I also wish to thank our panel of witnesses for appearing today. Their expertise will undoubtedly reinforce our understanding of the strategic importance of military technology and how we might best protect it.

The development and safekeeping of key technologies to support decisive military advantages are fundamental priorities for maintaining national security, but these are not new strategic principles. Although technologies and their influences change over time, military organizations have sought to establish technological advantages and to nullify the technological advantages of their competitors throughout the history of armed conflict. A persistent challenge lies in keeping up with the scope and the pace of technological change and all of its potential applications and adapting as necessary.

The Summary of the 2018 National Defense Strategy of the United States of America (the NDS Summary) recognizes this challenge. It states, "The drive to develop new technologies is relentless, expanding to more actors with lower barriers of entry, and moving at accelerating speed." A spectrum of state and non-state actors could obtain militarily significant technologies and leverage them to their advantage, and, given the complexity of the current security environment and the diversity of threats within it, we need to continue to promote innovation, enhance situational awareness, and bolster security standards for sensitive technologies. Regarding the Department of Defense, the NDS Summary asserts, "Maintaining the Department's technological advantage will require changes to industry culture, investment sources, and protection across the National Security Innovation Base."

However, protecting sensitive technologies will require a whole-of-government effort with contributions from numerous federal departments and agencies, including the Departments of State, Treasury, Justice, Commerce, Homeland Security, and Health and Human Services, and various facets of the intelligence and law enforcement communities. The United States government will also need to foster constructive relationships with industry and the science and technology communities and to engage our many allies and partners around the world to uphold sufficient security standards. Strategic competitors like China will demand holistic responses, and far-reaching innovation and technology protection requirements are clear indications that national security involves much more than defense.

The Congress must also stay engaged, as critical innovation and technology protections will continue to require legislative action and oversight. As we

consider relevant legislative proposals aimed at mitigating risk, I hope that we can resist temptations to overreact. Legislative remedies should be carefully and objectively tailored to address verifiable harms. We should take care to avoid legislating in ways that may be over- or under-inclusive, overly disruptive to markets or free enterprise, alienating to academic freedoms, or unjustly discriminatory in their application. I am particularly interested in learning from our witnesses how we might enable the Department of Defense to protect military technologies in a manner that is wholly consistent with our national values.

Thank you, Mr. Chairman. I look forward to our witnesses' testimony.

Department of Defense Joint Testimony on "Military Technology Transfer: Threats, Impacts, and Solutions for the Department of Defense"
Before the House Armed Services Committee
June 21, 2018

Chairman Thornberry, Ranking Member Smith, Members of this Committee: thank you for affording us the opportunity to appear before you today to discuss both a critical and sensitive national security topic: Military Technology Transfer, and what we are doing to maintain our technological advantage over our near-peer adversaries. Due to the sensitive nature of the material and the setting in which we appear before you today, we may be limited in the level of detail we can discuss about the threat and how we address it. However, we stand ready to provide you with further detailed information on any unanswered questions, in the appropriate classified setting.

Threats and Approaches

The Department of Defense is facing an unprecedented threat to its technological and industrial base. Continued globalization and our open society, both in academia and business, has offered China and others access to the same technology and information that is critical to the success of our future warfighting capabilities. China is making significant and targeted investments in the same technologies of interest to the Department. These include artificial intelligence, autonomous vehicles, cybersecurity, and unmanned aerial vehicle (UAV) technology. China has made it a national goal to acquire foreign technologies to not only advance its economy, but also to use these technologies to advance its military capabilities, and it is doing so through both licit and illicit means.

The Department's traditional approach to identifying and countering a foreign threat through technology transfer is not sufficient. Threat briefings to cleared defense contractors and investigations into potential foreign intelligence service activities will not decrease the threat from non-traditional collectors. An example is non-traditional collection. Foreign adversaries are scrutinizing public information, such as our own Department's innovation focus areas, to craft their investment strategies to overmatch our technology. Furthermore, the increasing ease of access to large amounts of unclassified or non-government data in the private sector offers opportunities for exploitation. Some of this data in aggregation can be as damaging as a breach of classified information. On a too frequent basis, we learn of cyber exfiltration potentially harmful to the Department. The combination of cyber exfiltration and the use of non-traditional collection has made this threat unprecedented.

Beyond the cyber exfiltration threat, the Department is seeing the technology transfer threat manifest through numerous non-traditional methods, including talent recruitment, academic collaboration, and supply chain access. Through numerous talent recruitment programs, such as the Thousand Talents Program, China is actively seeking the most talented engineers and scientists from around the world to work in or for Chinese private or public institutions. We have seen the Chinese target top talent in American universities, and research

labs of the private sector, including Defense contractors, and the U.S. Government. Lastly, Chinese access to, and acquisition of, elements of the DoD supply chain -- both inside and outside the United States -- has been a growing threat for the past decade. In some regards, the Chinese government could more easily understand the Department's supply chain through its relationships with sub-tier suppliers than the Department can understand its supply chain through its prime contractors.

Secretary Mattis, in the National Defense Strategy, articulates the protection of the National Security Innovation Base as a key priority for the Department. And while we support strengthening export controls and authorities of the Committee on Foreign Investment in the United States (CFIUS), we do not believe that those efforts alone will stop a motivated adversary. If China is willing to break and circumvent laws to meet its national goals, then we must strengthen the Department's counterintelligence capabilities, elevate the private sector's focus on security, and take a more holistic look at industrial security and supply chain integrity. The Department has four key lines of effort to meet these increasing intelligence and security needs.

1) First, to strengthen counterintelligence, the Department is increasing the number of full time employees in the field and analysts focused on critical technology protection at the Defense Security Service (DSS), and the Department's counterintelligence organizations (NCIS, AFOSI, and Army CI). The Department has also placed a premium on increasing its interagency collaboration with FBI, Homeland Security, State, Treasury, and Commerce to ensure we are actively coordinating and leveraging our authorities to protect top tier technologies.

2) Second, to elevate the private sector's focus on security, the Department has established a "Deliver Uncompromised" initiative focused on industry delivery of capabilities, services, technologies, and weapons systems that are uncompromised by our adversaries from cradle-to-grave. It aims to establish security as a fourth pillar in acquisition, on par with cost, schedule, and performance, and to create incentives for industry to embrace security, not as a "cost center," but as a key differentiator.

3) Third, the Department is implementing a more holistic approach to industrial and information security. We are transitioning from a compliance, checklist-based National Industrial Security Program (NISP) to a risk-based approach informed by the threat and DoD technology priorities. In addition, we are developing the program plan on how to apply these approaches to protect controlled unclassified information (CUI), which includes technical data and personally identifiable information (PII) available to private industry.

4) Lastly, the Department is implementing processes to strengthen the integrity of the supply chain, in large part enabled by Section 806 of the FY11 National Defense Authorization Act (NDAA), and also developing the plan to establish a pilot program to enhance information sharing with cleared defense contractors, as required by Section 1696 of the FY18 NDAA.

The Department expects that, through these efforts, we can begin to mitigate this unprecedented threat to the technology and information critical to our military advantage, and to deliver uncompromised capabilities to our warfighters. We also recognize that strong partnerships with industry, across the interagency, with our allies and partners, and with Congress are key to the successful implementation of these efforts. We thank this committee for its continued focus on the threat, its understanding of the impact to our warfighting capabilities, and its commitment to support the policies, programs, and resources necessary to maintain our technological advantage.

Technology Transfer and Investment

China is executing a multi-decade plan to transfer technology to increase the size and strength of its economy, currently the world's 2nd largest. By 2050, China's economy may be 150% the size of the U.S. which would surpass the size of the US and decrease the relative influence of the U.S. relevance. Technology transfer to China occurs in part through increasing levels of investment and acquisitions of U.S. and foreign companies. China participated in ~16% of all venture deals in 2015, up from a 6% average participation rate from 2010-2015.

China is investing in nascent technologies that are essential for future commercial and, in some instances, potentially military innovations and applications (e.g., artificial intelligence, robotics, autonomous vehicles, augmented and virtual reality, financial technology and gene editing). As a result, the process to determine whether a new product or service should be designated as dual use or a military article will likely become more complicated.

Investments are only one means of technology transfer, which also occurs through illicit activities where the cost of stolen intellectual property has been estimated at $300 billion per year. These activities include: industrial espionage, where China is by far the most aggressive country operating in the U.S.; cyber theft ((i.e., USG, US contractor, and ally and partner country/contractor exfiltration), deploying hundreds of thousands of Chinese army professionals; academia, including U.S. STEM education; China's use of open source information cataloguing foreign innovation on a large scale; Chinese-based technology transfer organizations; U.S.-based associations sponsored by the Chinese government to recruit talent; and technical expertise in financial deal-making, gained from U.S. firms themselves.

China's goals are to be #1 in global market share in key industries, to reduce reliance on foreign technology and to foster indigenous innovation. Through published documents such as Five-Year Plans and Made in China 2025, China's industrial policy is clear in its aims of import substitution and technology innovation. The Department is actively monitoring, through multiple organizations and mechanisms, the evolution of Chinese indigenous innovation in tandem with technology copying, as well as supply chain security in light of increased Chinese investment in necessary equipment and services.

Maintaining Our Technological Advantage

Today we appear before you to discuss the competition we are engaged in with our near-peer competitors, and the ways in which the United States is taking steps to maintain our technological advantage. Technology is transforming the battlespace. This committee, and other committees across Congress, have recognized this fact, and we thank you for doing your part to focus the Department and other agencies on the very real, and very tangible, erosion of our advantage.

It must be emphasized that we have not yet lost our advantage – the United States remains the world's preeminent military power, and we continue to maintain technology superiority. However, in order to continue to maintain this advantage in an environment of vigorous world competition, we must remain vigilant and employ whole-of-government approaches to the problem set at hand. We must not only adapt to our environment, but we must remain the drivers of global technological advances. We must get within the decision loops of our adversaries, and we must increase the speed and efficiency at which we **educate, invent, adapt, prototype, and demonstrate** to respond to current and future threats to ensure and preserve our dominance in the field.

In order to **educate**, we must invest, and education is an area in which the Department is investing heavily to improve our capabilities and workforce, with a focus on cultivating the intellect of our own citizens. The Science, Mathematics and Research for Transformation (SMART) Scholarship for Service Program has been established by the Department of Defense (DoD) to support undergraduate and graduate students pursuing technical degrees in Science, Technology, Engineering and Mathematics (STEM) disciplines. The program aims to increase the number of civilian scientists and engineers working at DoD laboratories by funding undergraduate, graduate, and doctoral degrees with a year-for-year payback. Following graduation, SMART scholarship recipients work in DoD laboratories and facilities. Our investment in education will contribute to accelerating our current modernization priorities by focusing the recruitment and development of the future STEM human capital of this nation to those priorities, such as in the area of microelectronics. These investments in education shall pay dividends to our future success and security as a nation.

The democratization of technological knowledge is the result, in part, of our hyper-connected world, and one of the ways in which our adversaries are attempting to erode our technological superiority. In response, we must continue to **invent**, both as a nation and as a department. While the United States remains tied for third in world-wide intellectual property filings as a percentage of the total number (at 7%), we lead the world in basic and applied research investments.

Innovation requires the courage to try new things, and to potentially fail quickly. We must **adapt** to the changing technological landscape around us, as our adversaries are not only copying our technologies, but also growing their own capabilities domestically. In order to adapt, we must continue to streamline the processes and requirements that unnecessarily slow our development compared to adversaries that simply lack the equivalent hindrance. We must push the envelope with regards to research, and we must innovate with regards to both operations and organizations.

In order to transition innovative ideas to reality, we must **prototype** in a way that balances risk with speed. We must change the idea that a failed test is in itself a failure – the one true failure is when an entire platform is delayed or cancelled due to a flaw being found too late in a program to address. We dramatically increase our risk of such a failure when we design testing to be easily passable, or decrease resources for early prototypes in order to speed the maturation of a platform in a way that may obscure major flaws in design. Congress has sought to address this problem in part through the creation of the Office of the Undersecretary for Research and Engineering, in order to move focus to critical developmental stages such as **prototyping and demonstration**. The Department remains committed to leveraging this and other organizational tools to accelerate the pace at which we develop and test new technologies and platforms, and in turn widen the gap between ourselves and our adversaries.

Congress has given the Department other tools, such as the Joint Federated Assurance Center (JFAC), which grows, shares, and provides expertise to new and innovative capabilities and applications. The JFAC, a current USD(R&E) initiative, is a DoD-level collaboration organization made up of participating Service and Agency labs that possess documented expertise in conducting software and hardware assurance of critical DoD systems. The Missile Defense Agency has successfully piloted the use of existing JFAC service providers to help detect and remediate software vulnerabilities as part of their independent assessments of Ballistic Missile Defense System (BMDS) Tactical Mission System software. JFAC's capabilities include the collaboration between service providers and practitioners with software source code analysis tools, anti-tamper and counterfeit detection capabilities, and a centralized knowledgebase of assessments and guidance from DoD components to deliver value to DoD programs. By pursuing its charter and congressional mandate of Public Law 112-239, JFAC expands its innovative philosophy of sharing software and hardware capabilities, tools, and subject matter expertise to enable the assured critical weapon systems that support our warfighter's mission and lethality.

The Department is also engaged in a broader, multi-vector campaign to maintain technology advantage. In 2016, the Department established a Joint Acquisition Protection and Exploitation cell (JAPEC), a joint analysis capability designed to assess technical information losses and determine the consequences of those losses in order to inform requirements and acquisition, down to programmatic and strategic courses of action. The JAPEC also identifies and prioritizes critical acquisition programs and technologies in need of protection, and takes measures to do so. JAPEC is one example of a collaborative, Department-wide approach, as JAPEC is co-led by USD(R&E) and USD(I), and includes the Military Departments, USD(A&S), USD(P), the DoD CIO, the Defense Security Service (DSS), the Defense Intelligence Agency (DIA), the Joint Staff, and the Missile Defense Agency as members.

As a critical piece of this campaign, the Department established a Maintaining Technology Advantage Cross-Functional Team (CFT) to address the globalized and commercialized technology development environment. The team developed a three-pronged campaign plan to address the speed, scope, and agility of the complex technology development ecosystem. These prongs are Promote (leaning forward to spur the S&T enterprise through investments in human capital), Protect (improving our mechanisms to monitor and limit illicit or

unintended technology transfer), and Combat (identifying exploitation opportunities and activities in order to support acquisition protection by raising adversary cost). The team's plan is implemented by conducting careful analysis and integration of DoD's needs, coupled with improvement of internal DoD process, and engagement with external stakeholders to include academia, industry, and both interagency and international partners.

While our adversaries have focused their research and development efforts in order to close the gap on the technological advantage of the United States, we remain vigilant in addressing this multi-faceted advance on numerous fronts. Through both our Department-wide and inter-agency approaches, as well as welcome help from Congress, we continue to accumulate the mechanisms for success and the tools to maintain dominance.

Dr. Michael D. Griffin
Under Secretary of Defense for Research and Engineering

Dr. Michael D. Griffin is the Under Secretary of Defense for Research and Engineering. He is the Department's Chief Technology Officer, and is responsible for the research, development, and prototyping activities across the DoD enterprise and is mandated with ensuring technological superiority for the Department of Defense. He oversees the activities of the Defense Advanced Research Projects Agency, the Missile Defense Agency, the Strategic Capabilities Office, Defense Innovation Unit Experimental, the DoD Laboratory enterprise, and the Under Secretariate staff focused on developing advanced technology and capability for the U.S. military.

Mike was previously Chairman and Chief Executive Officer of Schafer Corporation, a professional services provider in the national security sector. He has served as the King-McDonald Eminent Scholar and professor of Mechanical and Aerospace Engineering at the University of Alabama in Huntsville, as the Administrator of NASA, and as the Space Department Head at the Johns Hopkins University Applied Physics Laboratory. He has also held numerous executive positions in industry, including President and Chief Operating Officer of In-Q-Tel, CEO of Magellan Systems, and EVP/General Manager of Orbital ATK's Space Systems Group. Griffin's earlier career includes service as both Chief Engineer and Associate Administrator for Exploration at NASA, and as the Deputy for Technology at the Strategic Defense Initiative Organization. Prior to joining SDIO in an executive capacity, he played a key role in conceiving and directing several "first of a kind" space tests in support of strategic defense research, development, and flight-testing. These included the first space-to-space intercept of a ballistic missile in powered flight, the first broad-spectrum spaceborne reconnaissance of targets and decoys in midcourse flight, and the first space-to-ground reconnaissance of ballistic missiles during the boost phase. Mike also played a leading role in other space missions at the John Hopkins University Applied Physics Laboratory and NASA's Jet Propulsion Laboratory.

Griffin has been an adjunct professor at the University of Maryland, Johns Hopkins University and George Washington University, teaching spacecraft design, applied mathematics, guidance and navigation, compressible flow, computational fluid dynamics, spacecraft attitude control, estimation theory, astrodynamics, mechanics of materials, and introductory aerospace engineering. He is a registered professional engineer in California and Maryland, and the lead author of some two dozen technical papers and the textbook Space Vehicle Design.

He is a member of the National Academy of Engineering and the International Academy of Astronautics, an Honorary Fellow and former president of the American Institute of Aeronautics and Astronautics, a Fellow of the American Astronautical Society, and a Senior Member of the Institute of Electrical and Electronic Engineers. He is the recipient of numerous honors and awards, including the NASA Exceptional Achievement Medal, the AIAA Space Systems Medal and Goddard Astronautics Award, the National Space Club's Goddard Trophy, the Rotary National Award for Space Achievement, the Missile Defense Agency's Ronald Reagan Award, and the Department of DoD Distinguished Public Service Medal, the highest award which can be conferred on a non-government employee.

Griffin obtained his B.A. in Physics from the Johns Hopkins University, which he attended as the winner of a Maryland Senatorial Scholarship. He holds master's degrees in aerospace science from Catholic University, electrical engineering from the University of Southern California, applied physics from Johns Hopkins, civil engineering from George Washington University, and

business administration from Loyola University. He received his Ph.D. in aerospace engineering from the University of Maryland, and has been recognized with honorary doctoral degrees from Florida Southern College and the University of Notre Dame.

Mike is a 4000+ hour commercial pilot and flight instructor with instrument and multiengine ratings, and holds an Extra Class Amateur Radio license.

Kari A. Bingen
Principal Deputy Under Secretary of Defense for Intelligence

The Honorable Kari A. Bingen was nominated by President Trump as the Principal Deputy Under Secretary of Defense for Intelligence (PDUSD(I)) and unanimously confirmed by the United States Senate in May 2017.

As the PDUSD(I), Ms. Bingen is the deputy to the Under Secretary of Defense for Intelligence (USD(I)), the Honorable Joseph D. Kernan, who is the principal intelligence, counterintelligence and security advisor to the Secretary of Defense (SecDef), and the SecDef's principal representative to the Intelligence Community. The USD(I) is also dual-hatted as the Director of Defense Intelligence in the Office of the Director of National Intelligence, and reports to the DNI in that capacity. The USD(I) exercises authority, direction, and control on behalf of the SecDef over the National Security Agency/Central Security Service, the Defense Intelligence Agency, the National Geospatial- Intelligence Agency, the National Reconnaissance Office, and the Defense Security Service. The USD(I) establishes policy and priorities; and oversees the Defense Intelligence Enterprise, consisting of more than 110,000 component employees, and an annual budget of over $54B. This includes the Military Intelligence Program, the Defense portion of the National Intelligence Program and the Battlespace Awareness portfolio.

From 2013 to 2017, Ms. Bingen served as the House Armed Services Committee (HASC) Policy Director. Beginning in 2006, Ms. Bingen served in support of the Strategic Forces subcommittee of the HASC where she advised members conducting oversight of military intelligence programs, military space operations, missile defense, and the nuclear security enterprise of the DoD and Department of Energy.

Prior to entering government, Ms. Bingen was employed with SRA International's Adroit C4ISR Center as a space systems analyst. She also served as a senior space policy analyst at the Aerospace Corporation's Center for Space Policy and Strategy.

She is a graduate of the Massachusetts Institute of Technology with a degree in Aeronautics and Astronautics and a 2002 NRO Technology Fellow.

Eric D. Chewning
Deputy Assistant Secretary of Defense, Manufacturing and Industrial Base Policy

Appointed in October 2017, Mr. Eric Chewning currently serves as the Deputy Assistant Secretary of Defense for Manufacturing and Industrial Base Policy (MIBP). In this capacity, he is the principal advisor to the Under Secretary of Defense for Acquisition and Sustainment (A&S) for analyzing the capabilities, overall health, and policies concerning the industrial base on which the Department relies for current and future warfighting capabilities and requirements. MIBP is also responsible for developing the Department's position on the business combinations and transactions, both foreign and domestic, that shape and affect national security.

Mr. Chewning has over 17 years of experience advising decision makers in military-industrial markets. Prior to his assignment with the Office of the Secretary of Defense, he was a partner with the global management consulting firm McKinsey & Company, where he worked alongside financial sponsors and corporate leaders in the global aerospace, defense, government services, and space industries.

Mr. Chewning's analysis of foreign policy, military strategy, and the defense industrial base has been featured in a variety of national media outlets, including: American Interest, Defense News, Military Review, and War on the Rocks. A former US Army officer, he served as the tactical intelligence officer for the 1st Battalion 5th Cavalry Regiment and as a strategic intelligence officer at the National Ground Intelligence Center (NGIC). He is a veteran of Operation Iraqi Freedom and participated in the evacuation of New Orleans during Hurricane Katrina.

Prior to his military service, Mr. Chewning was an investment banker at Morgan Stanley & Co. where he focused on corporate finance and mergers & acquisitions in the global industrials sector.

He received a MBA from the Darden School of Business at the University of Virginia where he was recognized as a Shermet Scholar. He also earned a MA in international relations and BA with honors from the University of Chicago.

DOCUMENTS SUBMITTED FOR THE RECORD

JUNE 21, 2018

China's Technology Development Strategy

Non-Traditional Collectors	China uses individuals for whom science or business is their primary profession to target and acquire US technology.
Joint Ventures (JV)	China uses JVs to acquire technology and technical know-how.
Research Partnerships	China actively seeks partnerships with government laboratories-such as the Department of Energy labs-to learn about and acquire specific technology, and the soft skills necessary to run such facilities.
Academic Collaborations	China uses collaborations and relationships with universities to acquire specific research and gain access to high-end research equipment. Its policies state it should exploit the openness of academia to fill China's strategic gaps.
S&T Investments	China has sustained, long-term state investments in its S&T infrastructure.
M&A	China seeks to buy companies that have technology, facilities and people. These some-times end up as Committee on Foreign Investment in the United States (CFIUS) cases.
Front Companies	China uses front companies to obscure the hand of the Chinese government and acquire export controlled technology.
Talent Recruitment Programs	China uses its talent recruitment programs to find foreign experts to return to China and work on key strategic programs.
Intelligence Services	The Ministry of State Security (MSS), and military intelligence offices are used in China's technology acquisition efforts.
Legal and Regulatory Environment	China uses its laws and regulations to disadvantage foreign companies and advantage its own companies.

1802-00210

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

JUNE 21, 2018

QUESTIONS SUBMITTED BY MS. SPEIER

Ms. SPEIER. Our adversaries see academia as a soft target for recruitment, collection, and influence, as indicated by countless cases where college campuses were used to acquire sensitive information and influence sensitive conversations. What role can and is DOD playing to help develop a strategy that protects our intellectual property and sensitive technology on college campuses when many of China and Russia's activities are considered par-for-the-course, normal activities in an academic setting?

Secretary GRIFFIN. I am personally concerned that we are not as vigilant as we should be about making sure that that our research doesn't go to into the hands of our adversaries. Academic institutions specifically have a very long, multi-decade history of working on some of our nation's most interesting research challenges and in that environment our research is currently open to all students of those institutions. We are building an information campaign to educate our academic institutions on the potential threats to national security being pursued by our adversaries. We are establishing forums with Universities to discuss how best to mitigate these threats and yet retain access to the bright minds of students and researchers from around the world.

Ms. SPEIER. Who oversees dealing with technology transfer and technology protection within the Intelligence Community? How do the DOD and IC roles and responsibilities with respect to technology transfers and protections fit within a whole-of-government approach to protect sensitive technology?

Mr. SCHINELLA. [Response recorded elsewhere.]

Ms. SPEIER. Our adversaries see academia as a soft target for recruitment, collection, and influence, as indicated by countless cases where college campuses were used to acquire sensitive information and influence sensitive conversations. What role can and is the ODNI playing to help develop a strategy that protects our intellectual property and sensitive technology on college campuses when many of China and Russia's activities are considered par-for-the-course, normal activities in an academic setting?

Mr. SCHINELLA. [Response recorded elsewhere.]

Ms. SPEIER. Who oversees dealing with technology transfer and technology protection within the Department of Defense? How do the DOD and IC roles and responsibilities with respect to technology transfers and protections fit within a whole-of-government approach to protect sensitive technology?

Ms. BINGEN. Oversight of technology protection is a shared responsibility the Department, including the Under Secretary of Defense for Intelligence (USD(I)), the Under Secretary of Defense for Acquisitions and Sustainment (USD(A&S)), the Under Secretary of Defense for Research and Engineering (USD(R&E)), and the Under Secretary of Defense for Policy (USD(P)). The Military Departments and the individual program managers also play a key role in safeguarding critical technologies. Specifically, the Office of the USD(I), oversees a number of efforts to protect the Department's critical technologies. Through the "Deliver Uncompromised" effort, the OUSD(I) is working to elevating the private sector's focus on securing its capabilities, technologies, and weapons systems from our adversaries. OUSD(I) also plays a role in cross-DOD efforts, such as the Joint Acquisition Protection and Exploitation Cell (JAPEC). JAPEC seeks to integrate intelligence, counterintelligence, security, law enforcement, and acquisition efforts across the Department. We also leverage interagency partnerships with the FBI, Commerce, Homeland Security, and the Office of the Director for National Intelligence. These collaborative partnerships are necessary not only to increase the Department's understanding and awareness of the threat, but also to leverage additional authorities that are external to the Department. The Defense Security Service (DSS) is central to protecting DOD technologies that are developed under classified contracts by our industrial partners. The "DSS in Transition" initiative is an effort to shift DSS from a compliance-based approach to a risk-based approach of industry oversight. Through an understanding of a company's technologies and our adversaries' methods to acquire that technology, DSS is facilitating and collaborating with private industry to develop tailored security plans.

Ms. SPEIER. Our adversaries see academia as a soft target for recruitment, collection, and influence, as indicated by countless cases where college campuses were used to acquire sensitive information and influence sensitive conversations. What role can and is DOD playing to help develop a strategy that protects our intellectual property and sensitive technology on college campuses when many of China and Russia's activities are considered par-for-the-course, normal activities in an academic setting?

Ms. BINGEN. From a counterintelligence perspective, the Office of the Under Secretary of Defense for Intelligence (OUSD(I)) is involved in three major efforts to protect DOD's critical technologies and intellectual property that are being targeted by our adversaries through collection on college campuses. First, OUSD(I) is adjusting security and counterintelligence resources and approaches to strengthen our ability to apply counterintelligence protections, conduct outreach, and carry out fieldwork. Second, we are focusing on engaging our interagency partners to leverage a whole-of-government response against such efforts by our adversaries. Third, OUSD(I) is working with Congress to explore additional authorities and programs that would strengthen DOD's capabilities to respond to the threat. One such example is to prohibit foreign students and researchers who have taken part in foreign talent recruitment programs (such as China's Thousand Talents Program) from participating in DOD-funded or sponsored research programs on college campuses.

Ms. SPEIER. Our adversaries see academia as a soft target for recruitment, collection, and influence, as indicated by countless cases where college campuses were used to acquire sensitive information and influence sensitive conversations. What role can and is DOD playing to help develop a strategy that protects our intellectual property and sensitive technology on college campuses when many of China and Russia's activities are considered par-for-the-course, normal activities in an academic setting?

Mr. CHEWNING. It is imperative that U.S. academic institutions and research and development (R&D) labs are made aware of the serious threat posed by the widespread collection of sensitive U.S. science and technology (S&T) information through open academic and recruitment channels. Academic and R&D stakeholders must understand that this threat potentially erodes broad swaths of our society, including our academic and S&T excellence, economic vitality, industrial base, and national security. DOD's Manufacturing and Industrial Base Policy (MIBP) office recently initiated a campaign to inform S&T universities nationwide of the relentless tactics aimed at acquiring information, transferring critical technologies, and recruiting top talent to ultimately apply this knowledge to advance their own foreign interests, to include military and dual-use capabilities. MIBP's academic outreach campaign, which is coordinated with the Office of Under Secretary of Defense for Intelligence, will include discussions with researchers to identify over-the-horizon technologies that would be of great interest to our adversaries. An informed U.S. academic and research body at large will be more disposed to consider DOD and U.S. Government (USG) solutions to the pervasive threat of foreign collection. Solutions range from guidelines on restricting and monitoring access to information and facilities to oversight, protection, and support of select programs. Positive, proactive engagements with academics and others at the leading edge of U.S. technology R&D will be paramount to DOD's success in constantly modernizing and protecting the defense industrial base and, ultimately, future warfighting capabilities.

QUESTIONS SUBMITTED BY MS. ROSEN

Ms. ROSEN. The National Security Strategy of December 2017 states that "The United States will reduce the illicit appropriation of U.S. public and private sector technology and technical knowledge by hostile foreign competitors." How can we use blockchain—or other encryption/verification technology—to improve our cybersecurity and identify how foreign actors are illicitly acquiring U.S. intellectual property?

Secretary GRIFFIN. The Department continues to investigate methods of encryption technology to improve our cybersecurity and identify how foreign actors are illicitly acquiring U.S. intellectual property. The use of blockchain to improve our cybersecurity is still in its early stages and is not a guaranteed solution. Blockchain is built on widely understood and sound cryptographic principles that may help improve identity access and management/trusted credentials. However, there are issues with blockchain and similarly with current encryption/verification technology that must be considered as we continue to improve our cybersecurity and identify how foreign actors are illicitly acquiring U.S. intellectual property. These include how to deal with malicious users, how controls are applied, and the limitations of any encryption/verification technology implementation Technological ad-

vancements promise the development of computers that process information not according to the rules of classical physics and probability, as they today, but according to the rules of quantum mechanics. While quantum information itself is not yet developed to a high technology readiness level, neither are the defenses against the algorithms that quantum computation promises. Both are subjects of active research and may show interesting developments in the next decade.

Ms. ROSEN. The National Security Strategy of December 2017 states that "The United States will reduce the illicit appropriation of U.S. public and private sector technology and technical knowledge by hostile foreign competitors." How can we use blockchain—or other encryption/verification technology—to improve our cybersecurity and identify how foreign actors are illicitly acquiring U.S. intellectual property?

Mr. SCHINELLA. [Response recorded elsewhere.]

Ms. ROSEN. The National Security Strategy of December 2017 states that "The United States will reduce the illicit appropriation of U.S. public and private sector technology and technical knowledge by hostile foreign competitors." How can we use blockchain—or other encryption/verification technology—to improve our cybersecurity and identify how foreign actors are illicitly acquiring U.S. intellectual property?

Ms. BINGEN. Blockchain is one of many evolving encryption/verification technologies that the Department is exploring to improve the protection of our critical technologies. We recognize the value of technology to improve our cybersecurity posture. However, technology alone does not sufficiently address the threat posed by our adversaries. To properly address this threat, DOD must employ a number of different approaches, including enhanced counterintelligence resources, collaboration with interagency partners, and outreach to our partners in industry.

Ms. ROSEN. The National Security Strategy of December 2017 states that "The United States will reduce the illicit appropriation of U.S. public and private sector technology and technical knowledge by hostile foreign competitors." How can we use blockchain—or other encryption/verification technology—to improve our cybersecurity and identify how foreign actors are illicitly acquiring U.S. intellectual property?

Mr. CHEWNING. The Department is aware of foreign countries' efforts to exploit vulnerabilities in our networks to access information about U.S. technology and intellectual property and is evaluating innovative ways to secure critical information and avoid compromise or manipulation of cyber-enabled systems. Blockchains are public ledgers that securely store records of transactions in a way that is permanent and unalterable. Blockchain technology provides strong protection from malicious data tampering, and can be used to validate provenance of items within complex supply chains. Blockchain's distributed and decentralized network architecture is inherently resilient. When every node has a complete copy of the ledger there is no single point of failure, which means network operations can proceed even if some nodes are under attack. Although this technology is relatively new, blockchains with sound underlying cryptographic algorithms and adequate protocol implementation could be a successful tool to help secure DOD information, limit the impact of cyberattacks, and facilitate the identification of the foreign actors trying to acquire U.S. intellectual property. This year the Chief Information Officer submitted a briefing to Congress, as requested in Section 1646 of the 2018 NDAA, highlighting potential uses of blockchain to protect DOD as well as commercial data and transactions. Across the Federal government, identified opportunities include citizen services, identity management, benefits management, contract management, regulatory compliance, and disaster recovery.

○