STATEMENT OF

MICHAEL D. GRIFFIN

UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING

before the

HOUSE ARMED SERVICES

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

FY2020 SCIENCE AND TECHNOLOGY POSTURE HEARING

28 MARCH 2019

INTRODUCTION

Chairman Langevin, Ranking Member Stefanik, and Members of this Subcommittee: thank you for the opportunity to discuss the role of the Office of the Under Secretary for Research and Engineering (OUSD R&E) in advancing defense modernization in response to resurgent adversaries making dogged investments to outpace us and win the long game.

I am joined today by the Service Acquisition Executives to highlight the ways in which the Department of Defense (DoD) is working to change its processes, culture, and investment decisions to ensure we maintain the technical dominance necessary to deter our adversaries for as long as they choose to posture themselves as adversaries. As the Chief Technology Officer for the Department, it is my job to align the Department's investment portfolio in accordance with the modernization priorities outlined in the National Defense Strategy (NDS). I cannot do it alone. We must work together to counter the threats posed by our adversaries.

CHINESE AND RUSSIAN THREATS

I believe we all understand that we are now in an era of renewed great power competition. Our adversaries have self-declared, and our only choice is to respond appropriately, or cede the primacy of the rules-based order that the United States established in the aftermath of World War II and nurtured for three full generations.

Today China and Russia are actively challenging the current status quo while advancing indigenous military technologies at disturbing rates. China has doubled its defense budget in the last decade, has built and armed islands in the international waters of the South China Sea, has weaponized technologies from space and hypersonics to cyber and directed energy, and commits rampant theft of intellectual property, all to impose its will upon sovereign nations across the globe. Russia invaded Georgia and Ukraine, flouted the INF treaty, committed cybercrimes on a global scale, and publicly touts the development of new strategic nuclear hypersonic systems. Both nations have invested significantly in systems designed to disrupt, damage, and degrade U.S. space assets, holding at risk the systems we depend upon both to sustain our economy and to enable the American way of war.

The United States pioneered many of these technologies years or even decades ago, yet we chose not to develop them into military capabilities. But our adversaries get a vote, and their votes have been cast. The United States must respond.

MODERNIZATION PRIORITIES OF THE NATIONAL DEFENSE STRATEGY

The 2018 National Defense Strategy (NDS) outlines a clear approach to regaining and maintaining our once unquestioned technical advantage through investments in key modernization priorities: hypersonics, directed energy, space, autonomy, cyber, quantum science, microelectronics, biotechnology, artificial intelligence and machine learning (AI/ML), and fully-networked command, control, and communication. To pursue these priorities, the

President's Fiscal Year 2020 (FY20) budget request includes $14.1 billion for the cross-department Science and Technology enterprise, a 3% increase from the 2019 request. As Acting Secretary Shanahan noted, the FY20 budget directs more than $7.4 billion to the development and fielding of technologies for the future fight.

The Department has moved decisively to outpace our adversaries across these priorities:

<u>Hypersonics</u>

Hypersonic capabilities remain a major Department-wide modernization focus, and DoD is accelerating hypersonic systems development and demonstration. The $2.6 billion requested for hypersonics in FY20 represents an increase over the FY19 enacted amount. Moreover, DoD is nearly doubling our long-term investments from $6 billion to $11.2 billion over the next five years. We have significantly increased flight testing, as we intend to conduct approximately 40 flight tests over the next few years, to accelerate the delivery of capability to our warfighters years earlier than previously planned.

<u>Space</u>

Given the increased adversarial activity of China and Russia in space, the Department is changing how we field critical capabilities. The newly-formed Space Development Agency's (SDA) task is to field critical space technologies outside normal acquisition processes and at a more rapid pace. The FY20 budget request for SDA is $149.8 million, reflecting the creation of a lean organization that will complement existing DoD space organizations.

As its first priority, SDA will work with elements across the Department and industry to develop proliferated low Earth orbit (P-LEO) space sensors system in support of a number of mission areas.

<u>Directed Energy</u>

Achieving near-term directed energy technology progress is vital—moving from laboratories to weapons platforms. Our plan, in coordination with the services, accelerates operational weapon system development. Through our Laser Scaling Program, four teams are on the path to build 300 kW high-energy lasers by 2022, increasing to 500-1000kW capability over the next decade. We have partnered with the Special Operations Command to accelerate programs for airborne and land-based laser strike weapons, with initial operational capability by Fiscal Year 2024.

<u>Artificial Intelligence and Machine Learning</u>

In the field of AI/ML, the Defense Advanced Research Projects Agency (DARPA) continues to build on work begun almost 60 years ago, when they developed the expert-system technologies utilized in everyday tools such as tax preparation software. More recently, DARPA launched its $2 billion AI NEXT campaign, a multi-year effort to grow the current "second wave" of AI while exploring and creating the future "third wave." This work will be critical to making AI/ML less brittle, more accurate, and a more reliable partner for human operators by reinforcing and supplementing decision making. DARPA, along with the Defense Innovation Unit (DIU) and the broader R&E enterprise, are working with the new Joint Artificial Intelligence Center to

apply existing AI technologies to real-world problems, and scale and deploy successful applications.

Cyber Security

Our adversaries recognize cyber as a weapon, and therefore so must we. Defense against intrusions, as well as the development of tools and techniques to hold adversary assets at risk, is another critical priority for the R&E enterprise. We must also partner with colleagues in the intelligence community and other U.S. government agencies.

Further, as we expand our capabilities in space, with AI/ML, and moving into 5G wireless technologies, we expand the avenues for adversary action against our networks and systems even as we expand the opportunities these new approaches bring. Distributing and diluting our hardware attack surface, whether in space or in the "internet of things," does no good if we ignore the vulnerabilities of the expanded cyber attack surface. Our initiatives in AI/ML, space, 5G, and other attractive new technologies must be accompanied by an awareness of and attention to the cyber vulnerabilities they create. Cybersecurity initiatives will thus be critical across the range of NDS modernization priorities.

Microelectronics

The U.S. presently lacks the domestically owned foundries that have in the past produced uncompromised, state of the art semiconductors for both commercial and national security applications. Equally important is the need to focus on technologies that allow us to operate securely in an environment where hardware, systems and networks are known to be compromised. Industrial base development in this area is critical, and we are working with industry to assess and understand their challenges. We will continue our efforts with the Office of the Director of National Intelligence and the Department of Energy National Nuclear Security Administration to develop fiscally responsible and realistic options, including investments, incentives, and regulatory approaches, to provide long-term, economically-viable sources to meet our needs for state-of-the-art microelectronics.

Quantum Science

While quantum science and technology will be important in the future, they are still in their formative stages. Despite media hype, we are many years from functional quantum computers. However, there is justifiable optimism that quantum clocks, magnetometers, and inertial navigation sensors could be available in a few years. Such devices could greatly reduce our dependence on space-based or other external systems for critical position, timing, and navigation functions, an important consideration for military operations in a GPS-denied environment. In R&E, we will work with USG partners from the National Science Foundation to the intelligence community to contribute to quantum computing advances, but our focus will be on deployment of clocks and development of sensors.

THE OUSD R&E ORGANIZATION

Section 901 of the FY17 NDAA re-established position of Under Secretary of Defense for Research and Engineering (USD R&E) for the first time since 1986, formally splitting the Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics into two components. The USD R&E is charged with directing research and development funding priorities across the Department, with conducting independent technical risk assessments of major programs, and is the DoD Chief Technology Officer. Our job is to shape the future force in such a forbidding manner that no adversary ever believes that today is the day they can confront America and win.

The 2018 NDS is our guide, further informed by seasoned judgement and awareness of the evolving threat. The OUSD R&E organization is built around the NDS modernization priorities, and is composed of two major entities: Research and Technology (R&T), which includes oversight of the labs, Federally Funded Research and Development Centers, University Affiliated Research Centers, and academic research, and Advanced Capabilities (AC), which accelerates and prototypes more mature technologies. AC also oversees the Department's conduct of developmental test and evaluation, and investment in the associated range infrastructure through the Test Resource Management Center (TRMC). Each entity is headed by a Director for Defense Research and Engineering (DDRE), and between them, DDRE (RT) and DDRE (AC) comprise the research, development, engineering, prototyping, test and evaluation responsibility of the Office of the Secretary of Defense (OSD).

Within these two major arms are the critical foci of the new R&E organization: the Assistant Directors for each modernization priority, individuals charged with serving as Department-wide "portfolio managers" for each priority. They work closely with the military services and defense agencies to establish and advise Department leadership on budgetary and programmatic priorities, to avoid unintended programmatic duplication and unnoticed capability gaps, and to ensure that we are focusing our resources as best we can in their areas of responsibility. The exception is the Assistant Director for AI/ML. Because of the importance and interdisciplinary nature of the AI/ML enterprise, it will report directly to the Under Secretary and Deputy.

Several agencies crucial to the national research and development enterprise fall within the R&E enterprise: DARPA, DIU, the Strategic Capabilities Office (SCO), the Missile Defense Agency (MDA), the Strategic Intelligence Analysis Cell, and the new SDA.

MDA, with a $9.4 billion FY20 budget request, is charged to develop a more capable, more reliable, and more lethal missile defense system. This request includes $157 million for hypersonic defense and $304 million for technology maturation initiatives. MDA also has a critical role in responding to the evolving threat environment in space, as well as contributing to Department-wide technology initiatives, such as ongoing laser scaling efforts.

DARPA, with a $3.5 billion FY20 budget request, has a 60-year legacy of developing breakthrough technologies and capabilities that both avoid and impose technological surprise. DARPA remains in my opinion one of this nation's brightest crown jewels. I am honored to be able to assist and support that agency in carrying out its mission.

SCO, with a $1.4 billion FY20 budget request, identifies, demonstrates, and provides near-term capabilities to deliver new effects for the warfighter. By working closely with the military services and combatant commanders to leverage existing technologies for new and disruptive uses, SCO moves the needle on regaining the element of surprise.

DIU, with a $164 million FY20 budget request, seeks out commercial products and capabilities with the potential for military application, but which have not or would be otherwise unlikely to come to the attention of DoD. By offering a connection to the potential military user, with an expedited contracting process, DIU provides a channel to some of the highest technology, fast-paced, and adaptive segments of the U.S. industrial base. DIU will manage the National Security Innovation Capital (NSIC) program, pursuant to the Congressional direction of Section 230 of the FY19 NDAA, which will focus on dual-use hardware, a sector underserved by U.S. venture capital. In an effort to put similarly-focused organizations under a single leadership structure, I have asked DIU also to assume responsibility for the National Security Innovation Network (NSIN), formerly MD5, the National Security Technology Accelerator which focuses on human capital and commercializing technology from DoD labs.

SIAC, with an FY20 budget request of $26.1 million, collaborates with the Joint Staff, Services, and the Intelligence community to provide an operational, technical, and threat-based analytic foundation to help inform technology strategies and decisions across the R&E enterprise.

PROTECTING CRITICAL TECHNOLOGY

OUSD R&E executes numerous technology protection initiatives designed to foil adversary attempts to exfiltrate national security information and intellectual property (IP). We are, by now, all too familiar with the many examples of both illicit behavior and behavior which is technically legal but designed by adversaries to benefit from the hard-won knowledge and experience gained by U.S. innovators.

I, too, am concerned about these things, and I have spent a good portion of this testimony discussing the means by which we intend to help combat these threats. I would now like to turn the coin over and examine the other side.

I have watched for a generation and more as we have tried to protect our unquestioned earlier advantage in aerospace technology through export control mechanisms such as the International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR). While these and related attempts to ensure American security by controlling access to our markets have been effective in the short term, they have not been effective in the long term.

It is my judgement, my personal opinion, that the practical effect of our export control regulations has been that other nations – allies as well as adversaries – have simply decided to invest in the development of their own capabilities, which they have then taken to the global marketplace – a marketplace from which the US has removed itself. Worse yet, by withdrawing much of our own industrial base from the global market, we restrict the competitive environment for our domestic firms, which over time has the effect of eroding the technological advantage we

so eagerly want to protect.   I invite anyone to open their favorite internet search engine and enter keywords such as "ITAR free satellite"; the results are sobering.

My experience in aerospace causes me to be very concerned that, when we talk about restricting competition on the newer playing fields of microelectronics, artificial intelligence, next-generation communication networks, etc., we are merely changing the older "aerospace nouns" for newer nouns, while leaving all the same verbs in place. I believe that we must go with the strategy that got us to where we are today: we are the nation, we are the people, ours are the enterprises from whom and which others want to steal. Our adversaries are trying to steal our IP, we are not trying to steal theirs. China wants to send its students to our universities; we aren't trying to send our students to theirs. It is when others no longer want what we have that I will truly begin to worry.

I am not proposing that we open everything we know to the goal of unfettered global competition. We must wisely implement export controls so as to protect both critical technology and U.S. competitive advantage. There are some things that simply must be protected, and some actors from whom such protection is most important. But we must be explicit about what we want to protect, from whom we want to protect it, and clever about how we do so, especially in regard to emerging technologies. For example, we should not wall off artificial intelligence, but we may want to protect certain data sets. We need to devise protections that are dynamic and do not hinder U.S. competitiveness, and government cannot do it alone. As we consider the implementation of the Export Control Reform Act of 2018, we should engage both academia and the private sector to establish an effective regime that preserves rather than erodes U.S. competitiveness in the global marketplace.

We also need to address the leakage of leading-edge IP from our academic institutions. We need more counterintelligence resources, and we need to educate our universities to the threats of industrial espionage and ensure they employ best practices to protect sensitive research.

Finally, we need to ensure that there is sufficient national and long-term investment in science and technology. We will continue to stay ahead of our adversaries if we believe, and invest, in ourselves and in the strategy that got us here.

CONCLUSION

Both Department and Congressional leadership clearly understand the emerging threat posed by China and Russia because of their ever-increasing adversarial behavior across multiple fronts. As the NDS states, we cannot expect success fighting tomorrow's conflicts with yesterday's weapons. Our adversaries have watched as we have been embroiled in numerous local and regional conflicts. They know how we fight.

If we are to respond, if we are to maintain the global rules-based order that we, in company with our partners and allies, have led for three generations, we must respond. We must up our game. It is not our purpose to draw even with those who reject the values we espouse and the freedoms we protect. We seek dominance, we seek unquestioned advantage, so that on every single day

every single adversary declines to start the fight – because they know they would lose. OUSD R&E, in collaboration with the military services, defense agencies, and combatant commanders, will work to ensure that dominance is sustained.