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.