DEPARTMENT OF STATE

WRITTEN TESTIMONY

OF

EDWARD J. RAMOTOWSKI

DEPUTY ASSISTANT SECRETARY OF STATE

BUREAU OF CONSULAR AFFAIRS

DEPARTMENT OF STATE

BEFORE THE

UNITED STATES SENATE

COMMITTEE ON HOMELAND SECURITY & GOVERNMENTAL AFFAIRS

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

NOVEMBER 19, 2019

Chairman Portman, Ranking Member Carper, thank you for the opportunity to testify today about the Department of State's role in safeguarding our national security and the visa screening process, particularly as it pertains to Chinese nationals. We share the concerns expressed by the Subcommittee and our interagency partners regarding the threat certain Chinese talent programs pose to our national security, and the risks associated with certain Chinese students and researchers engaging in the nontraditional collection of sensitive technology and information. We have no higher priority than the safety of our fellow citizens at home and overseas and we are fully dedicated to the protection of our borders from threats such as the ones you have detailed here today. The Department of State continues to refine its visa security screening procedures to stay ahead of these threats.

In his recent testimony to the Senate Foreign Relations Committee, Assistant Secretary for East Asian and Pacific Affairs David Stilwell spoke about Beijing's strategy of military-civil fusion. This policy prioritizes the development or acquisition of advanced technology that is useful militarily, either for the modernization of the People's Liberation Army or for other domestic security purposes, such as general surveillance or the particularly egregious repression occurring in Xinjiang. Chinese acquisition of this technology occurs via both legitimate means, such as advanced study at U.S. universities or joint research and development with foreign firms or collaboration with foreign universities, but also via illicit means, such as theft and espionage. The Department of State is committed to countering illicit behavior.

We continue to welcome Chinese students who come here lawfully to study in the United States. We also recognize the inherent value of interpersonal exchange between our two countries. China consistently sends more students to the United States than any other country. In fact, the number of Chinese students studying in the United States is roughly equivalent to the number of students from the next six countries combined. The overall number of Chinese students in the United States continues to rise, with more than 360,000 students during the most recent school year. While we welcome these students, national security must be our number one priority. President Trump reiterated this point from the Oval Office in October. The strength of our global leadership in science and research rests on our openness. The U.S. greatly values international scientists as members of our research enterprise. For decades, foreign scientists, including from China, have contributed substantially to scientific progress and innovations at research institutions across the United States. But we must also be cautious as we pursue certain kinds of

international study and exchange programs. Through its policy of military-civil fusion, Chinese authorities are actively engaged in large-scale collection of sensitive and proprietary technological and expertise from the United States. Unfortunately, the Chinese government is actively encouraging, and in many cases coercing, its citizens to abuse the goodwill and openness of our country for its own benefit. Such actions undermine fundamental values and principles that underpin the scientific enterprise – those of openness, transparency, meritocracy and reciprocity – as well as the integrity of the enterprise itself.

The State Department is working across the U.S. government and the domestic scientific community to protect the integrity of the U.S. scientific enterprise through the National Science and Technology Council's Joint Committee on the Research Environment. We are also working with our allies and partners to build a shared awareness of risks and to identify approaches that could mitigate those risks.

A Layered Approach to Visa Security

In coordination with interagency partners, the Department has developed, implemented, and refined an intensive visa application and screening process. We require personal interviews for most applicants, employ analytic interviewing techniques, and incorporate multiple biographic and biometric checks in the visa process. Underpinning the process is a sophisticated global information technology network that shares data within the Department and with other federal law enforcement and intelligence agencies. Every visa decision is a national security and public safety decision. Our rigorous security screening regimen applies to all visa applications.

Visa applicants submit online applications which enable consular and fraud prevention officers, as well as our intelligence and law enforcement partners, to analyze data in advance of the visa interview, including the detection of potential non-biographic links to derogatory information.

Consular officers use a multitude of tools to screen visa applications. No visa can be issued unless all relevant concerns are fully resolved. The vast majority of visa applicants – including all applicants triggering potential concerns – are interviewed by a consular officer. During the interview, consular officers analyze case-relevant issues pertaining to the applicant's identity, qualifications for the requested visa category, and any information pertaining to possible ineligibilities

including those related to criminal history, prior visa applications or travel to the United States, and/or links to terrorism and other security threats.

All visa applicant data is screened against the Department's Consular Lookout and Support System (CLASS), an online database containing approximately 36 million records of persons, including those found ineligible for visas and persons who are the subjects of potentially derogatory information, drawn from records and sources throughout the U.S. government. CLASS is populated, in part, through an export of the Terrorist Screening Database (TSDB) and the federal terrorism watchlist. CLASS employs sophisticated name-searching algorithms to identify matches between visa applicants and derogatory information contained in CLASS. We also run all visa applicants' names against the Consular Consolidated Database (CCD, our internal automated visa application record system) as a secondary check for derogatory information regarding visa applicants and visa holders, and to flag prior visa applications, refusals, and issuances. The CCD contains more than 181 million immigrant and nonimmigrant visa records dating back to 1998. This robust searching capability, which takes into account variations in spelling and naming conventions, is central to maintaining visa security. In addition, all visa applicants are subjected to a robust interagency counterterrorism review before their visas can be issued. Finally, we employ a suite of biometric reviews, which check each applicant against U.S. government counterterrorism holdings and which vet applicants against other partner data.

Assessing Visa Eligibility According to the INA

Consular officers also employ a variety of statutory tools to adjudicate visa applications. Under the law that applies to most nonimmigrant visa classifications, if the consular officer believes a nonimmigrant visa applicant may fail to abide by the requirements of the visa category in question, including by engaging in non-permitted activities or by remaining in the United States beyond their authorized stay, the application will be refused under section 214(b) of the Immigration and Nationality Act (INA). A consular officer may also initially refuse a case under INA section 221(g) to confirm information presented in the application, request additional information from the applicant, request a security or legal review from Washington, or pursue local leads or other information to determine whether the applicant is subject to a security or non-security-related ineligibility.

Consular officers also assess all visa applicants' eligibility under the security-related grounds of the INA. For example, the consular officer considers whether there are reasonable grounds to believe that a visa applicant seeks to enter

the United States to engage solely, principally, or incidentally in activity that violates or evades U.S. law prohibiting the export from the United States of goods or technology. This includes commodities and technology that are subject to export controls under the Export Administration Regulations, International Traffic in Arms Regulations, or other U.S. regulations such as those imposing economic sanctions. As export controls are broadened or refined by the multilateral export control regimes or through unilateral foreign policy decisions to cover new and innovative fields, and as changes are adopted into U.S. control lists, consular officers can be empowered to deny visas to applicants seeking to study or work in those areas, as warranted. The broader these export controls are, the more often we can use them to deter and disrupt activities of concern.

Export controls are targeted at items of proliferation concern, weapons of mass destruction, their delivery systems, and advanced conventional weapons, among other areas. They do not necessarily control items that are sensitive from an intellectual property or "trade secrets" perspective, although such technology may be protected under other legal frameworks. Under the INA, consular officers cannot currently deny a visa application on national security grounds if they have reason to believe that the visa applicant seeks to enter the United States to lawfully gain knowledge through work or study in a sensitive area of technology that is not export controlled – for example, certain technology related to robotics or artificial intelligence.

Continuous Vetting and Visa Revocation

The Department of State has broad authority to revoke visas, and we use that authority widely to protect our borders. Cases for revocation consideration are forwarded to the Department of State's Visa Office by embassies and consulates overseas, National Targeting Center (NTC), National Counterterrorism Center (NCTC), and other entities. As soon as information is established to support a revocation (i.e., information that surfaced after visa issuance that could lead to an ineligibility determination, or otherwise indicates the visa holder poses a potential threat), a code showing the visa revocation, and lookout codes indicating specific potential visa ineligibilities, are added to the CLASS system, as well as to biometric identity systems, and then shared in near-real time (within approximately 15 minutes) with the DHS lookout systems used for border screening. Every day, we receive requests to review and, if warranted, revoke visas for aliens for whom new derogatory information has been discovered since the visa was issued. We continue to work with our interagency partners to refine the visa revocation and associated notification processes. As we are able to identify those seeking to gain

access to sensitive and controlled technologies, and perhaps strengthen our export control regime to better protect U.S. innovation and technology, visa revocation is another tool we can use to prevent the theft of sensitive knowledge and technologies.

Revocations are typically based on new information that has come to light after visa issuance. Since individuals' circumstances change over time, and people who once posed no threat to the United States can become threats, continuous vetting and revocation are important tools. In addition to the millions of visa applications we refuse each year, since 2005, the Department has prudentially revoked more than approximately 100,000 visas, based on information that surfaced following visa issuance, for a variety of reasons.

Going Forward

State and our partner agencies have taken initial steps to mitigate the risks posed by the Chinese Communist Party's Military-Civil Fusion strategy by increasing scrutiny of certain Chinese visa applicants. This effort will augment already existing criteria for enhanced vetting of certain Chinese nationals as well as specialized training for consular officers serving in China.

The Department of State is also often the first U.S. government agency to have contact with foreign nationals wishing to travel to the United States. Like you, we are committed to preventing individuals from exploiting the visa process as a means of entering our country with the intent to do harm or to improperly acquire and exploit sensitive and proprietary U.S. goods and technology. Our visa operation in China is one of the largest in the world. In FY 2019 alone, the Department of State issued almost 1,500,000 nonimmigrant visas to Chinese citizens around the world.

However, the Immigration and Nationality Act currently allows consular officers to make visa ineligibility findings for only a narrow set of applicants whose expected activities involve violation of a current export control law. While we work in close partnership with other State bureaus, DHS, and other relevant US government agencies to protect our borders, ultimately the law as it is currently written restricts the discretion of consular officers to find visa applicants ineligible, even when there is reason to believe the applicant may intend to export technology many consider to be sensitive but which is not currently controlled.

The Department of State recognizes that this threat cannot be countered through the visa applicant screening process alone. An effective strategy to

counter Beijing's intentions requires a comprehensive approach that engages all relevant stakeholders, including the academic and business communities about the nature of the threats and the actions we are taking to counter them.

For example, more public engagement is needed in order to counter the false narrative pushed by the Chinese government that the United States is "weaponizing visas" against ordinary Chinese citizens. In truth, the Chinese government has repeatedly chosen to pursue the acquisition of sensitive technologies in such a way that we have been forced to respond to protect our vital interests. And by involving Chinese students and researchers in its pursuit of these technologies, the Chinese government has put at risk the visas of some of its own citizens. We must not allow the Chinese government to control this narrative. We are taking appropriate and reasonable measures to safeguard our national security. Far from "weaponizing visas," our response is measured and targeted.

We therefore welcome your continued engagement on this topic with your constituents and contacts to raise their awareness of our shared concerns and reassure them that the U.S. government still believes in the value of academic exchange when conducted with integrity. Meanwhile, the Department of State will continue a comprehensive review of its visa security screening process to adapt to these challenges. The Department of State will continue to apply rigorous screening to all applicants to protect our people, the integrity of our academic institutions, and the intellectual property of our nation.