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 THE JUDICIARY

SUBCOMMITTEE ON BORDER SECURITY AND IMMIGRATION

JUNE 6, 2018

Good morning Chairman Cornyn, Ranking Member Durbin, and distinguished Members of the Subcommittee, and thank you for this opportunity to testify at today's hearing. We share the concerns expressed by the Subcommittee and our interagency partners regarding the potential for a limited number of foreign government-directed international students and professors in the United States to engage in 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 described here today.

We recognize that the United States is a global leader in international scholarly exchange, and that our leadership enriches our academic community, drives innovation at home, contributes to jobs and economic growth in all 50 states, and strengthens our connections and channels of international influence. More than a dozen current heads of state are U.S.-educated, and thousands of cabinet officials, legislative leaders, and titans of industry in countries around the world have forged beneficial and lasting ties with Americans through study in the United States. We strive to facilitate legitimate travel to our country when it is in our national interest, while protecting against those who would do us harm.

The President detailed in his December 2017 National Security Strategy (NSS) that China has repeatedly engaged in efforts to acquire sensitive and proprietary technologies from the United States. The NSS notes that the Chinese and possibly others use largely legal means to build relationships and gain access to experts and fields in the United States in order to fill capability gaps and erode America's long-term competitive advantages. FBI Director Christopher Wray recently testified that the use of non-traditional collectors of intelligence is common in academic settings and that such actors have exploited the opportunity to work with renowned U.S. scholars and researchers and have taken advantage of the very open research and development environment prevalent at U.S. colleges and universities. We are also aware of FBI reporting that indicates foreign students, often with no nefarious intent in their plan to study in the United States, are later co-opted to work for their government and share their newly-acquired technical expertise.

Although this can carry enormous consequences for the United States' long-term technological and competitive advantage, much of this transfer of information and knowledge may be legal under today's export control laws. Although this would be in the Department of Commerce's area of expertise, we believe that export control laws and regulations should be continuously scrutinized and updated to ensure that new and innovative U.S. technologies that are sensitive or proprietary are properly protected against threats or competitors. We have robust interagency visa screening and vetting processes and are constantly working to find mechanisms to improve them. As the U.S. government identifies new sensitive technologies that are threatened, we look to our interagency partners to assist us in identifying those threats to allow us to effectively screen against them. The consequences for not doing this can be serious, as the President's NSS noted, "losing our innovation and technological edge would have far-reaching negative implications for American prosperity and power."

In order to address the threat of foreign visitors, including students, who seek to acquire sensitive and proprietary U.S. technologies, we and our partner agencies throughout the federal government have built a layered visa and border security screening system, and continue to refine and strengthen the five pillars of visa security: technological advances, biometric innovations, personal interviews, data sharing, and training. We work closely with partner agencies to identify and define new threats and applicants of concern, including applicants who seek to work or study in sensitive or proprietary fields that are subject to U.S. export controls. The Department of State is often the first U.S. government agency to have contact with foreign nationals wishing to travel to the United States, and 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 acquire sensitive and proprietary U.S. goods and technology in violation of U.S. law.

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 first time 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. The rigorous security screening regimen I describe below 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 for whom there are any concerns – are interviewed by a consular officer. During the interview, consular officers pursue case-relevant issues pertaining to the applicant's identity, qualifications for the particular visa category in question, 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 any 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) to detect and respond to any derogatory information regarding visa applicants and visa holders, and to check for prior visa applications, refusals, or 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 our procedures. 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, other checks that review each applicant against U.S. government counterterrorism holdings, and checks that 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 activities not permitted or remaining in the United States after the end of 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 to violate or evade 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 are 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.

There are, however, a wide variety of legal grounds in the INA that can lead consular officers to deny a visa. In CY 2016, consular officers denied 2,980,271 **immigrant and non-immigrant** visas worldwide.

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, NTC, 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 CLASS, 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 non-traditional collectors, 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. Although a visa revocation for an individual who is already present in the United States is normally made effective upon the individual's subsequent departure, we use our authority to revoke a visa immediately in circumstances in which we believe there is an immediate threat regardless of the individual's location, after which we will notify the issuing post and interagency partners as appropriate. In addition to the millions of visa applications we refuse each year, since 2005, the Department has prudentially revoked approximately 100,000 visas, based on information that surfaced following visa issuance, for a variety of reasons.

Going Forward

We are dedicated to maintaining our vigilance and strengthening the measures we take to protect the American public, as well as protect sensitive and proprietary American technology and innovations. Those with the intent to do us harm have demonstrated their ability to quickly adapt to changes in screening policies and we therefore must also be constantly honing our screening and vetting procedures. We also recognize that overreaching restrictions on foreign students and scholars at our world-class universities would challenge U.S. leadership in scientific discovery and innovation and erode U.S. dominance in attracting the brightest talent and preparing the most advanced technical workforce in the world. We therefore must balance protective measures with the concerns of academia and business leaders that drive America's economic and technological success. We will continue our outreach efforts to broaden and diversify the pool of legitimate academics who contribute to our national success and advance our foreign policy interests, while working with partner agencies to ensure a coordinated and effective approach to visa security, based on an increasing knowledge of threats, and our ability to identify and interdict those threats.

We constantly analyze our current processes to identify areas where we could improve. We work closely with our interagency partners such as DHS to identify new threats and screen against them. We believe these endeavors will provide us insights to continue to ensure the visa process is as secure, effective,

and efficient as possible. As part of our long-term strategic planning to improve efficiency and accuracy in visa adjudications, we are investigating the applicability of advanced technology in data analytics, risk screening, and credibility assessment. Investing in these high-tech solutions would give us more robust data analytics capabilities to help us to identify trends and reduce threats from overseas while keeping the United States open for business.

We will continue to work closely with our law enforcement and intelligence agency partners to refine our vetting practices based on the most up-to-date threats identified to us by those partners. Towards that end, we are very engaged in the establishment of the National Vetting Center (NVC), which will be housed within DHS. We look forward to the collaborative vetting efforts resulting from combining the capabilities of the entire U.S. intelligence community in order to identify nefarious actors and prevent them from entering the United States.

Mr. Chairman, Ranking Member, and Members, I assure you that the Department of State continues to refine its intensive visa application and screening process, including personal interviews, employing analytic interview techniques, incorporating multiple biographic and biometric checks, and interagency coordination, all supported by a sophisticated global information technology network. We look forward to working with the committee staff to address both the threats and the tools necessary to combat those threats to our national security in a cooperative and productive manner.