



U.S. Immigration and Customs Enforcement

STATEMENT

OF

LOUIS A. RODI III

ACTING ASSISTANT DIRECTOR
NATIONAL SECURITY INVESTIGATIONS DIVISION
HOMELAND SECURITY INVESTIGATIONS

U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT
DEPARTMENT OF HOMELAND SECURITY

REGARDING A HEARING ON

*“FOREIGN THREATS TO TAXPAYER FUNDED RESEARCH: OVERSIGHT
OPPORTUNITIES AND POLICY SOLUTIONS”*

BEFORE THE

UNITED STATES SENATE
COMMITTEE ON FINANCE

Wednesday, June 5, 2019
9:45 a.m.
215 Dirksen Senate Office Building

Introduction

Chairman Grassley, Ranking Member Wyden, and distinguished members of the committee:

Thank you for the opportunity to discuss the role U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) plays in addressing *Foreign Threats to Taxpayer Funded Research*. The threat posed by nation-states illegally and/or subversively seeking to exploit legitimate educational and research opportunities in the United States is evolving. ICE HSI plays a pivotal role in identifying the avenues, methods, and strategies that foreign nationals use to attack our research institutions. State actors routinely engage in or facilitate the procurement of U.S. technology and theft of intellectual property, sometimes in violation of federal laws and regulations. Combatting these activities is at the forefront of HSI's priorities, with multiple divisions and mission sets within the agency collaborating to identify and uncover foreign actors and networks exploiting U.S. academic and research institutions and to strategically disrupt their operations.

HSI is the principal investigative arm of the U.S. Department of Homeland Security, responsible for investigating a wide range of domestic and international activities arising from the illegal movement of people and goods into, within, and out of the United States. As part of its mission, HSI oversees a diverse portfolio of investigative and administrative programs that safeguard the United States against national security and public safety threats, and against the violation of customs and immigration laws of the United States. As part of today's testimony, I would like to highlight some of the initiatives HSI has implemented and is seeking to further enhance.

Current State of Play / Nature of the Threat

The United States is home to thousands of universities and colleges, many of which are among the most advanced institutions in the world for higher education and scientific, technological, and medical research. As a result, each year thousands of foreign nationals seek to obtain nonimmigrant visas to enable them to travel to the United States to pursue educational degrees or research at these institutions. Thousands more are already present in the United States attending U.S. colleges and universities or conducting advanced research in a multitude of fields.

As of May 2019, there are just over 1.13 million nonimmigrant students present in the United States. This includes 1,129,816 active F-1 students and 9,755 active M-1 students. There are 558,784 F-1 students who are studying or engaged in research in science, technology, engineering, and mathematic (STEM) related fields.

While openness and international collaboration in academia and research are important aspects of facilitating significant enhancements in science and technology, they also can create an environment that U.S. adversaries exploit as a means to gain access to sensitive technology and information, some of which is controlled for export, and transferred to foreign entities. The largest number of ongoing HSI Counter Proliferation Investigations (CPI) cases on controlled exports, including intangible exports (*i.e.*, the transmission of technical data from the United

States, or transfer to foreign nationals within the United States) involves China, Iran, and Russia. From these investigations and based on trend analysis, HSI knows that these countries are actively implementing a multitude of schemes to illicitly or subversively acquire and transfer export- controlled military and dual use technology and commodities, and are employing myriad schemes to circumvent U.S. export control laws.

Exploitation of academia and U.S. research institutions is just one of the schemes these countries are employing to obtain access to sensitive research and export-controlled information and technology, and to facilitate its transfer abroad. These countries are attempting to obtain this information, in many instances in an illegal or subversive manner, in order to advance their own military capabilities or economic goals, many times in contravention to the national security of the United States.

Foreign nationals from China, Iran, and Russia represent a sizeable portion of the overall nonimmigrant student population currently in the United States. As of May 2019, there are 357,863 F-1 Chinese students in the United States with 181,980 such students enrolled in STEM-related academic programs at U.S. institutions. There are also 11,323 F-1 Iranian students and 6,196 F-1 Russian students, with the respective STEM student breakdown of 9,057 for Iran and 2,008 for Russia.

HSI Efforts to Identify and Mitigate the Threat

HSI has established a multi-dimensional approach to safeguarding the Homeland against transnational threats of this nature. HSI's first line of effort is preventative, and aims to identify and disrupt the ability of known or suspected national security or public safety threats from obtaining nonimmigrant visas to lawfully travel to, and obtain entry into, the United States. A core component of this effort is the HSI-led Visa Security Program (VSP). Through the VSP, HSI analysts and special agents work in conjunction with U.S. interagency and foreign government partners to maximize the opportunity to screen, vet, and investigate potential threats prior to the U.S. Department of State (DOS) making a visa determination and well before the applicant presents for admission to the United States. This includes those applying for student or exchange visitor visas. If sufficient derogatory information is uncovered relating to the intentions of visa applicants, HSI – working in conjunction with DOS – can recommend refusing visas on a number of grounds, including for suspected involvement in the illicit procurement or attempted procurement of controlled technology.

In addition to these preventative measures, HSI also implements multiple programs to identify and protect against foreign entities already in the United States who may seek to exploit legitimate academic and research opportunities for the ultimate benefit of adversarial state actors. The Student and Exchange Visitor Program (SEVP) fulfills a compliance-centric role, and is responsible for monitoring certified educational institutions and the nonimmigrant students they enroll. The Counterterrorism and Criminal Exploitation Unit (CTCEU) coordinates investigative and enforcement actions in cases in which nonimmigrant visa holders, including students and exchange visitors, overstay their visas or violate the terms of their visas and are suspected of posing a concern to U.S. national security or public safety. If students or exchange visitors appear to be involved in efforts to acquire and transfer sensitive information or technology

obtained during the course of their research or academic pursuits, HSI's CPI plays a role in coordinating an investigative and enforcement response to those activities.

Together, these programs form the backbone of HSI's efforts to identify and mitigate the threats posed by foreign entities seeking to exploit legitimate academic and research opportunities within the United States. Each of these programs is described in more detail below.

HSI Visa Security Program:

The HSI VSP leverages resources in the United States and abroad to screen and vet non-immigrant visa applicants, identify and prevent the travel of those who constitute potential national security or public safety concerns, and launch investigations into transnational criminal- and terrorist-affiliated networks operating around the globe. The VSP was formed in response to the September 11, 2001 attacks, authorized by Section 428 of the *Homeland Security Act of 2002* and implemented by a 2003 Memorandum of Understanding between the Secretaries of State and Homeland Security.

Currently, HSI VSP operations are conducted at 36 visa-issuing posts in 27 countries. In FY 2018, VSP screened 2,196,708 visa applications, made 1,251 nominations or enhancements to the terrorist watchlist, and recommended the refusal of 9,007 visa applications. Additionally, deployed special agents conducted 5,101 interviews and initiated 348 investigations in support of VSP operations. One key facet of VSP operations is the overseas assignment of HSI Special Agents to diplomatic posts worldwide. Embedded within American Embassies and Consulates, these agents work alongside DOS Consular Affairs personnel, other partner agencies at post, and appropriate host country officials to identify and investigate terrorists, criminals, or other individuals who pose a threat to the United States.

A second critical component to VSP is the Pre-Adjudicated Threat Recognition Intelligence Operations Team (PATRIOT), administered by HSI International Operations (IO) in collaboration with U.S. Customs and Border Protection (CBP), which conducts centralized screening and vetting in the National Capital Region (NCR) in support of VSP operations. PATRIOT enables the automated screening of visa application information against DHS holdings, as well as holdings of other U.S. agencies, at the earliest point in the visa process, well in advance of the visa applicant's interview and visa adjudication. Derogatory information discovered during automated screening process is manually vetted by PATRIOT personnel utilizing law enforcement techniques, open source information, and classified systems. PATRIOT analysts then provide HSI Special Agents assigned to VSP posts with relevant information to use during interviews of visa applicants or other investigative activities conducted abroad prior to visa adjudication. Following the analysis of all known derogatory information, HSI Special Agents at VSP posts provide a unified DHS recommendation to DOS on visa eligibility.

In addition to the PATRIOT process, VSP personnel also participate in other U.S. government screening and vetting efforts focused on protecting the Homeland from diverse national security and public safety threats. Generally, these processes entail collaboration between HSI, DOS, and other partner agencies involved in screening and vetting. This includes

conducting intensive reviews of visa applications from visa-issuing posts worldwide that are considered high risk for the applicant's potential involvement in the unlawful procurement, transfer, or export of sensitive military or dual-use U.S. information and technology. At times, these applications may involve individuals seeking to exploit the U.S. educational system by enrolling in graduate level studies or engaging in research, teaching, or exchange programs as a way to acquire and transfer sensitive, export-controlled technology or information on behalf of adversaries or organizations that pose a national security risk to the United States. In some instances, a more intensive screening and vetting of a visa application is prompted by risk factors indicative of a visa applicant's potential involvement in activities related to the unlawful procurement, transfer, or export of sensitive U.S.-origin military or dual-use goods or technology on behalf of foreign adversaries or criminal organizations. After such reviews, VSP personnel then provide consular officers advice and background information to properly adjudicate immigrant and nonimmigrant visa applications of security or foreign policy interest.

Whether through the PATRIOT process or other screening and vetting efforts in which the VSP is engaged, the VSP ultimately provides recommendations for visa issuance or refusal to DOS based on information uncovered during the review, vetting, and investigative process. In all cases where the VSP team recommends the refusal of a visa, the VSP coordinates in advance with CBP's National Targeting Center-Passenger (NTC-P) regarding the applicant's admissibility or inadmissibility, per the Immigration and Nationality Act (INA). This ensures that DHS presents a single, uniform position on visa eligibility and admissibility to DOS.

The combination of the international and domestic dimensions of VSP equips HSI with a unique capability to investigate suspicious travelers, enhance existing information, and identify previously unknown threats, rather than simply denying visas and potential travel of these applicants. These efforts allow VSP to operate as a counterterrorism tool that mitigates threats posed by transnational terrorist and criminal networks. Utilizing information obtained through the visa application process, the VSP enhances the national security and border security of the United States by identifying national security or public safety concerns at the earliest part of the visa lifecycle and preventing their travel to and admission into the United States.

HSI Student and Exchange Visitor Program:

Foreign nationals who receive nonimmigrant visas to pursue educational, vocational, or research programs in the United States will interact with the Student and Exchange Visitor Program (SEVP). As of May 2019, there are 1,139,571 nonimmigrant students attending 6,410 SEVP-certified schools.

SEVP uses the Student and Exchange Visitor Information System (SEVIS) to monitor F and M students and the schools that enroll them while in the United States. SEVIS also contains the information for the Exchange Visitor program (J-visas), which is administered by DOS. SEVIS contains information such as a student's name, physical and mailing addresses, date of birth, phone number, email address, academic major, and employment information (if applicable). SEVIS information is updated by Designated School Officials (DSOs), but the system will auto-terminate a student's record if the student fails to enroll or report to school,

meaning the student must depart the United States or he or she may be put into removal proceedings.

SEVP is also responsible for the school certification process. The certification process is rigorous and continual. To obtain initial certification, schools must submit required evidence and applications, undergo site visits, and recommend DSOs. These school officials must be U.S. citizens or lawful permanent residents and must affirm their knowledge and intent to comply with all federal regulations. The schools are furthermore subject to biennial recertification, unannounced site visits and out-of-cycle reviews at any time. Schools that do not comply with the regulations may be withdrawn and, subsequently, ineligible to enroll nonimmigrant students until successfully re-petitioning for approval and meeting all certification standards.

Beyond the certification process, SEVP uses SEVIS data to engage in risk management and has enhanced its risk management framework by developing a compliance dashboard to identify schools with risk indicators. SEVP employs this risk analysis tool to identify schools that may have violated SEVP regulations when conducting recertification reviews, adjudicating school updates, and determining whether to initiate out-of-cycle reviews. SEVP regularly conducts compliance site visits to schools to ensure that approved programs are functioning as reported in SEVIS. In addition, SEVP continuously vets leads reported by the public concerning both schools and students, acting decisively to protect public safety and the integrity of the immigration system.

While many of SEVP's processes and programs have proven to be effective, HSI strives to improve and enhance these programs. For example, SEVP has mitigated previously identified national security gaps and system vulnerabilities within SEVIS and is using an adaptive maintenance approach to continuously add enhancements to the system. These enhancements have improved data integrity and the stability of the system. SEVP is currently working towards transforming SEVIS into a person-centric database. In March 2018, SEVP launched the SEVP Portal for students participating in Optional Practical Training (OPT) related to STEM degrees. The Portal allows nonimmigrant students to directly upload their required SEVIS information, including their employer's name and address, as well as other key information for monitoring purposes. The portal interfaces with SEVIS and shares information but does not give students direct access to SEVIS. The Portal has been a success with more than 166,402 registered portal users (i.e., 74.7 percent of the students eligible for Portal Accounts). The portal will be expanded to all F and M students, resulting in SEVIS data that is more accurate, captures changes in a student's information quicker and ensures students are accountable for the data inputted.

Additionally, SEVP started conducting criminal background checks on proposed DSOs in May 2017, due to the fact that these individuals have access to a secure government database and a role in reporting information in that database. HSI is actively working to expand this process and incorporate such vetting as part of its regular review of approved schools and DSOs, both to safeguard against potential vulnerabilities and to ensure the integrity of the information in SEVIS. SEVP's current programs, ongoing enhancements, and proposed expansion will further secure our nation from those wishing to exploit the nation's education system. For more information about the privacy risks that HSI takes on while operating SEVP and the subsequent

mitigations, please view the SEVIS privacy impact assessment (PIA) and subsequent updates available at www.dhs.gov/privacy.

HSI Counterterrorism and Criminal Exploitation Unit:

HSI's CTCEU actively identifies and initiates enforcement action on nonimmigrant visa overstay violators, and works closely with SEVP and CPI to ensure leads and other information related to potential status violators are referred to HSI field offices for appropriate action. Within the agency, CTCEU focuses on overstay violators who pose a national security, border security, or public safety concern. This includes individuals who entered the United States as nonimmigrant students or exchange visitors. CTCEU leverages special agents, analysts, information systems, and interagency partnerships to determine viable national security related overstay leads to pursue.

In an average year, CTCEU analyzes over one million potential status violator records, incorporating data from various government systems, such as SEVIS and CBP's Arrival and Departure Information System (ADIS). CTCEU conducts both batch and manual vetting against government databases, public indices, and open source information. The vetting helps determine whether an individual who overstayed has departed the United States, adjusted to a lawful status, has a pending immigration benefit application, or would be appropriate for an enforcement action.

CTCEU proactively develops cases for investigation, monitors the latest threat reports, and addresses emergent issues. This practice is designed to detect and identify individuals and schools exhibiting specific risk factors; it is formulated based on intelligence reporting, travel patterns, and in-depth criminal research and analysis. It has contributed to the counterterrorism mission by initiating and supporting high-priority national security initiatives, based on specific intelligence. CTCEU considers several fraud indicators when reviewing schools, such as a high volume of students engaged in OPT or Curriculum Practical Training (CPT), low completion rates, over-enrolled schools with student populations exceeding indicated I-17 amount, schools receiving Federal funding for sensitive research, or schools exhibiting various other fraud indicators. CTCEU also reviews SEVP Analysis Operation Center (SAOC) Tip Logs and HSI Tip Line information to further enhance or corroborate information received on schools or school officials.

LeadTrac is the database owned by CTCEU and is used to vet and manage leads pertaining to visitors in the United States who are suspected of overstaying their period of admission or otherwise violating the terms of their admission, as well as organizations suspected of immigration violations. LeadTrac's structure supports a subject-centered data model, ensuring multiple leads about a single subject are linked within the system. For more information about the privacy risks that HSI CTCEU takes on while operating LeadTrac and the subsequent mitigations, please view the LeadTrac PIA available at www.dhs.gov/privacy.

In FY 2018, CTCEU reviewed 1,429,395 leads regarding potential overstays. Numerous leads were closed through an automated screening process, most commonly due to subsequent departure from the United States. A total of 8,968 leads were sent to HSI field offices for

investigation. Of these, 2,212 were pending further investigation, 2,795 were closed for being in compliance (pending immigration benefit application, granted asylum, approved adjustment of status application, or departed the United States) and the remaining leads were returned to CTCEU for continuous vetting and further investigation. In FY 2018 alone, HSI made 1,808 arrests pursuant to visa violator leads. In FY 2019 through March 31, 2019, CTCEU has reviewed 765,543 leads regarding potential overstays and sent 4,940 leads to HSI field offices for further investigation. HSI has made 1,025 arrests pursuant to visa violator leads in FY 2019.

CTCEU refers leads that do not meet HSI criteria for further investigation to ICE Enforcement and Removal Operations (ERO) National Criminal Analysis and Targeting Center (NCATC) which works in close coordination with CTCEU for further vetting. If necessary, the lead is forwarded to the respective ERO field office for enforcement action.

Key Initiatives on Overstay Enforcement

Outreach is an important component of CTCEU's operations. HSI special agents have been conducting outreach visits to SEVP-certified institutions as part of HSI's Project Campus Sentinel (PCS) program. This outreach program, which was established in 2011, aims to build a mutual partnership between local HSI special agents and SEVP-certified institutions by collaboratively preventing the criminal exploitation of SEVP through direct and open communication. It furthermore creates an avenue for improved direct communication between DSOs and local HSI special agents. In recent years, this outreach program has been expanded to include SEVP Field Representatives and Campus Public Safety entities. This partnership provides all stakeholders the opportunity to openly exchange information, improve cooperation, and bolster the safety and security of students, faculty, and institutions. Since inception, HSI special agents have conducted over 4,000 PCS outreaches.

Other key initiatives in HSI's overstay enforcement efforts include the Domestic Mantis and Visa Lifecycle programs. The Domestic Mantis and Visa Lifecycle programs help identify nonimmigrant students who have access to sensitive technology, better capture the overarching visa lifecycle, provide another layer of security for the nation, and serve as innovative investigative tools to support the enforcement of U.S. immigration laws.

CTCEU developed the Domestic Mantis Program in response to a Government Accountability Office (GAO) assessment that identified a potential vulnerability with nonimmigrant students who enter the United States to study in a non-sensitive field of study and subsequently transfer to a sensitive field of study. These individuals could pose a substantial risk related to the diversion of sensitive technology, materials, or information.

The Domestic Mantis Program aims to enhance national security by preventing the export of goods, technology, or sensitive information through activities such as graduate-level studies, teaching, research, training, or employment. The program works by identifying students that have changed their field of study to a sensitive area and evaluates those individuals against risk-based targeting criteria. To accomplish this, CTCEU manually extracts and reviews SEVIS data pertaining to students from countries that have an elevated risk of proliferation activity. The potential leads are analyzed using a comprehensive vetting process, including a review against

Intelligence Community holdings for additional derogatory information, open source information, and academic journals. These Domestic Mantis checks are performed twice a year to identify new students who enroll at varying times within the school year.

Visa Lifecycle Program

The Visa Lifecycle Program tracks nonimmigrant visitors from the time they file visa applications to the time they depart from the United States, become overstays, or otherwise fail to comply with their terms of admission (i.e., become “out-of-status”). This program allows HSI to continuously vet and identify derogatory information on nonimmigrant visitors for the validity of the visa. In instances where violators are identified, appropriate enforcement actions are initiated.

The Visa Lifecycle Program focuses on nonimmigrants seeking business/tourist (i.e., B1/B2) or student/exchange (i.e., F, J, and M) visas from five DOS visa issuing posts. These posts were selected to complement existing HSI screening efforts in response to recent global acts of terrorism perpetrated in those countries. Working in coordination with HSI’s VSP, CTCEU receives information on these visa applicants pulled from PATRIOT and the DOS Consular Consolidated Database (CCD). CTCEU ingests this data into its lead management system and continuously vets these nonimmigrant visa holders using an automated open source vetting platform in conjunction with Intelligence Community holdings.

HSI Counter Proliferation Investigations Program:

Cases involving the attempted acquisition and transfer of sensitive, export-controlled commodities, technology, or information fall within the purview of the HSI CPI program. HSI is designated as the primary law enforcement agency for investigating violations of U.S. export laws related to military items, controlled dual-use goods, and sanctioned/embargoed countries. HSI, through its CPI program, has statutory authority to investigate violations of U.S. export control laws, and is uniquely equipped – as the only agency enforce with border search authority, undercover authority, forfeiture authority, and an extensive international footprint – to combat the trafficking of weapons and technology, to include chemical, biological, radiological, nuclear materials, and other items required to produce weapons of mass destruction (WMD).

HSI’s CPI mission is directly aligned with U.S. national security and defense strategies, as they pertain to protecting the American war fighter and the Homeland from having sensitive U.S.-origin military and WMD technology fall into the hands of U.S. adversaries; securing the U.S. border from firearms being smuggled to transnational criminal organizations; disrupting the supply chains of illicit procurement networks by preventing terrorist groups and hostile nations from acquiring U.S. military hardware, firearms, sensitive technical data, dual-use technology, and materials used to develop weapons of mass destruction; protecting U.S. industry from sensitive intangible technology transfers; and keeping U.S. industry’s intellectual property, as well as ground breaking research and development, from being exploited by U.S. adversaries.

HSI, and its predecessor agency, the U.S. Customs Service, has been exercising its export enforcement authority for over 100 years. Although other federal law enforcement, regulatory, intelligence, and military agencies are involved in the overall U.S. export control efforts, HSI is empowered with full statutory authority to investigate violations of all U.S. export control laws, such as the *Arms Export Control Act* (AECA) and International Traffic in Arms Regulations (ITAR); the *Export Controls Act of 2018* (ECRA) and the Export Administration Regulations (EAR); the *International Emergency Economic Powers Act* (IEEPA); and *Trading with the Enemy Act* (TWEA). From 2012 to 2018, HSI CPI investigations have resulted in over 17,000 cases initiated, 4,006 arrests, and 8,288 seizures.

U.S. export control laws are comprehensive and include restrictions on tangible exports (*i.e.*, the actual shipment of items from the U.S.), intangible exports (*i.e.*, the transmission of technical data from the United States, or transfer to foreign nationals within the United States), re-exports and transshipments (*i.e.*, exports from one foreign country to another), and controls on services and other business activities (*i.e.*, training, brokering, and financing services). Because of the complexity of U.S. export control laws and the multiple licensing agencies involved, HSI CPI special agents conduct outreach visits and provide presentations to private industry and academic institutions. This program, known as Project Shield America (PSA), is designed to increase public awareness of export control laws and regulations, and to equip private industry and the academic community with the knowledge needed to aid in recognition, detection, and resolution of attempted illegal acquisitions of sensitive, export-controlled goods and technology. Since 2001, HSI special agents have conducted more than 32,000 PSA outreach presentations, resulting in successful HSI criminal investigations worldwide.

Currently, the United States is facing an unprecedented threat from foreign governments, such as Iran, China, and Russia, who have launched far-reaching campaigns to illicitly acquire sensitive, and in some cases export-controlled, commodities, technology, research, and/or information needed to further their strategic military and economic goals. One area targeted by these state actors is academia. These adversarial nations take advantage of academic openness in the name of “fundamental research” to target U.S. institutions of higher learning to capture U.S. technology, processes, and other intellectual property. This process is generally labeled non-traditional collection. In the context of academia, this entails foreign adversaries facilitating or supporting academic research and expertise development in sensitive fields by student and exchange visitor nonimmigrant visa holders. Through this process, these students and researchers acquire, export, or transfer information or technology to foreign entities in a subversive manner and without licenses, if the information or technology is export controlled. These activities pose a threat to U.S. national security and compromise the integrity of the U.S. academic and research system.

To mitigate this threat, HSI has recently taken proactive steps to increase outreach to export control officers and other officials within the academic community, particularly at universities or research institutions with large foreign student populations enrolled in STEM-related programs. These outreach efforts are conducted in conjunction with SEVP and CTCEU representatives. The goal of this increased focus on academia outreach is to raise awareness of the potential proliferation risk posed by students and researchers seeking to acquire and transfer sensitive research, technology, and/or intellectual property (some of which may be export

controlled) on behalf of foreign governments or sanctioned entities. This initiative also aims to enhance the capacity of academic institutions to recognize potential instances of potential illicit procurement, intellectual property theft, or other possible violations of U.S. laws, and to provide a conduit to report any suspicious activities detected by universities or research institutes.

While raising awareness within the U.S. academic sector and the private sector is an important step, HSI is also making a concerted effort to prevent the acquisition and transfer of technology by foreign nationals through non-traditional collection means. To that end, HSI has initiated efforts to combine and coordinate resources and information available to CPI, CTCEU, SEVP, and VSP in a joint effort to identify, investigate, and prevent destination-controlled technology and export-controlled technology transfers out of the United States that violate U.S. laws and/or weaken the U.S. technological advantage in key fields. This effort will focus on the role foreign students, primarily from sensitive countries, studying at U.S. universities and colleges play in these activities, and will aim to utilize the full breadth of HSI's administrative and criminal authorities to combat the threat posed by these foreign actors.

HSI is committed to free and open academic environment, but this must be balanced against national security measures; if not, these institutions will be taken advantage of and critical U.S. technology and research can be acquired easily by adversaries.

Conclusion

In closing, mindful of the United States' historical role in the development of critical technology in coordination with foreign partners and U.S. academic institutions, HSI remains committed to maintaining a free and open academic environment within the United States; however, this must be balanced with an appropriate focus on national security and public safety. The threat posed by adversarial nation-states illegally and subversively seeking to exploit legitimate educational and research opportunities in the United States, many of which are funded with U.S. taxpayer dollars, is real, and the United States must continue to pursue all appropriate means to combat it.

HSI will continue to work with academia, law enforcement partners, and other agency partners, to use its extensive administrative and criminal authorities to identify and disrupt the activities of individuals or organizations who seek to harm the United States in this arena and the multitude of others in which HSI is engaged. HSI is well positioned to mitigate this threat through the many programs highlighted today, all of which provide a multi-layered level of security aimed at protecting the Homeland from illicit transnational activities of its adversaries. From the preventative angle of the VSP, to the compliance focus of SEVP, and through the investigative and enforcement programs executed by the CTCEU and CPI programs, HSI is and will continue to be engaged in countering this critical problem. Enhancements and expansion of these programs, combined with enhanced administrative and criminal enforcement authorities, will only improve HSI's ability to identify and thwart the efforts of foreign actors who pose national security or public safety concerns to the United States. HSI looks forward to continuing to work with the Committee regarding these HSI programs.

Thank you again for inviting me today to explain HSI's critical role in protecting the national security and public safety of the United States. I would be pleased to answer your questions.