OPENING STATEMENT

Ranking Member Donald S. Beyer (D-VA)
of the Subcommittee on Oversight

House Committee on Science, Space, and Technology
Subcommittee on Oversight
Subcommittee on Research and Technology
"Scholars or Spies: Foreign Plots Targeting America's Research and Development"
April 11, 2018

Thank you, Chairman Abraham and Chairwoman Comstock.

First, I would like to take a moment before digging into the topic of academic espionage to again implore this Committee to take action on Environmental Protection Agency (EPA) Administrator Scott Pruitt. Administrator Pruitt's unethical behavior, wasteful use of taxpayer money, and his ongoing efforts to undermine the EPA's mission of protecting our environment and public health warrant some serious congressional oversight. I have previously requested that Chairman Smith bring Administrator Pruitt before the Science Committee to testify, as is standard practice – and now, amidst various scandals, this is more crucial than ever. Administrator Pruitt's predecessor, Gina McCarthy, testified before this Committee on three occasions during the second term of the Obama Administration, testifying first just four months after her confirmation. By comparison, Administrator Pruitt was confirmed 14 months ago, but has yet to appear before the Committee. Pruitt cannot be allowed to continue to sell our nation's clean air and water to special interests without consequences – if the President refuses to hold him accountable Congress must do its job and conduct meaningful oversight.

Turning back to the topic of the day: vigilance against espionage threats is important on all fronts, from cybersecurity breaches to intelligence gathering by covert operatives on the ground. As a committee, we have conducted numerous bipartisan investigations into cyber breaches. Hacking, however, is but one tool used by intelligence agencies to target U.S. universities. In cases of academic-related espionage, a student or researcher is recruited by a foreign government to study or do research at an American institution and passes along sensitive scientific research or technology to the foreign government. American universities play a critical role in driving fundamental research and developing innovative technologies for our nation. The loss of this sort of data can have tremendous economic consequences, endanger our national security, and diminish our technological lead in critical technologies.

Although an essential tenet of academia is its open pursuit of scientific research, professors, students and university scientists need to understand the potential value of their research to foreign adversaries. They should be properly educated about potential espionage threats and trained on how to take appropriate security measures whether they are online or at an international conference presenting their research findings. What I do not believe we want to do, however, is pull the welcome mat out from under the more than one million foreign students who come to America to study every year, contributing more than $36 billion to our economy annually, creating hundreds of thousands of U.S. jobs, and contributing to America's academic

leadership. In fact, immigrants to America have won 81 Nobel Prizes in Chemistry, Medicine, and Physics between 1960 and 2017.

The media has recently painted a poor picture of the academic community being disinterested or naïve about the potential security threats they face. I am not sure that is an accurate portrait. The higher education community has several vehicles they use to identify threats and train their members to take actions to mitigate their vulnerabilities to attack. These include the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC), the Higher Education Information Security Council (HEISC), and the newly formed Omni Security Operations Center (OmniSOC), described as a "pioneering initiative that helps higher education institutions reduce the impact of cybersecurity threats." The new group is based at Indiana University and includes collaboration with Northwestern University, Purdue University, Rutgers University and the University of Nebraska-Lincoln.

Cooperation in the security arena is critical, so I am glad to see this. However, universities also need cooperation from the law enforcement and intelligence community to help ensure they are apprised of specific threats or risks.

In 2005, to help foster better lines of communication between the FBI and the U.S. academic community, the FBI created the National Security Higher Education Advisory Board (NSHEAB), originally composed of 15 Presidents and Chancellors of leading U.S. universities, including Carnegie Mellon, Johns Hopkins, UCLA and MIT. Unfortunately, this past February, the Members of this board received a letter from the FBI announcing their decision to disband it. The letter praised the cooperation between intelligence agencies, law enforcement and academia, and said the FBI was exploring the creation of a new board. Officials in the academic community, however, believe the board played an important role in helping universities understand the intelligence risk they faced, and were both surprised and disappointed it was disbanded without a plan in place for its replacement.

I am attaching this letter to my statement, as well as a letter from the Association of American Universities (AAU), Association of Public and Land-grant Universities (APLU), American Council on Education (ACE), and the Council on Governmental Relations (COGR) regarding this important issue.

Ultimately, we cannot let concern over academic espionage crowd out the multitude of benefits from the international exchange of scholarship. Balancing legitimate security risks with international scientific cooperation is critical, as America's leadership in science and technology is highly dependent upon its openness to scholars from around the globe. Any action we take to respond to the threat of academic espionage must take into account the value of cooperation between the intelligence community and the academic community, who must work together to secure our sensitive research.

I look forward to hearing from today's witnesses about how we can balance these two important issues regarding security and scholarship.

Thank you, Mr. Chairman. I yield back.