ONE HUNDRED FIFTEENTH CONGRESS
SENATOR MARCO RUBIO, CHAIRMAN
REPRESENTATIVE CHRISTOPHER H. SMITH, COCHAIRMAN

May 9, 2018

Mr. Wilbur Ross
Secretary of Commerce
U.S. Department of Commerce
1401 Constitution Ave. NW
Washington, DC 20230

Dear Secretary Ross,

We write concerning the Chinese governments and Communist Party use of technology for repression and control, rather than for legitimate law enforcement activities. There is compelling evidence that U.S. companies are selling Chinese authorities products to improve the surveillance capability of police and security forces. Therefore, we wish to inquire whether the Bureau of Industry and Security in the Department of Commerce is tracking the sale of equipment and technology by U.S. companies that may be used by Chinese police and other security agencies for the surveillance and detention of individuals.

The actions of Chinese police and security agencies particularly in the Xinjiang Uyghur Autonomous Region (XUAR) and elsewhere are deeply problematic. They continue to violate international protections of due process, privacy, association, religious practice and international prohibitions against torture and arbitrary detention. The ongoing abuses in the XUAR are a clear example of how the government is using technology, including U.S. made, to systematically crackdown on its people. According to human rights organizations and multiple media reports, XUAR authorities have dramatically increased surveillance activities of Uyghur Muslims and other ethnic minorities, augmenting existing efforts with the latest technologies, including facial recognition, iris scanning, and advanced biometrics such as DNA sequencing, voice samples, and fingerprinting.

While estimates vary, there are reports that mass surveillance has contributed to the detention of between 500,000 to a million people in "political education centers"—a staggering figure and one of the largest instances of mass incarceration of a minority population in the world today. Authorities have also used the surveillance apparatus in the XUAR to severely limit the freedoms of movement, expression, and religion of ethnic minorities in the region. Among those targeted by XUAR authorities are dozens of family members of Radio Free Asia (RFA) Uyghur Service journalists, potentially to intimidate U.S. government employees and undermine some of the most effective reporting and broadcasting regarding recent developments in the XUAR.

Recently, Human Rights Watch and other organizations have identified Thermo-Fisher Scientific, a Massachusetts based company, as selling DNA sequencers with advanced microprocessors under the Applied Biosystems (ABI) Genetic Analyzer brand to the Chinese Ministry of Public Security and its Public Security bureaus across China. Citizen Lab, at the University of Toronto, has found that software capable of filtering, censorship, and surveillance via the internet has been sold in China from U.S. based companies and subsequently used in other countries (Syria, Russia, and Venezuela) currently under U.S. sanctions.

We respectfully request answers to the following questions:

1) Given that most crime control and detection and surveillance equipment, software and technology are controlled under the Export Administration Regulations, what factors are being used to determine the suitability of an export to an agent of state security? How did Thermo-Fisher surmount a presumption of denial to sell their product to the Chinese government?

2) What other product licenses have been sought under Export Administration Regulations sections 742.7, 742.13, 744.17(c), or other sections, to sell to agencies of China's state security?

3) In light of recent reports, how are you—in coordination with the Department of State—reviewing the export of items being used by Chinese military and police end-users for surveillance, detection, and censorship, to determine whether more scrutiny is needed over the proliferation of "dual-use" information, software, and communication technologies? Are new legislation or new authorities needed to revisit/revise export control regulations so they are consistent with the rapid evolution of technology? Is software or technology which could be used for the purpose of domestic repression, subject to export controls with respect to Chinese end-users of concern?

4) In addition to possible export controls, is there any discussion currently underway to, at the very least, restrict the end-users of such technologies, in this case Xinjiang Public Security and related entities?

U.S. companies should not be assisting the Chinese government's repression or the detention of the families of U.S. government employees. We look forward to your response and working with you and the BIS on these issues.

Sincerely,

Marco Rubio
Chair

Chris Smith
Cochair