August 25, 2026

The Honorable Howard Lutnick
Secretary of Commerce
U.S. Department of Commerce
1401 Constitution Avenue, NW
Washington, DC 20230

Dear Secretary Lutnick:

We write to request that the Department of Commerce, through the Bureau of Industry and Security (BIS), promptly finalize and implement regulations proposed in 2024 to restrict U.S. citizen and business support for foreign civilian intelligence, or security agencies from countries of concern, such as China and Russia. Congress gave the executive branch expanded export control authorities in 2022 to prevent Americans from working with or aiding intelligence and security agencies in foreign countries that spy on dissidents, journalists, and American citizens.

The executive branch, under both Democratic and Republican administrations, has, however, failed to fully implement these new authorities in the Export Administration Regulations (EAR). As a result, foreign intelligence agencies in many countries can still legally hire consultants in the United States and buy advanced U.S. surveillance, cyber, and artificial intelligence technology, for use in their intelligence operations to target Americans, and operate against American national security and foreign policy interests.

It is also still legal for U.S. companies to export to Chinese intelligence agencies otherwise uncontrolled commercial items with knowledge that they will be used for intelligence collection, including against American companies. U.S. companies can still legally provide support services to military, security, and intelligence end-users in China. Companies are also still not prohibited from exporting to intelligence and security agencies in countries of concern facial recognition systems for use in domestic surveillance.

The background to these glaring loopholes that harm U.S. national security and foreign policy interests is that the Export Control Reform Act of 2018 (ECRA), as originally drafted, only granted BIS the authority to regulate such activities if they were in connection with "foreign military-intelligence" end-users. “Military-intelligence” end-users is a narrow subset of foreign military, intelligence and security end-users. In 2022, a bipartisan group of Members of Congress realized that this gap in ECRA left civilian intelligence and security agencies, such as China’s Ministry of State Security, entirely outside the scope of the authority for BIS to impose licensing requirements. To resolve this glaring national security gap, we worked on a bipartisan basis to expand this authority for BIS to also control U.S. person services and items for non-military intelligence and security agencies too.

The first Trump Administration implemented the 2018 ECRA authority in January 2021, adding new export controls in the EAR covering U.S. person support for “military-intelligence” end-uses or end-users and over the export, reexport, and transfer of otherwise controlled items for military-intelligence end-use or end uses in China and other countries of concern. We request that the Trump Administration close the loopholes with the authority Congress created for BIS in 2022.

To ensure that these regulations are genuinely effective and leave no room for evasion, the final rule must incorporate the key strengthening measures identified by Congress during the 2024 public comment period, which include:

- Extending export controls to cover all serial human rights abusers and espionage threats. The originally proposed country lists omitted numerous repressive regimes and nations that conduct espionage against the United States. BIS should establish a "trusted countries list" composed of nations with strong track records of respecting human rights and that do not surveil the United States. A license should be required for U.S. persons to do business with intelligence and security agencies in all countries not on that list. Additionally, BIS must harmonize the framework so that any transaction with a foreign security agency requires a license under the same strict standards applied to intelligence agencies, rather than limiting security controls to narrow lists or specific items.

- Close due diligence loopholes for private surveillance contractors. Private spyware and cyber-surveillance firms frequently mask their client lists to bypass regulations. BIS must close this loophole by explicitly applying export restrictions to all foreign surveillance technology companies unless they provide their U.S. suppliers with a sworn attestation confirming that their clients do not include any intelligence or security end-users outside the trusted countries list.

- Control the export of all biometric surveillance and classification technologies: Although the 2024 draft rule proposed adding facial recognition to the EAR's Commerce Control List (CCL), oppressive regimes rely on a wider array of digital tracking tools. The final regulations must expand this category to include broader biometric identification technologies—such as gait or cardiac signature recognition—as well as biometric classification technologies used to sort individuals by demographic traits such as race, sex, or ethnicity.

Implementing these crucial enhancements to fully close this loophole is vital to preventing foreign adversaries from leveraging American tools and expertise against the U.S. government, our citizens and strategic interests.

Thank you for your prompt attention to this urgent matter.

Sincerely,

Ron Wyden
United States Senator

Pat Harrigan
Member of Congress

Peter Welch
United States Senator

John Cornyn
United States Senator

Sara Jacobs
Member of Congress

Michael T. McCaul
Member of Congress