

# Congress of the United States

Washington, DC 20515

October 31, 2024

The Honorable Alan F. Estevez  
Under Secretary of Commerce for Industry and Security  
Bureau of Industry and Security  
United States Department of Commerce  
1401 Constitution Ave NW  
Washington, DC 20230

## **Response to proposed rules, with request for comment:**

- *End-Use and End-User Based Export Controls, Including U.S. Persons Activities Controls: Military and Intelligence End Uses and End Users*
- *Export Administration Regulations: Crime Controls and Expansion/Update of U.S. Persons Controls*

Dear Mr. Estevez:

I write to commend the Bureau for its work to protect human rights and U.S. national security by implementing a law that I authored with Senator John Cornyn and Congressman Tom Malinowski in 2022, and urge you to further strengthen the Bureau's proposed regulations in order to keep American technologies and expertise out of the hands of repressive foreign military, intelligence, and security agencies.

The proposed export controls will make it harder for regimes to engage in human rights abuses ranging from mass surveillance of their citizens to hacking into the phones of dissidents and independent journalists. However, I am concerned that the draft rules contain gaps that would allow autocratic governments to continue buying technologies and services from American companies to commit human rights abuses. This is not just a human rights issue. Surveillance technologies and services provided to foreign governments by American cyber mercenaries can be exploited by foreign governments against Americans, or even the U.S. government, threatening national security.

There is a long and disturbing history of American corporations facilitating human rights abuses by selling technology to oppressive regimes. For example, IBM sold computers to South Africa's apartheid-era government that the regime used to maintain racial classification records. Before that, the company sold punch card machines that the Nazis used to run concentration camps. Cisco custom-built the so-called "Great Firewall of China," which enables the Chinese government to conduct surveillance and censorship against its citizens. More recently, Gatekeeper Intelligence Security sold facial recognition technology to the repressive monarchies of Saudi Arabia and the United Arab Emirates and Honeywell helped Egypt's military dictatorship build an AI-powered network of surveillance cameras.

American surveillance-related exports are not limited to physical items. According to an investigative report published by Wired, the U.S. technology company Corellium, which operates a cloud-based platform for discovering software vulnerabilities in phones, has sold access to its services to surveillance companies that develop technologies for hacking into phones and whose customers include security agencies in China, Saudi Arabia, and Bahrain.

Our country's export control regulations can be an effective tool for keeping American technology out of the hands of those who would use them to commit grave harms. But while there are controls on the sale of some technologies and services to foreign intelligence agencies, significant gaps exist in current controls. This means that American technology companies and surveillance mercenaries can equip dictatorships with the tools of oppression and terror without any review by U.S. government agencies. In response, Senator Cornyn, Congressman Malinowski, and I authored legislation that became law in 2022, giving the Bureau of Industry and Security (BIS) the authority to regulate the export of all products and the provision of all services by Americans to foreign military, intelligence, and security agencies.

The Biden-Harris administration has made bold efforts to reform U.S. export controls to curb technology-enabled human rights abuses, particularly by foreign makers of spyware. The administration took another step in the right direction in July 2024, when BIS proposed a pair of draft rules implementing the Wyden-Cornyn-Malinowski law. The proposed rules would create new requirements for U.S. exporters to apply for a license before doing business with "security end users" such as police agencies or "intelligence end users" in certain countries. Under these proposed rules, BIS could deny an application if it concluded that there was an unacceptable risk that the security or intelligence agency would use the technologies to commit human rights abuses or undermine the security of the United States.

While the proposed rules would be a major step forward for human rights and U.S. security, some gaps exist that are likely to limit their effectiveness. I urge you to strengthen the proposed rules by making the following changes:

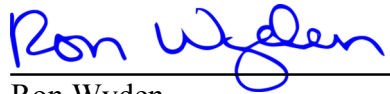
1. **Extend export controls to cover all serial human rights abusers and countries that have a history of conducting espionage against the United States government.**
  - a. The proposed license requirements for exports of U.S.-origin goods to foreign security agencies (known as end-use and end-user rules) would apply only to the 23 countries that are under arms embargoes or unilateral economic embargoes, or are designated as state sponsors of terrorism, which leaves out many other severely repressive regimes, such as the governments of Azerbaijan, Egypt, Laos, Saudi Arabia, Turkmenistan, the United Arab Emirates, and Vietnam.
  - b. While the proposed end-use / end-user licensing requirements for exports to foreign intelligence agencies would apply to a longer list of countries (45), this list also omits many regimes that have troubling human rights records, such as Algeria, Brunei, El Salvador, Ethiopia, Hungary, India, Morocco, Thailand, Tunisia, Turkey, and Uganda. The list also leaves out the home countries of some state and non-state foreign intelligence entities that carry out espionage and other disruptive activities against the United States.

- c. BIS should create a list of trusted countries that have strong track records of respecting human rights and that do not pose an espionage or cyber threat to the United States. The intelligence and security end-use / end-user rules should require a license to do business with intelligence and security agencies in all countries not on that list.
  - d. Unlike the intelligence end-use / end-user rule, which covers all exports to intelligence agencies in specified countries, the security end-use / end-user rule would only control exports of specific goods that BIS has identified on the Commerce Control List (CCL). Similarly, while BIS would require American companies or individuals to apply for a license to help any intelligence agency in a specified country obtain or use foreign-made goods (known as a U.S. persons rule), such a transaction with a foreign security agency would only require a license if BIS had specifically named the agency on the Entity List.
  - e. BIS should instead require a license for any transaction with a foreign-security agency that would be controlled if the customer was an intelligence agency.
2. **Close loopholes in due diligence requirements for exporters and consultants.**
- a. The proposed rules also apply if a U.S. company wants to do business with a private foreign company that provides goods or services to intelligence or security agencies in designated countries. However, the rules contain a loophole: no license would be required if the foreign company does not disclose its client list. And as a general rule, surveillance companies such as spyware providers don't reveal which governments they sell to.
  - b. BIS should close this loophole by clarifying that the export restrictions apply to exports and services provided to all foreign companies that have not provided their U.S-suppliers with a sworn attestation that their clients do not include any intelligence or security end users in any country outside the trusted countries list.
  - c. This measure would enable BIS to review proposed transactions with foreign companies that do work with agencies outside trusted countries, while minimizing compliance burdens on U.S. exporters and providing them safe harbor protections.
  - d. Such a requirement will create strong incentives for foreign surveillance technology companies to restrict their government customers to those on the trusted country list, which will further limit dictators' access to digital tools of repression.
3. **Control the export of all biometric surveillance technologies.**
- a. BIS is also proposing to add facial recognition technologies to the CCL. This update will require vendors of facial recognition systems to apply for a license before exporting these products, so BIS can ensure they are not sold to governments intending to misuse them to carry out mass surveillance of protestors and dissidents. Yet facial recognition is not the only kind of biometric technology that can be misused for surveillance. BIS should instead create a broader category of biometric identification technologies, to include systems designed to identify individuals based on other unique biometric characteristics, such as gait or cardiac signature.
  - b. There are also biometric technologies that are designed to classify individuals into demographic groups (e.g. age, sex, ethnicity) or infer mental states such as

aggression. While these technologies do not directly identify individuals, they can still enable oppressive surveillance. BIS should also add a category for biometric classification technologies to the CCL.

Thank you for your attention to this important human rights issue.

Sincerely,

A handwritten signature in blue ink that reads "Ron Wyden". The signature is fluid and cursive, with the first name "Ron" and last name "Wyden" clearly distinguishable.

---

Ron Wyden  
United States Senator