October 15, 2024

U.S. Department of Commerce
Regulations Branch
Bureau of Industry and Security
14th Street and Pennsylvania Avenue NW
Washington, DC 20230

RE: Proposed Rules – End-Use and End-User Based Export Controls, Including U.S. Persons Activities Controls: Military and Intelligence End Uses and End Users in Docket 240712-0193 (RIN 0694-AJ43) and Export Administration Regulations: Crime Controls and Expansion/Update of U.S. Persons Controls in Docket 240712-0191 (RIN 0694-AI35)

Access Now, Advocacy for Principled Action in Government, Amnesty International, the Committee to Protect Journalists, the Electronic Privacy Information Center, Freedom House, Human Rights Watch, the Organization for Identity & Cultural Development, Resilience Technologies, and Transparência Brasil appreciate the opportunity to provide comments to the Bureau of Industry and Security (BIS) in response to its proposed rules. We view export controls as critical tools in protecting and advancing human rights and democracy around the world, and we commend BIS for its efforts to strengthen its export control regulations and licensing policies to this end.

Access Now is an international organization that defends and extends the digital rights of people and communities at risk worldwide. By combining direct technical support, strategic advocacy, grassroots grantmaking, and convenings such as RightsCon, Access Now fights for human rights in the digital age.

Advocacy for Principled Action in Government offers expert policy analysis and recommendations to governmental leaders and other powerful actors to support the continuation and progressive evolution of key domestic and international law regulations, norms, standards, and good practices to protect and expand the rule of law, civil liberties, human rights, privacy, social and environmental sustainability, democracy, peace, security, transparency, accountability, and justice, including to optimize the positive pro-social potential and minimize the downside risks of existing and emerging technologies in such realms as surveillance, control, cybersecurity, artificial intelligence, facial recognition, robotics, lethal autonomous weapons, and quantum computing.

Amnesty International is an international non-governmental, non-profit organization representing the largest grassroots human rights movement in the world, with more than ten million members, supporters and activists. Amnesty International USA is the global organization's presence in the United States, and includes members and activists in all 50 states. Amnesty International's mission is to undertake research and action focused on preventing and ending grave abuses of all of the human rights enshrined in the Universal Declaration of Human Rights and other international human rights instruments. Amnesty International advocates for global

compliance with international human rights law, the development of human rights norms, and the effective enjoyment of human rights by all persons. It monitors state compliance with international human rights law and engages in advocacy, litigation, and education to prevent and end human rights violations and to demand justice for those whose rights have been violated. Amnesty International has researched, documented, and campaigned on the human rights impacts of biometric mass surveillance technologies, including facial recognition.

The Committee to Protect Journalists (CPJ) is an independent, nonprofit organization that promotes press freedom worldwide. CPJ defends the right of journalists to report the news safely and without fear of reprisal.

The Electronic Privacy Information Center (EPIC) is a public interest research center based in Washington, DC that uses advocacy, research, and litigation to secure the fundamental right to privacy in the digital age for all people in order to protect freedom of expression and democratic values.

Freedom House is the oldest human rights and democracy organization in the United States, founded in 1941 by Eleanor Roosevelt and Wendell Wilkie. The organization works to expand and defend freedom in the United States and around the world through a unique combination of research, programming, and advocacy.

Human Rights Watch is an international nongovernmental human rights organization whose work involves investigating and documenting violations of international human rights and humanitarian law by state and non-state actors in over 100 countries around the world.

The Organization for Identity & Cultural Development (OICD.net) addresses destructive tribalism, polarization, and conflict, especially their effects on vulnerable groups, by systematically applying knowledge from the Arts, Humanities, Human, Life, Data and Computer Sciences to ethically and intelligently repair identity-based and cultural divisions (often worsened by social media, facial recognition, artificial intelligence, and other technologies), to deploy real world educational and advocacy activities and interventions that help prevent and reverse harms such as persecution, discrimination, inequality, violent conflict, terrorism, and climate change.

Resilience Technologies is a social enterprise providing research-driven, innovative digital security solutions and services to civil society organizations, at-risk communities, and democracy defenders across Africa. The organization provides technical assistance and strategic guidance to civil society and at-risk communities to enhance their institutional capacity, fortify them against digital threats and attacks, and ensure that their work is without disruption.

Transparência Brasil is an independent Brazilian civil society organization founded in 2000 and dedicated to fostering efficiency and quality of public expenditures through the promotion of public transparency and civic oversight. The organization works towards defending public interest and the integrity of public institutions as a means of strengthening democracy.

Access Now, Advocacy for Principled Action in Government, Amnesty International, the Committee to Protect Journalists, the Electronic Privacy Information Center, Freedom House, Human Rights Watch, the Organization for Identity & Cultural Development, Resilience Technologies, and Transparência Brasil applaud many aspects of the proposed rules. To strengthen the proposed end user controls even further, we encourage BIS to expand the current country scopes for foreign-security and military end-users to include all Group D countries (in alignment with the country scope for intelligence end users). In addition, we recommend that new rules create a “remote biometric identification” technology control and improved export transparency. Detailed recommendations follow below.

Executive summary

I. Setting the scene: U.S. global leadership needed to combat malign uses of surveillance technologies
II. Response to proposed rules
    a. Intelligence end user control
    b. Foreign-security end user control
    c. Military end user control
    d. U.S. persons controls and restrictions
    e. Facial recognition technology control
III. Recommendations for new rules
    a. “Remote biometric identification” technology control
    b. Improved export transparency
IV. Conclusion

Setting the scene: U.S. global leadership needed to combat malign use of surveillance technologies

Surveillance technologies used in the facilitation of human rights violations and/or abuses close democratic space, harm the ability of human rights defenders and journalists to do their work, and undermine U.S. national security and foreign policy objectives. The proposed rules from the BIS would help curb the proliferation of such surveillance technologies and send an important signal to governments around the world that action is needed to curb their abuse. It cannot be overstated that U.S. government leadership on this topic, given the U.S.'s role as a hub of technological innovation, is essential to defend human rights and democracy in the digital age.

We encourage the U.S. government to work with countries around the world to replicate these proposed rules to stem the flow of surveillance technologies used in the facilitation of human rights violations and/or abuses. The U.S. government has already taken admirable steps to leverage export controls to protect human rights, such as through the Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware, which explicitly notes the importance of export controls, and the Export Controls and Human Rights Initiative.

Response to proposed rules

We commend the BIS for the proposed rules and offer tailored recommendations to ensure the new policies achieve the greatest impact.

1. ***Intelligence end user control***

We applaud the proposed revision of the "intelligence end user" control, to include "foreign government intelligence, surveillance, or reconnaissance organizations or other entities performing functions on behalf of such organizations." Many foreign government intelligence agencies are known facilitators of human rights violations, within and beyond their borders. For example, the Rwandan government engages in extraterritorial surveillance of Rwandan nationals viewed as a threat to the government.[1]

We also appreciate that the country scope for this end user control is expansive, as it includes countries in Country Groups D and E (that are also not identified in Country Group A:5 or A:6 of supplement no. 1 to part 740 of the Export Administration Regulations (EAR)). Country Groups D and E include countries that pose a national security threat to the United States or are at risk of misusing weapons or other arms.[2] While this is a positive step forward, there are more

[1] Human Rights Watch. *"Join us or die": Rwanda's Extraterritorial Repression*. (2024, April 22). https://www.hrw.org/report/2023/10/10/join-us-or-die/rwandas-extraterritorial-repression.
[2] Countries in Group D and/or Group E (that are also not identified in Country Group A:5 or A:6) are Afghanistan, Armenia, Azerbaijan, Bahrain, Belarus, Burma, Cambodia, Central African Republic, People's Republic of China (China), Democratic Republic of Congo, Cuba, Egypt, Eritrea, Georgia, Haiti, Iran, Iraq, Jordan, Kazakhstan, Kuwait, Kyrgyzstan, Laos, Lebanon, Libya, Macau, Moldova, Mongolia, Nicaragua, North Korea, Oman, Pakistan, Qatar, Russia, Saudi Arabia, Somalia, South Sudan, Sudan, Syria, Tajikistan, Turkmenistan, United Arab Emirates, Uzbekistan, Venezuela, Vietnam, Yemen, and Zimbabwe.

countries with problematic records of misusing surveillance tools that should also be subject to these rules.

To enhance the effectiveness of this control, we suggest that the description explicitly note that "intelligence end user" refers to both foreign intelligence gathering *and* domestic intelligence gathering. Without this language, the control may be misinterpreted to refer to exclusively foreign intelligence gathering. Domestic intelligence services often leverage surveillance technologies in the facilitation of human rights abuses. For example, in Zimbabwe, the Central Intelligence Organization allegedly used Circles spyware to record conversations of Vice President Kembo Mohadi.[3]

2. Foreign-security end user control

We applaud the proposed creation of the new "foreign-security end user" control that appropriately includes, among other actors, law enforcement bodies, which are often perpetrators of human rights violations. For example, in China, the police surveilled 1.2 million mobile phones in Xinjiang to identify Uyghur and other Turkic Muslim residents for interrogation and arrest as part of the government's crimes against humanity in the region.[4]

In addition, we especially appreciate that the expansive definition of "foreign-security end user" includes law enforcement and security services at all levels of government, including municipal, provincial, and regional. We are also pleased to see that the proposed rule includes non-government entities as a potential foreign-security end user, since private sector entities may help support government authorities to facilitate human rights abuses. For example, in Zimbabwe, the government partnered with United Arab Emirates-based company Mulk International to build "Zim Cyber City." According to Context,[5] Mulk International claims "Zim Cyber City" will utilize surveillance technology connected directly to law enforcement agencies.[6]

We also appreciate that the BIS's assessment in the proposed rules notes, "using a Country Group reference instead of a specific list of countries or destinations promotes ease of regulatory compliance and reduces regulatory complexity." While we agree with this statement, we encourage BIS to expand the current proposed country scope of D:5 and E countries to include all countries in Group D (that are not also identified in Country Group A:5 or A:6 of supplement no. 1 to part 740 of the EAR).

---

[3] NewsHawks. *Zim uses Israeli spying technology to snoop on Citizens' calls, messages*. (2021, February 27). https://web.archive.org/web/20210227105209/https:/thenewshawks.com/zim-uses-israeli-spying-technology-to-snoop-on-citizens-calls-messages.

[4] Human Rights Watch. *China: Phone search program tramples Uyghur rights*. (2023, May 4). https://www.hrw.org/news/2023/05/04/china-phone-search-program-tramples-uyghur-rights.

[5] Matiashe, F. S. *Zimbabwe's Cyber City: Urban utopia or surveillance menace?* (2023, February 20). Context. https://www.context.news/surveillance/zimbabwes-cyber-city-urban-utopia-or-surveillance-menace.

[6] Macdonald, A. *Zimbabwe govt faces criticism over biometric surveillance project for New Smart City: Biometric update*. (2023, February 28). Biometric Update. https://www.biometricupdate.com/202302/zimbabwe-govt-faces-criticism-over-biometric-surveillance-project-for-new-smart-city.

This country scope expansion for foreign-security end user controls to include all countries in Group D is important for two main reasons:

- First, it would ensure countries identified in lists D:1-D:4 do not fall through the cracks. For example, a police command center (a foreign-security end user) in Kyrgyzstan (a D:1 and D:3 country) is expanding use of facial recognition technology.[7] Kyrgyzstan recently signed a data sharing agreement with the Russian government to provide information that could include identifying Russian conscripts who escaped military service or anti-war activists. Since Kyrgyzstan is not a D:5 country, it would not be captured in the foreign-security end user category as currently proposed. This is a clear missed opportunity for the U.S. government to leverage its export control authorities to combat repression from the Russian and Kyrgyzstan governments, at home and abroad.[8]
- Second, relying on different country lists to separately control foreign intelligence and foreign-security support may be complicated and counterproductive. Restricting support to an intelligence end user but not a foreign-security end user (i.e., local law enforcement) in the same country may create holes in the export control regime that companies and governments exploit.

3. Military end user control

Like our recommendations regarding the expanded country scope for foreign-security end users, we also encourage the BIS to include all D and E countries (that are not also identified in Country Group A:5 or A:6 of supplement no. 1 to part 740 of the EAR) for the military end user control. Like intelligence end users and foreign-security end users, military end users may also facilitate human rights violations. For example, in Venezuela, the General Directorate of Military Counterintelligence allegedly acquired Cellebrite's surveillance technology to likely spy on human rights defenders.[9] (Cellebrite has denied directly selling the software to the Venezuelan government.[10])

4. U.S. person controls and restrictions

We applaud the proposed expansion of U.S. person controls for activities in connection with foreign-security end users, and the proposed revisions to U.S. person restrictions for support of military and intelligence end users. These changes make it more challenging for U.S. persons to

[7] Mills, L., & Wang, M. *Facial recognition deal in Kyrgyzstan poses risks to rights*. (2019, November 15). Human Rights Watch. https://www.hrw.org/news/2019/11/15/facial-recognition-deal-kyrgyzstan-poses-risks-rights.
[8] The Moscow Times. *Kazakhstan and Kyrgyzstan to share data with Moscow on anti-war Russians, conscripts*. (2023, June 22). https://www.themoscowtimes.com/2023/06/22/kazakhstan-and-kyrgyzstan-to-share-data-with-moscow-on-anti-war-russians-conscripts-a81594.
[9] Diario las Américas. *Régimen de Maduro Hackea Celulares con software de Empresa Israelí*. (2021, November 1). https://www.diariolasamericas.com/america-latina/regimen-maduro-hackea-celulares-software-empresa-israeli-n4235839.
[10] Yaron, O. *Israeli firm Cellebrite allegedly sold phone-hacking tech to Venezuela; company says will not sell its new system to the current regime.* (2020, September 11). Haaretz via Business & Human Rights Resource Centre. https://www.business-humanrights.org/en/latest-news/israeli-firm-cellebrite-allegedly-sold-phone-hacking-tech-to-venezuela-company-says-will-not-sell-its-new-system.

abet the malign activities of foreign governments, which happened, for example, when former U.S. National Security Agency employees worked on behalf of the United Arab Emirates to surveil human rights defenders, according to Reuters.[11] U.S. persons should not support the activities of foreign-security, military, and intelligence end users that facilitate human rights violations.

5. Facial recognition technology control

We applaud the proposed control for facial recognition technology (FRT) used for mass surveillance and crowd scanning. It is well-documented that this particular use facilitates human rights violations and/or abuses that undermine not only the right to privacy, but also the rights to free expression and assembly. For example:

- In Russia, a 34-year-old English teacher Yulia Zhivtsova was detained on a metro platform when police scanned her face and matched it to a picture taken a month prior at an anti-war protest. Another protest was happening that day, and even though Yulia was not planning on attending, the police arrested her "preemptively" and detained her for several hours to prevent her participation.[12]
- In Uganda, the government used FRT to identify and arrest alleged protesters demonstrating against the arrest of an opposition presidential candidate.[13]

The use of FRT to analyze photo and video footage of peaceful protests and demonstrations to specifically identify and/or punish protesters may deter individuals from participating in protests, thus limiting the rights to free expression and peaceful association and assembly. Crucially, opacity in the future use or sharing of biometric data collected at protests, and the lack of safeguards against this, can also further complicate any calculation an individual makes to assemble. As in the example of Yulia, once a government actor identifies a face, a person may become a marked target for harassment and/or detention. All to say, it is the technology that so dramatically amplifies the power of repressive governments.

The UN Human Rights Committee that oversees the implementation of the International Covenant on Civil and Political Rights, which the U.S. government signed and ratified, makes clear that the use of surveillance at protests and other assemblies can have a chilling effect.[14] In addition, the former UN Special Rapporteur on the promotion and protection of the right to

[11] Bing, C., & Schectman, J. *Exclusive: Ex-NSA cyberspies reveal how they helped hack foes of UAE*. (2019, January 30). Reuters Investigates: Project Raven. https://www.reuters.com/investigates/special-report/usa-spying-raven.
[12] Loucaides, D. *The changing face of protest*. (2024, March 27). Rest of World. https://restofworld.org/2024/facial-recognition-government-protest-surveillance/#/an-end-to-privacy.
[13] Kafeero, S. *Uganda is using Huawei's facial recognition tech to crack down on dissent after anti-government protests*. (2020, November 27). Quartz. https://qz.com/africa/1938976/uganda-uses-chinas-huawei-facial-recognition-to-snare-protesters.
[14] United Nations Human Rights Committee. *General comment No. 37 (2020) on the right of peaceful assembly (Article 21),* para 10. (2020, September 17). https://documents.un.org/doc/undoc/gen/g20/232/15/pdf/g2023215.pdf.

freedom of opinion and expression, David Kaye, acknowledged the chilling effect of surveillance on the rights to freedom of expression and association:

> "In environments subject to rampant illicit surveillance, the targeted communities know of or suspect such attempts at surveillance, which in turn shapes and restricts their capacity to exercise rights to freedom of expression [and] association."[15]

Furthermore, governments may use this technology to intentionally target certain individuals or groups of people based on their protected characteristics, including ethnicity, race, and gender.[16] For example, in China, FRT systems, including those of the Chinese Company Sensetime, are used to identify and profile Uyghur and other Turkic Muslims, against whom China continues to commit crimes against humanity.[17] The Chinese government also uses FRT to surveil Uyghurs who have foreign ties.[18] The discriminatory impacts of the technology have an especially devastating impact in repressive societies like the Uyghur region, where it is used in ways that can exacerbate the abuses against already-marginalized groups of people.

What is more, FRT has a high inaccuracy rate for people from marginalized groups. In the United States, Black and other communities of color are most at risk of being misidentified and falsely arrested – in some cases, facial recognition has a 95% inaccuracy rate.[19] And, in a study by Timnit Gebru and Joy Boulamwini, FRT algorithms were found to generate a greater error rate for people—especially women—of color.[20] Due in part to the biased training data used when developing the system, the technology has been embroiled in false arrests of Black people.[21]

---

[15] Office of the United Nations High Commissioner for Human Rights. *A/HRC/41/35: Surveillance and human rights - Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. (2019, May 28). https://www.ohchr.org/en/documents/thematic-reports/ahrc4135-surveillance-and-human-rights-report-special-rapporteur.

[16] Amnesty International. *Ban the Scan NYC*. (2022). https://banthescan.amnesty.org/nyc.

[17] Bhuiyan, J. *US sanctioned China's top facial recognition firm over Uyghur concerns. It still raised millions*. (2022, January 7). The Guardian. https://www.theguardian.com/world/2022/jan/06/china-sensetime-facial-recognition-uyghur-surveillance-us-sanctions.

[18] Amnesty International. *China: Draconian repression of Muslims in Xinjiang amounts to crimes against humanity*. (2021, June 10). https://www.amnesty.org/en/latest/news/2021/06/china-draconian-repression-of-muslims-in-xinjiang-amounts-to-crimes-against-humanity.

[19] Amnesty International. *Ban the Scan NYC*. (2022). https://banthescan.amnesty.org/nyc.

[20] Buolamwini, J., & Gebru, T. *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*. (2018). Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81:77-91. https://proceedings.mlr.press/v81/buolamwini18a.html.

[21] Thanawala, S. *Facial recognition technology jailed a man for days. His lawsuit joins others from Black plaintiffs*. (2023, September 25). AP News. https://apnews.com/article/mistaken-arrests-facial-recognition-technology-lawsuits-b613161c56472459df683f54320d08a7.

Further recommendations

Our additional recommendations are intended to help strengthen U.S. export control regulations and licensing policies to best protect human rights in the digital age.

1. "Remote biometric identification" technology control

In addition to FRT, other remote biometric-enabled technologies can facilitate human rights violations and/or abuses. Therefore, we propose that "remote biometric identification" should also be included in the Commerce Control List.

"Remote biometric identification" tools use machine learning processes, like those undergirding FRT, that collectively result in the ability to identify or distinguish a person from a larger set of individuals (i.e. one-to-many matching). NIST defines "biometrics" as "the measurement of physiological characteristics like – but not limited to – fingerprint, iris patterns, or facial features that can be used to identify an individual."[22] The use of these technologies to single out or track individuals using their eyes, gait, voice, personal appearance, or any other biometric identifier in a manner that enables mass surveillance may impact the human rights of religious, ethnic, and racial minorities, political dissidents, and other marginalized groups.[23] For example, a government authority could compare a person's gait to a database of people walking from a protest or religious ceremony to see if there is a match. This database might be relatively small (i.e. a watch-list) or very large (i.e. a national identity database).[24]

Specific examples of remote biometric-enabled human rights violations include:

- In China, pseudo-scientific inferences about emotional state may be used in some cases in ways that restrict individuals' ability to access their basic rights.[25]
- In Russia, race detection technologies purport to be able to identify the racial category of individuals, generating heightened risk for those most subject to biases.[26]

2. Improved export transparency

Finally, we believe that, in addition to these expanded controls, further transparency around the issuance of licenses to, and exports by, U.S. persons and entities, concerning technology items that have the potential to undermine human rights, would enable better cooperation between the Department of Commerce and civil society organizations to prevent human rights violations

[22] National Institute of Standards and Technology, US Department of Commerce. (2021, December 1). Biometrics. https://www.nist.gov/programs-projects/biometrics.
[23] Amnesty International. *Open letter calling for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance.* (2021, August 16). https://www.amnesty.org/en/documents/doc10/4254/2021/en.
[24] European Digital Rights (EDRi). *Remote biometric identification: a technical & legal guide*. https://edri.org/our-work/remote-biometric-identification-a-technical-legal-guide.
[25] ARTICLE 19. *Emotion Recognition Technology Report*. https://www.article19.org/emotion-recognition-technology-report.
[26] Bacchi, U. *Analysis- "Racist" facial recognition sparks ethical concerns in Russia*. (2021, July 5). Reuters. https://www.reuters.com/article/world/analysis-racist-facial-recognition-sparks-ethical-concerns-in-russia-idUSKCN2EB0BB.

and/or abuses. We understand there are confidentiality requirements, set forth in 15 CFR 748.1(c), regarding information collected for the purpose of considering license applications. However, we believe that even within the current regulatory framework, more comprehensive, consistent, and frequent reporting, on an anonymized and aggregated basis, regarding licensing and export flows can be published.

While we commend the publication of the “Annual Country Licensing and Trade Analysis" reports available on the BIS website (both the country-specific and global), we note that the last round of reports published concerns 2022 data and that there are gaps in terms of the countries covered in the reports. We would encourage BIS to produce annual reports that not only address a greater number of countries, but to also make certain data available every six months to allow for public use to enable timely responses to emerging patterns of exports potentially related to human rights abuses. Moreover, the structure of these reports is such that information is at times presented at the level of Export Control Classification Number (ECCN) “series” and not specific ECCN classifications, except for the “Top Ten ECCN” lists. A more nuanced presentation of information regarding the export of key technology items, like FRT items, regardless of their relative weight as compared to other items in terms of license issuances and exports, would facilitate the identification of exports used for malicious purposes.

Additionally, we believe that the “Annual Country Licensing and Trade Analysis" reports, and other publications meant to provide further transparency of critical exports, would benefit from increased coordination between BIS and the Census Bureau in terms of the information collected and analyzed. We understand that the Census Bureau similarly faces limitations due to confidentiality requirements set forth in 15 CFR 30.60(a). However, the Electronic Export Information (EEI) reports filed with the Automated Export System can provide information that could be presented on an anonymized and aggregated level to expand upon the data currently shared and make more transparent when exports of certain items controlled for human rights reasons are occurring.

For example, in line with other BIS efforts to better synchronize Schedule B and ECCN classifications, the BIS could work with Census to ensure that there are Schedule B numbers that can be more easily associated with items that are controlled for human rights reasons. To illustrate, FRT items do not have a clear designation under Schedule B and would likely be considered an “other” item, under either 8523 (“Discs, tapes, solid-state non-volatile storage devices, ‘smart cards,’ and other media for the recording of sound or of other phenomena,…” etc.) or 8543 (“Electrical machines and apparatus, having individual functions, not specified or included elsewhere in this chapter”). Therefore, information under these present Schedule B classifications would not be useful for purposes of public scrutiny of FRT exports. However, a clearer mapping between information drawn from EEI reports and ECCN numbers could enable Census to collect the information required to support BIS efforts to gather information necessary to assess the efficacy of its own controls and to make the data accessible for public review to further civil society efforts to advance human rights. The BIS could also ensure that EEI filings for the export of items that are controlled for human rights purposes are made by amending 15

CFR 758.1(b) to include these exports among those for which exporters must file EEIs regardless of value and destination.

Conclusion

Access Now, Advocacy for Principled Action in Government, Amnesty International, the Committee to Protect Journalists, the Electronic Privacy Information Center, Freedom House, Human Rights Watch, the Organization for Identity & Cultural Development, Resilience Technologies, and Transparência Brasil applaud many aspects of the proposed rules that seek to strengthen export controls to better protect human rights around the world. Now more than ever, U.S. global leadership, and collaboration with other countries ready to act, is needed to combat the malign use of surveillance technologies that harm human rights. The new and/or modified intelligence end user control, foreign-security end user control, military end user control, U.S. person controls and restrictions, and facial recognition technology control are all major advances. To strengthen the proposed end user controls even further, we encourage BIS to expand the current country scopes for foreign-security and military end-users to include all Group D countries (in alignment with the country scope for intelligence end users). In addition, we recommend that new rules create a "remote biometric identification" technology control and improved export transparency.

Thank you again for the opportunity to submit comments on the proposed rules. Access Now, Advocacy for Principled Action in Government, Amnesty International, the Committee to Protect Journalists, the Electronic Privacy Information Center, Freedom House, Human Rights Watch, the Organization for Identity & Cultural Development, Resilience Technologies, and Transparência Brasil are grateful for the invitation to contribute and look forward to further collaboration on the topic.

Sincerely,

Michael DeDora
U.S. Policy and Advocacy Manager
Access Now

Chip Pitts
Chair, Advocacy for Principled Action in Government
Executive Committee, The Organization for Identity & Cultural Development

Amanda M. Klasing
National Director, Government Relations & Advocacy
Amnesty International USA

Gypsy Guillén Kaiser
Advocacy and Communications Director
The Committee to Protect Journalists

Jeramie D. Scott
Director, Project on Surveillance Oversight
The Electronic Privacy Information Center

Annie Boyajian
Vice President of Policy and Advocacy
Freedom House

Deborah Brown
Deputy Director, Technology and Human Rights
Human Rights Watch

Adeboro Odunlami
Programs Director
Resilience Technologies

Juliana Sakai
Executive Director
Transparência Brasil