Submitted via Federalregister.com

Jeremy Pelter
Acting Under Secretary
Bureau of Industry and Security
U.S. Department of Commerce
2201 C St., NW
Washington, DC 20520

December 6, 2021

RE: Comments of Access Now in response to an interim final rule from the Bureau of Industry and Security, Department of Commerce, Docket No. 211013-0209

Dear Mr. Pelter,

Thank you for the opportunity to submit our comments on the interim final rule.[1] We, Access Now, are an international non-governmental, non-profit organization working to defend and extend the digital rights of users at-risk around the world, with a particular focus on privacy and data protection, freedom of expression and assembly, digital security, and connectivity.[2]

Access Now has repeatedly called attention to the dangers of surveillance and censorship technologies,[3] and has urged governments to take active measures to stop the uncontrolled export and use of these tools to facilitate human rights violations.[4] This includes the tools sold by NSO Group and Candiru, which the Department of Commerce recently added to the Entity List.[5]

---

[1] *Information Security Controls: Cybersecurity Items*, Federal Register, https://www.federalregister.gov/documents/2021/10/21/2021-22774/information-security-controls-cybersecurity-items.
[2] *About Us*, Access Now, https://www.accessnow.org/.
[3] *From India to Rwanda, the victims of NSO Group's WhatsApp hacking speak out*, Access Now, https://www.accessnow.org/nso-whatsapp-hacking-victims-stories/; *Two years after Khashoggi's slaying, no accountability for spyware firm or Saudi government*, Access Now, https://www.accessnow.org/khashoggi-two-years-later/; *New report: FinFisher changes tactics to hook critics*, Access Now, https://www.accessnow.org/new-report-finfisher-changes-tactics-to-hook-critics/
[4] *Enough is enough! States must intervene on NSO Group's unchecked power*, Access Now, https://www.accessnow.org/enough-is-enough-nso-group/.
[5] *Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities*, U.S. Department of Commerce, https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list.

We applaud the introduction of new controls on cybersecurity items, a necessary step in the broader effort to control high-risk surveillance technologies. This proposal complements initiatives across the United States government intended to affirm human rights, press freedom, and democratic values through diplomacy. It also aligns with U.S. government efforts to ensure commercial entities only export goods and services for legitimate and human rights-respecting purposes. This proposed rule also strengthens global cooperation to integrate a human rights-based approach into export controls. Earlier this year, the European Union also adopted a new export control regime for dual-use surveillance items, which, among other things, increases transparency of exports and adds human rights risks as a criteria of the licensing assessment.[6] Access Now and our partners' advocacy spurred these EU reforms and we see the present proposal in line with this global drive towards accountability and transparency.

To ensure the Bureau of Industry and Security's (BIS) interim final rule will work as intended, we recommend the following:

1. **BIS should consider expanding the definition of "cybersecurity items" to sufficiently cover products with a high risk of repression.**

We understand that the definitions of "cybersecurity items," i.e., intrusion software and IP network surveillance, are aligned with those of the Wassenaar Arrangement decision of 2013, as amended in 2017.

However, these proposed definitions do not sufficiently cover certain products with a high risk of abuse, which should be equally controlled.

a. The scope of IP network surveillance systems (ECCN 5A001.j)

First, we have concerns that the requirements under 5A001.j.1.a. for controlled IP network communications surveillance systems or equipment are not strict enough. Surveillance technologies could be misused at any layer, not just at the application layer. Only controlling these technologies if they perform analysis at the *application* layer (e.g., Layer 7 of Open Systems Interconnection (OSI) model (ISO/IEC 7498-1)) on a carrier class IP network is too narrow. For example, exploitation of UDP, TCP, IP, and IPsec protocols or attacks similar to the NotPetya attack on Ukraine's infrastructure can be done at layers lower than application layers. Therefore, we recommend removing "analysis at the *application* layer" as a required function for controlling IP network communications surveillance systems.

Second, regarding the remaining requirements listed under 5A001.j.1., we believe that the requirement for controlled IP network communications surveillance systems to be performing *all* of those functions on a carrier class IP network is limiting. This is because *any one* of the listed functions on a carrier class IP network can allow governments to misuse these technologies and violate human rights.

[6] *New EU dual use export control rules finally adopted, but leave a lot of room for improvement*, Access Now, https://www.accessnow.org/eu-dual-use-export-control-rules-room-for-improvement/.

Third, certain surveillance technologies, such as the Blue Coat (now Symantec) Deep Packet Inspection (DPI) technology, do not have the function of mapping the relational network of an individual or of a group of people (j.2.b.). Nevertheless, it was found on networks of many human rights-violating regimes, such as China, Egypt, Russia, and Venezuela,[7] and used by the Syrian government for surveillance and filtering purposes.[8] Sandvine's DPI was also reportedly used to inject malicious and dubious redirects for users in Turkey, Syria, and Egypt.[9] Further, in 2020, Sandvine's DPI equipment was used in Belarus for internet throttling during the elections.[10] Thus, we also recommend revising the rule to include such technologies.

Finally, we also believe that the exemptions for marketing, network Quality of Service (QoS), or Quality of Experience (QoE) purposes should not be allowed for items performing *any* of the functions under 5A001.j.1. These exemptions introduce the risks of excluding equipment that may not be specifically designed or publicly marketed for intelligence gathering purposes, but can nevertheless be used for such purposes, especially when deployed on a carrier class IP network. Such is the nature of dual use surveillance items — they can be used for both commercial and military aims. For example, DPI technology can be used for network QoS purposes and spying on journalists and dissidents or censoring information. Thus, given that any one of the listed functions under 5A001.j.1. are highly invasive and can allow governments to exploit the grey areas to violate human rights, exemptions for marketing, QoS, or QoE should not be allowed.

b. The scope of Intrusion software (ECCN 4A005)

i. The rule should be robustly enforced against device forensic tools as well as remote hacking tools.

We understand the definition of "intrusion software," which are specially designed "to avoid detection by security monitoring tools or to defeat protective countermeasures," covers not only

---

[7] See, e.g., *Appendix A: Summary Analysis of Blue Coat "Countries of Interest,"* The Citizen Lab, https://citizenlab.ca/2013/01/appendix-a-summary-analysis-of-blue-coat-countries-of-interest/.
[8] *US probes Syria's use of internet blocking equipment*, BBC News, https://www.bbc.co.uk/news/mobile/technology-15437696; *Digital dominion: new report exposes the depth of Syrian regime's mass surveillance*, Access Now, https://www.accessnow.org/digital-dominion-syrian-regime-mass-surveillance/; *Planet Blue Coat: Mapping Global Censorship and Surveillance Tools*, The Citizen Lab, https://citizenlab.ca/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/.
[9] *BAD TRAFFIC: Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?*, The Citizen Lab, https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/.
[10] *Sandvine Use to Block Belarus Internet Rankles Staff*, Bloomberg, https://www.bloomberg.com/news/articles/2020-09-11/sandvine-use-to-block-belarus-internet-rankles-staff-lawmakers; *Francisco Partners-owned Sandvine profits from shutdowns and oppression in Belarus*, Access Now, https://www.accessnow.org/francisco-partners-owned-sandvine-profits-from-shutdowns-and-oppression-in-belarus/.

remote hacking tools, e.g. Pegasus spyware by NSO Group, but also device forensics tools, which overcome the security system of the device. The representative examples of these device forensic tools are Universal Forensic Extraction Device (UFED) by Cellebrite, Detective by Oxygen Forensic, SmartPhone Forensic System Professional (SPF Pro) by Salvationdata Technology, GreyKey by Greyshift, and Mobile Device Investigator by ADF.

Unlike remote hacking tools, these forensic tools need physical access to devices; however, they are similarly abused by authoritarian regimes against journalists, dissidents, and human rights defenders, without obtaining consent or with forced consent.[11] Therefore, we recommend robustly enforcing the final rule equally over those device forensic tools as well as remote hacking tools.

ii. The rule should control after-sales support, e.g., user training, project management, as well as pre-installation consultation.

Part 772 of Export Administration Regulations defines "technology" as "information necessary for the development, production, use, operation, installation, maintenance, repair, overhaul, or refurbishing [...] of an item." In contrast, ECCN 4E001 is defined as "[t]echnology" only for the "development" of "intrusion software." This narrower definition apparently covers only installation work of intrusion software and excludes the after-sale support work such as training, monitoring, and project management.

Companies which export spyware typically not only provide the spyware technology itself, but also ancillary services, such as installation, customization, training, monitoring, project management, and customer support, which are included in the price of the product.[12] To control the after-sales support as well as installation service, we recommend defining ECCN 4E001 as "[t]echnology" for "development," "production," "use," "operation," "installation," "maintenance," "repair," "overhaul," or "refurbishing" of "intrusion software."

2. BIS should consider controlling a larger set of surveillance technology items, beyond cybersecurity items.

Other than "cybersecurity items," there are technologies at high risk for facilitating human rights abuses, such as:

- Biometric surveillance technologies;[13]

---

[11] *What spy firm Cellebrite can't hide from investors*, Access Now, https://www.accessnow.org/what-spy-firm-cellebrite-cant-hide-from-investors/.

[12] E.g., NSO Group reportedly provides "ongoing technical support and other services to their clients as they deploy NSO's spyware against Apple's products and users, including journalists, human rights activists, dissidents, public officials, and others." (Apple v. NSO Group Complaint, https://www.apple.com/newsroom/pdfs/Apple_v_NSO_Complaint_112321.pdf)

[13] *Open letter calling for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance*, Access Now, https://www.accessnow.org/cms/assets/uploads/2021/06/BanBS-Statement-English.pdf; *Surveillance*

- Electronic systems or equipment, designed for surveillance and monitoring of the electromagnetic spectrum for military intelligence or security purpose;[14] and
- Unmanned Aerial Vehicles capable of conducting surveillance.[15]

We recommend expanding the scope of controlled items to include the above items.

3. BIS should engage with civil society to keep the control items updated.

Civil society organizations have first-hand, updated, and reliable information on the use of surveillance technologies against other civil society actors, such as journalists, human rights defenders, and activists. For example, organizations such as Access Now, The Citizen Lab, Amnesty International, Privacy International, Committee to Protect Journalists, and others have long been documenting and reporting on such abuses, facilitated by companies, such as NSO Group, Candiru, Sandvine, Cellebrite, Hacking Team, FinFisher, Blue Coat, and many others.[16]

To keep the list of controlled items updated, BIS should more actively engage with these organizations to gather relevant information, invite open input from the public, and modify the list under a transparent and clear process. To achieve this robust feedback, we recommend holding an annual consultation with civil society and establishing an ongoing civil society "point of contact" or liaison officer at BIS.

4. For the end-use restriction, BIS should require an exporter to conduct due diligence.

We are pleased with the end-use restriction introduced in the interim final report. BIS should establish the following supplemental rules to ensure the restriction operates effectively.

The interim final rule sets out that License Exception Authorized Cybersecurity Exports (ACE) is not authorized if the exporter knows or has reason to know at the time of export that the "cybersecurity item" will be used to affect the confidentiality, integrity or availability of information

---

Tech in Latin America: Made Abroad, Deployed at Home, Access Now, https://www.accessnow.org/surveillance-tech-in-latin-america-made-abroad-deployed-at-home/.

[14] *Colombia's record on privacy, surveillance, and human rights under renewed scrutiny at the United Nations*, Privacy International, https://privacyinternational.org/press-release/1326/colombias-record-privacy-surveillance-and-human-rights-under-renewed-scrutiny.

[15] *Drones, fever goggles, arrests: millions in Asia face 'extreme' Covid surveillance*, The Guardian, https://www.theguardian.com/global-development/2020/oct/01/drones-fever-goggles-arrests-millions-in-asia-face-extreme-covid-surveillance.

[16] E.g., see: *Two years after Khashoggi's slaying, no accountability for spyware firm or Saudi government*, Access Now, https://www.accessnow.org/khashoggi-two-years-later/; *Targeted Threats*, The Citizen Lab, https://citizenlab.ca/category/research/targeted-threats/; *Amnesty Tech*, Amnesty International, https://www.amnesty.org/en/tech/#disruptingsurveillance; *Taming Pegasus: A Way Forward on Surveillance Tech Proliferation*, Privacy International, https://privacyinternational.org/news-analysis/4602/taming-pegasus-way-forward-surveillance-tech-proliferation; *Spyware and Press Freedom*, Committee to Protect Journalists, https://cpj.org/spyware/.

or information systems, without authorization by the owner, operator, or administrator of the information system (including the information and processes within such systems).[17]

However, considering a cybersecurity item's inherent high risk of abuse, BIS should *not authorize* the License Exception ACE *unless* the exporter shows that it does not know or does not have reason to know that the item will be abused. For an exporter to meet this condition, BIS should request that, at the time of the export, the exporter:

> (i) performed end-use due diligence in accordance with the Guidance on Implementing the UN Guiding Principles for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities issued by the Department of State (Guidance);[18] and
> (ii) as a result of such due diligence, did not find any red flag which is specified in the Guidance or other risk indicators of abuse.

BIS should require the exporter to submit a sworn declaration and supplemental evidence to verify (i) and (ii). Companies often present their due diligence mechanism as effective, despite ample evidence that their internal controls fail or are inadequate to prevent the technologies from being repeatedly misused, like in the case of NSO Group.[19] Evidence-based judgment is critical.

Additionally, to bring more transparency to the value chain of cybersecurity items, BIS should require an exporter to publicly disclose the destination country(ies) for which License Exception ACE is authorized.

We thank you for the opportunity to provide these comments and reiterate our support for these rules, which, if strengthened as we outline above, will help ensure that cybersecurity items are only exported for legitimate purposes and do not contribute to repression of individuals around the world.

For more information, please contact Peter Micek, General Counsel of Access Now.

Peter Micek
General Counsel of Access Now (www.accessnow.org)
peter@accessnow.org | +1-888-414-0100 x709

[17] § 740.22 of the Export Administration Regulations.
[18] *Guidance on Implementing the UN Guiding Principles for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities*, U.S. Department of State, https://www.state.gov/wp-content/uploads/2020/10/DRL-Industry-Guidance-Project-FINAL-1-pager-508-1.pdf.
[19] *Rights groups to NSO: actions speak louder than words in human rights compliance*, Access Now, https://www.accessnow.org/nso-group-actions-louder-than-words-human-rights/.