23 August 2022

Gina M. Raimondo
U.S. Secretary of Commerce
1401 Constitution Ave NW
Washington, DC 20230

Antony J. Blinken
U.S. Secretary of State
2201 C St., NW
Washington, DC 20520

Lloyd J. Austin III
U.S. Secretary of Defense
1000 Defense Pentagon
Washington, DC 20301-1000

Jennifer M. Granholm
U.S. Secretary of Energy
1000 Independence Ave., SW
Washington, DC 20585

Re: Why NSO Group should not be removed from the U.S. Department of Commerce Entity List

We, the undersigned, represent a coalition of human rights and press freedom organizations around the world who monitor NSO Group's unabated use of spyware against human rights defenders and journalists without accountability and in contravention of fundamental freedoms and the rule of law. We, therefore, have commended the efforts made by the Department of Commerce in placing NSO Group on the Entity List for Malicious Cyber Activities (the "Entity List"), in recognition of these human rights abuses as well as risks to national security. This measure supports efforts to place human rights at the "center of U.S. foreign policy," including through export controls, and to counter digital authoritarianism globally. Equally, we are relieved to see the heightened scrutiny of NSO Group by the House Select Intelligence Committee, which has held its own public hearing on the threats of foreign-made, commercial spyware like NSO Group's Pegasus.

At the same time, we are alarmed by reports that NSO Group is making attempts to reverse their inclusion on the Entity List. For that reason, we are writing to you to submit that any reconsideration of

NSO Group's status on the Entity List is unwarranted, given that they continue to facilitate human rights abuses with impunity. In fact, the evidence of the use of Pegasus spyware against human rights defenders, journalists, opposition parties, and state officials by repressive regimes continues to mount, contrary to NSO Group's claim that their spyware is used as a tool for investigating criminal activitiy and terrorism.

The following are some of the key revelations since NSO Group was added to the Entity List on November 3, 2021, including prior targeting that has subsequently become publicly known:

- In November 2021, Lima Fakih, head of the Beirut office of Human Rights Watch, was informed by Apple that her iPhone may have been targeted by state-sponsored attackers. Fakih is a dual American-Lebanese citizen and frequently faces reprisal for her human rights advocacy. Forensic analysis by Human Rights Watch, with the support of Amnesty International's Security Lab, confirmed that her devices were infected with Pegasus. In response to NSO Group's claims that they take reports of abuse seriously and encourage victims to submit complaints pursuant to their Whistleblower Policy, Human Rights Watch submitted a complaint and supporting evidence that Pegasus was used to target Lima in January 2022. On June 27, NSO Group responded that their internal investigation did not find any evidence that the Human Rights Watch's staff member was targeted. This highlights the inefficacy of the internal safeguards at NSO Group, despite the company's repeated reassurances to the contrary.
- According to December 2021 reports, at least 11 U.S. diplomats based in Uganda learned that their devices were targeted with Pegasus. This underscores that U.S. officials and American citizens are and will continue to be vulnerable to these attacks by hostile actors that pose a substantial threat to national security.
- In December 2021, forensic analysis by Amnesty International revealed that the devices of four activists in Kazakhstan were infected with Pegasus between June and July 2021, further supporting allegations that Pegasus is used extensively against dissenters and human rights activists.
- In January 2022, Access Now and Front Line Defenders, with assistance from the Citizen Lab and Amnesty International's Security Lab, revealed the hacking of devices of two women human rights defenders from Bahrain and Jordan with Pegasus spyware in 2019 and 2021. These

revelations particularly bring to light the vulnerabilities of women in these contexts, compounded by existing gendered power imbalances.

- In January 2022, a report by Access Now and the Citizen Lab, in collaboration with Front Line Defenders and other organizations, confirmed 35 cases of journalists and members of civil society in El Salvador whose phones were infected with Pegasus spyware between July 2020 and November 2021.
- Between December 2021 and January 2022, investigations by the Citizen Lab revealed the hacking of Polish Senator Krzysztof Brejza, who was infected with Pegasus nearly three dozen times in 2019 when he was running the opposition's campaign; of Lawyer Roman Giertych and prosecutor Ewa Wrzosek; as well as of an agrarian political leader and the co-author of a book about the head of Poland's secret services. Research by Amnesty International also showed that Magdalena Łośko, the former assistant to Polish senator Krzysztof Brejza, and Brejza's father, Ryszard Brejza, received text messages in 2019 that were technically consistent with spyware attacks by clients of NSO Group using Pegasus.
- In March, an analysis by Amnesty International's Security Lab confirmed that two phones belonging to a prominent Sahraoui human rights defender in Morocco, Aminatou Haidar, were targeted and infected as recently as November 2021.
- In April 2022, Citizen Lab revealed that the devices of four Jordanian human rights defenders, lawyers, and journalists were hacked with Pegasus spyware between August 2019 and December 2021. **This is particularly concerning because an iPhone belonging to one of the targets was successfully hacked in December 2021, after the NSO Group's Entity List designation.**
- In April 2022, a report by the Citizen Lab also revealed evidence that at least 65 Catalonian individuals were infected with mercenary spyware, of which 63 were infected with Pegasus. These individuals included Members of the European Parliament, Catalan legislators, jurists, and members of civil society. A small sample of victim data was shared with Amnesty International, which verified the Citizen Lab's findings in accordance with their own methodology. Further, in May 2022, the Spanish government convened a press conference stating that the mobile phones of the prime minister, Pedro Sánchez, and the defence minister, Margarita Robles, were both infected last year with Pegasus spyware. It is alleged that foreign governments may have played a role in this targeting.

- It was also reported in April that Pegasus spyware may have been used to target the office of the Prime Minister, as well as the Foreign and Commonwealth Office in the United Kingdom.
- Alarmingly, the European Union is currently investigating evidence that its employees' phones have been compromised with Pegasus spyware. The EU Commissioner for Justice, Didier Reynders, received a notification from Apple that his devices may have been compromised by Pegasus. Though investigators analyzing the personal devices of Reynders and other EU staff have not found conclusive evidence that the devices were infected with Pegasus, they have found indicators of security compromises.
- In July 2022, the Citizen Lab, jointly with iLaw and DigitalReach, revealed "an extensive espionage campaign" targeting Thai pro-democracy protesters and activists calling for reforms, spanning between October 2020 and November 2021. The report identified at least 30 Pegasus victims among key civil society groups in Thailand, including activists, academics, lawyers, and NGO workers. **As the report demonstrates, a number of infections occurred after NSO Group's Entity List designation**. A few days after the report's publication, five members of Thailand's political opposition also revealed their devices had been compromised. The Thai Minister of Digital Economy and Society, Chaiwut Thanakamanusorn, admitted to the use of spyware in cases of national security by Thai authorities. He subsequently backtracked from this statement.
- Last month, the House Intelligence Committee heard testimony from Carine Kanimba, an American-Belgian citizen whose device was infected with Pegasus. This targeting took place around the same time Ms. Kanimba was communicating with U.S. and Belgian officials, including the U.S. Congressman Joaquin Castro, about the abduction and incarceration of her father, Rwandan activist Paul Rusesabagina, who inspired the film Hotel Rwanda. In July 2022, forensic experts at the Citizen Lab were further able to confirm the use of spyware against Mr. Rusesabagina's nephew, who is a Belgian citizen. This targeted surveillance thus impacts an American citizen and a Belgian citizen in their efforts to pursue remedies to assist an incarcerated activist, as much as it impacts state officials in Belgium and the United States that interact with their constituents.

In recognition of these harms, there have been calls for a moratorium on sale, transfer, and use of mercenary spyware by international human rights experts and state representatives. National and

regional courts and authorities all over the world, including the United States, the European Union, the United Kingdom, and India, are also continuing to scrutinize NSO Group's involvement in hacking of government officials, human rights defenders, and journalists. In the same vein, we acknowledge the efforts made by your offices in issuing a rule amending § 740.17 and § 740.22 of the *Export Administration Regulations* to impose controls on exports that can be used for malicious cyber activities in recognition of national security concerns.

We urge you to maintain the NSO Group's designation on the Entity List, in consideration of the mounting evidence of the unabated use of the spyware technology against human rights defenders, journalists, and state officials, and its impact on human rights advocacy, journalism, and democracy globally.

You may contact Peter Micek, General Counsel at Access Now at peter@accessnow.org, to facilitate detailed submissions or further evidence as may be required by your offices.

ORGANIZATIONS

Access Now
Amnesty International
ARTICLE 19
Committee to Protect Journalists (CPJ)
Heartland Initiative
Reporters Without Borders (RSF)

INDIVIDUALS

Courtney Radsch, Fellow, UCLA Institute for Technology, Law and Policy
David Kaye, Clinical Professor of Law, the University of California, Irvine School of Law
Hinako Sugiyama, Digital Rights Fellow, International Justice Clinic, the University of California, Irvine School of Law
John Scott-Railton, Senior Researcher, the Citizen Lab at the University of Toronto's Munk School of Global Affairs and Public Policy
Ron Deibert, Director, the Citizen Lab at the University of Toronto's Munk School of Global Affairs and Public Policy

Copy to:
Jacob J. Sullivan, National Security Advisor, The White House