JAMES COMER, KENTUCKY
CHAIRMAN

ONE HUNDRED NINETEENTH CONGRESS

ROBERT GARCIA, CALIFORNIA
RANKING MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143
MAJORITY (202) 225–5074
MINORITY (202) 225–5051
https://oversight.house.gov

May 6, 2026

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

Dear Secretary Lutnick:

According to the *Wall Street Journal*, an American company recently purchased a controlling stake in the Israeli spyware company NSO Group. NSO Group has long been subject to government sanctions, as governments across the globe have used its spyware technology against political dissidents, human rights advocates, journalists, and even American officials. Yet it seems NSO Group thinks it has now found an ally in the Trump Administration. NSO Group's new executive chairman, David Friedman, has stated that he "expect[s]" the Trump Administration will be "receptive" to considering NSO Group's technologies for government use. Mr. Friedman has close ties to the Trump Administration, as the former U.S. ambassador to Israel and President Trump's former bankruptcy lawyer.[1] Moreover, the Biden Administration previously raised significant concerns with NSO Group and any acquisition of the company by an American entity, warning that such a purchase would present "serious counterintelligence and security concerns for the US government."[2] Given these close ties between NSO Group and the Trump Administration, and the serious concerns about how NSO's technology could be used to spy on American citizens, we write to request information regarding the purchase of NSO Group by an American company and the potential usage of NSO Group spyware by federal law enforcement.

In November 2021, the Department of Commerce's Bureau of Industry and Security (BIS) placed NSO Group on the "Entity List for Malicious Cyber Activities" (Entity List) comprised of people and organizations "reasonably believed to be involved, have been involved, or pose a significant risk of being or becoming involved, in activities contrary to the national

---

[1] *Israeli Spyware Maker NSO Gets New Owners, Leadership and Seeks to Mend Reputation*, Wall Street Journal (Nov. 9, 2025) (online at www.wsj.com/tech/israeli-spyware-maker-nso-gets-new-owners-leadership-and-seeks-to-mend-reputation-166ac50e).

[2] *Id.*; *US Defence Firm Ends Talks to Buy NSO Group's Surveillance Technology*, The Guardian (July 10, 2022) (online www.theguardian.com/us-news/2022/jul/10/us-defence-firm-ends-talks-to-buy-nso-groups-surveillance-technology).

security or foreign policy interests of the United States."[3] NSO Group was placed on the Entity List "based on evidence that [it] developed and supplied spyware to foreign governments that used these tools to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers."[4]

Recognizing the insidious nature of spyware platforms and technology's potential to spy on citizens and civil society groups, the Biden Administration issued an executive order in 2023 prohibiting the federal government—including law enforcement—from using commercial spyware that poses a risk to national security or has been used to enable human rights abuses by foreign actors. The executive order highlighted BIS's placement of foreign entities on the Entity List due to "engaging in the proliferation and misuse of cyber intrusion tools."[5] That same year, the White House issued warnings to any firm that sought to do business with NSO Group that such an action would trigger a counterintelligence review.[6] In February 2024, out of continued concern about the dangers of commercial spyware, the State Department announced that "the misuse of commercial spyware threatens privacy and freedoms of expression, peaceful assembly, and association."[7]

The restrictions that the Biden Administration placed on those misusing spyware, including NSO Group, sought to highlight and elevate awareness of spyware as a dangerous tool of repression and invasion of privacy. For example, NSO Group's Pegasus software has relied on "zero-click exploits," through which a Pegasus user can gain full access to a target's phone simply by sending a message to a target's phone; the target does not even need to interact with the message for the software to gain access.[8] Security researchers and civil society groups have found NSO Group spyware on devices belonging to dozens of reporters, including a journalist who wrote a book about Saudi Arabian Crown Prince Mohammed bin Salman, Amnesty International staff members, and imprisoned activists.[9] The Citizen Lab at the University of

---

[3] U.S. Department of Commerce, Bureau of Industry and Security, *Press Release: Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities* (Nov. 4, 2021) (online at www.bis.gov/press-release/commerce-adds-nso-group-other-foreign-companies-entity-list-malicious-cyber-activities)

[4] *Id*.

[5] The White House, *FACT SHEET: President Biden Signs Executive Order to Prohibit U.S. Government Use of Commercial Spyware that Poses Risks to National Security* (Mar. 27, 2023) (online at https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/03/27/fact-sheet-president-biden-signs-executive-order-to-prohibit-u-s-government-use-of-commercial-spyware-that-poses-risks-to-national-security/).

[6] *White House Issues Warning to US Firms Interested in Acquiring Israeli Surveillance Tech*, The Guardian (June 29, 2023) (online at www.theguardian.com/us-news/2023/jun/29/israel-nso-surveillance-spyware-pegasus-simonds-biden-national-security).

[7] U.S. Department of State, *Announcement of a Visa Restriction Policy to Promote Accountability for the Misuse of Commercial Spyware* (Feb. 5, 2024) (online at https://2021-2025.state.gov/announcement-of-a-visa-restriction-policy-to-promote-accountability-for-the-misuse-of-commercial-spyware/).

[8] *Triple Threat: NSO Group's Pegasus Spyware Returns in 2022 with a Trio of iOS 15 and iOS 16 Zero-Click Exploit Chains*, Citizen Lab (Apr. 18, 2023) (online at https://citizenlab.ca/2023/04/nso-groups-pegasus-spyware-returns-in-2022/).

[9] *"Cat and Mouse Game": How Citizen Lab Shone a Spotlight on Israeli Spyware Firm*, The Guardian

Toronto has tracked infection of NSO Group's Pegasus software to conflicts in Armenia and Azerbaijan and abuses in Mexico, as well as spying on pro-democracy advocates in Thailand, human rights groups in Jordan, and civil society groups in El Salvador, among others.[10] A separate analysis found that NSO Group customers may have targeted approximately 50,000 people around the globe including activists and heads of state.[11]

Despite the clear dangers of NSO Group's spyware and the many ways that the U.S. government has restricted the use of its technology, NSO Group has not given up on making money from the United States—including continuing to seek contracts with the U.S. government. After its Entity List designation, NSO Group experienced a "financial freefall" and nearly defaulted on an outstanding $500 million debt.[12] When the Hamas terrorist attack occurred in Israel on October 7, 2023, NSO Group took it as an opportunity and volunteered to assist Israel's security services in tracking people who were kidnapped as part of Hamas's attack. That same year, in an apparent attempt to rehabilitate its image, NSO Group engaged multiple public relations and law firms and reportedly spent nearly $1 million on lobbying.[13] In the words of the NSO Group executive chairman, the acquisition came at a time when NSO Group had "been struggling and looking for capital" and this deal "brings with it sufficient capital to maintain the business," allowing it to continue to sell spyware.[14]

The Trump Administration appears to be broadly receptive to using commercial spyware to infiltrate cell phones and allowing U.S. investment in sanctioned spyware companies like NSO Group. In a previous letter, we requested information regarding the Department of Homeland Security's (DHS) decision to reactivate a contract with a spyware company that operates a product similar to NSO's Pegasus, through which users can gain access to phones remotely and without the phone owner's knowledge or approval.[15] In response to that letter, DHS confirmed that they believed that it could use this technology as it did "not pose significant security or counterintelligence risks, or significant risks of improper use by a foreign government or foreign person."[16] DHS did not provide any of the information requested by Committee

---

(May 12, 2020) (online at www.theguardian.com/world/2020/may/12/cat-and-mouse-game-how-citizen-lab-shone-a-spotlight-on-israeli-spyware-firm-nso).

[10] Citizen Lab, *NSO Group* (online at https://citizenlab.ca/tag/nso-group/) (accessed Nov. 26, 2025).

[11] *Notorious Spyware Maker NSO Group Is Quietly Plotting a Comeback*, Wired (Jan. 24, 2024) (online at www.wired.com/story/nso-group-lobbying-israel-hamas-war/).

[12] *Id*.

[13] *Id*.

[14] *Israeli Spyware Maker NSO Gets New Owners, Leadership and Seeks to Mend Reputation*, Wall Street Journal (Nov. 9, 2025) (online at www.wsj.com/tech/israeli-spyware-maker-nso-gets-new-owners-leadership-and-seeks-to-mend-reputation-166ac50e)

[15] Letter from Ranking Member Summer Lee, Subcommittee on Federal Law Enforcement, Ranking Member Shontel Brown, Subcommittee on Cybersecurity, Information Technology, and Government Innovation, Committee on Oversight and Reform, and Congresswoman Yassamin Ansari to Secretary Kristi Noem, Department of Homeland Security (Oct. 6, 2025) (online at https://drive.google.com/file/d/1hepcrk651kcQaTzGvJJSouPjbizr5e_g/view).

[16] Letter from Senior Official Performing the Duties of the Director Todd M. Lyons, Immigration and Customs Enforcement, to Ranking Member Summer L. Lee, Committee on Oversight and Government Reform,

Democrats and dismissed our serious concerns about how this technology can be used for counterintelligence and to attack civil liberties.

NSO Group also appears to view the Trump Administration as friendly to its interests in the United States, pitching itself as a vital tool for the U.S. government to safeguard national security. In recent court filings, NSO Group claimed that "[i]t is reasonably foreseeable that a law enforcement or intelligence agency of the United States will use Pegasus," arguing also that an injunction limiting the use of Pegasus software could hinder government operations in a time of "crisis."[17]

As a result of this deeply troubling fact pattern, I ask that you provide a briefing for Committee staff regarding the following questions by May 20, 2026:

1. Any deliberations, discussions, or communications regarding NSO Group or NSO Group technologies at the Department of Commerce, including, but not limited to, potential U.S. government use of NSO Group technologies or other commercial spyware, and the purchase of NSO Group by an American company;

2. Any communications with the White House regarding NSO Group, NSO Group technologies, or the employment of commercial spyware, including, but not limited to, potential U.S. government use of NSO Group technologies or other commercial spyware, and the purchase of NSO Group by an American company; and

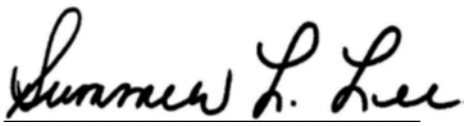
3. Any meetings, communications, or documents with outside organizations or individuals, including, but not limited to, David Friedman, regarding NSO Group, NSO Group technologies, potential U.S. government use of NSO Group technologies or other commercial spyware, and the purchase of NSO Group by an American company.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at "any time" under House Rule X. If you have any questions about this request, please contact Committee Democratic staff at (202) 225-5051. Thank you for your prompt attention to this request.

Subcommittee on Federal Law Enforcement (Apr. 1, 2026) (online at https://drive.google.com/file/d/1KXpgCBxk519hLKvJMIhHJ0cfziMlHQ0R/view).

[17] Defendants' Response and Objection to Plaintiffs' Second Proposed Order Granting Motion for Permanent Injunction and Request for Administrative Stay and for Briefing Schedule for Motion to Stay, WhatsApp Inc. and Facebook, Inc. v. NSO Group Technologies Limited and Q Cyber Technologies Limited (Nov. 4, 2025) Case No. 4:19-cv-07123-PJH (online at https://storage.courtlistener.com/recap/gov.uscourts.cand.350613/gov.uscourts.cand.350613.805.0.pdf).

Sincerely,



Summer L. Lee
Ranking Member
Subcommittee on Federal Law Enforcement

cc: The Honorable James Comer, Chairman

The Honorable Clay Higgins, Chairman
Subcommittee on Federal Law Enforcement