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

October 6, 2025

The Honorable Kristi Noem
Secretary
Department of Homeland Security
2707 Martin Luther King Jr. Avenue, SE
Washington, DC 20528

Dear Secretary Noem:

We write with deep concern regarding reports that Immigrations and Customs Enforcement (ICE) has activated a contract with the foreign spyware company Paragon Solutions, which operates a spyware software called Graphite. Graphite can gain unauthorized access into mobile phones without the owner's knowledge or consent, allowing access to encrypted applications, the phone's location data, as well as messages and photographs saved to the phone.[1] Given the Trump Administration's disregard for constitutional rights and civil liberties in pursuit of rapid mass deportation, we are seriously concerned that ICE will abuse Graphite software to target immigrants, people of color, and individuals who express opposition to ICE's repeated attacks on the rule of law.

While Paragon claims it has more safeguards in place to protect civil liberties and privacy than its competitor Pegasus, which has been used to spy on French President Emmanuel Macron, Saudi journalist and U.S. resident Jamal Khashoggi, as well as other prominent activists and academics,[2] the Graphite product still gives the purchaser "access to the instant messaging applications" on a target's phone, including through the use of a "zero-click" exploit where something as simple as receiving a message on a platform like WhatsApp allows their phone to become infected.[3] In March 2025, WhatsApp informed 90 users in Europe—including

---

[1] *Ice Obtains Access to Israeli-Made Spyware That Can Hack Phones and Encrypted Apps*, The Guardian (Sept. 2, 2025) (online at www.theguardian.com/us-news/2025/sep/02/trump-immigration-ice-israeli-spyware). The Biden Administration had paused this contract with Paragon, pending a compliance review to ensure that that the contract did not violate an executive order requiring that the United States "not make operational use of commercial spyware that poses significant counterintelligence or security risks to the United States Government or significant risks of improper use by a foreign government or foreign person." *Id*; Executive Order 14093 "Prohibition on Use by the United States of Commercial Spyware that Poses Risks to National Security" (Mar. 27, 2023) (online at www.presidency.ucsb.edu/documents/executive-order-14093-prohibition-use-the-united-states-government-commercial-spyware-that).

[2] Electronic Privacy Information Center, *When Courts Reach The Merits, Spyware Loses* (May 8, 2025) (online at https://epic.org/when-courts-reach-the-merits-spyware-loses/).

[3] Citizen Lab, *Virtue or Vice? A First Look at Paragon's Proliferating Spyware Operations* (Mar. 19, 2025) (online at https://citizenlab.ca/2025/03/a-first-look-at-paragons-proliferating-spyware-operations/).

journalists and human rights activists—that they had been targeted by Paragon spyware.[4] Freedom House, which tracks democracy and human rights around the world, found that 49 countries have employed sophisticated spyware and data extraction software to spy on their own citizens—including journalists and human rights groups. The proliferation of commercial surveillance software deployed to consumer devices threatens human rights, privacy, and national security.[5]

Allowing ICE access to spyware that can be used to easily track and monitor the public—including those vocally opposed to governmental overreach— threatens Americans' freedom of movement and freedom of speech. In 2014, the Supreme Court ruled in *Riley v. California* that warrantless search of a cellphone would amount to an unreasonable invasion of privacy due to the incredible amounts of data available.[6] In the 2018 Supreme Court decision *Carpenter v. United States*, the Court ruled that law enforcement must have a warrant to obtain location data gathered from cell phone towers, because even though that data is held by a person's phone carrier, individuals have a reasonable expectation of privacy in their movements over a weeks-long period of time.[7] Allowing ICE to utilize spyware raises serious questions about whether ICE will respect Fourth Amendment protections against warrantless search and seizure for people residing in the U.S.

Given the constitutional, national security, and civil liberty concerns, if ICE were to begin using spyware to track and steal information from individuals residing in the U.S., we request that you provide answers to the following questions and all requested documents to staff by October 20, 2025:

1. All communications and documents discussing ICE's use of spyware, including but not limited to Paragon Solutions software like Graphite;

2. All communications and documents regarding the legality of and legal justification for using spyware or mass electronic surveillance for immigration enforcement;

3. A comprehensive list of data surveillance targets and ICE's strategy for deploying spyware or mass data surveillance within the United States; and

---

[4] Amnesty International, *Europe: Paragon Attacks Highlight Europe's Growing Spyware Crisis* (Mar. 19, 2025) (online at www.amnesty.org/en/latest/news/2025/03/europe-paragon-attacks-highlight-europes-growing-spyware-crisis/).

[5] Freedom House, *How Stronger Export Controls Can Better Protect Human Rights* (Feb. 8, 2024) (online at https://freedomhouse.org/article/how-stronger-export-controls-can-better-protect-human-rights).

[6] Electronic Privacy Information Center, *Fourth Amendment* (https://epic.org/issues/privacy-laws/fourth-amendment/) (accessed Sept. 19, 2025).

[7] Brennan Center for Justice, *The Fourth Amendment in the Digital Age* (Mar. 18, 2021) (online at www.brennancenter.org/our-work/policy-solutions/fourth-amendment-digital-age).

4. All communications and documents regarding the legality of using spyware against individuals residing within the United States given Executive Order 14093.

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.

Sincerely,

Summer L. Lee
Ranking Member
Subcommittee on Federal Law Enforcement

Shontel M. Brown
Ranking Member
Subcommittee on Cybersecurity, Information Technology, and Government Innovation

Yassamin Ansari
Member of Congress

cc: The Honorable James Comer, Chairman

The Honorable Clay Higgins, Chairman
Subcommittee on Federal Law Enforcement

The Honorable Nancy Mace, Chairwoman
Subcommittee on Cybersecurity, Information Technology, and Government Innovation