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

February 19, 2026

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

Dear Secretary Noem:

We write as members of Congress concerned about recent reports that U.S. Immigration and Customs Enforcement (ICE) has acquired surveillance tools from Penlink designed to collect and analyze cellphone location data across entire neighborhoods.[1] Mass surveillance of entire communities or city blocks raises serious questions about data privacy and potential violations of civil liberties.

Penlink reportedly collects cellphone location data and allows users to search this data to understand which cellphones were in certain locations at certain times and what other locations those cellphone users have visited.[2] Location data can reveal intimate details of a person's life, including where they live, work, worship, go to school, or seek medical care. DHS could use these tools to identify individuals for targeting based solely on their presence in certain locations, without a warrant or probable cause, and regardless of their citizenship or residency status. The indiscriminate collection of such data poses significant risks to privacy and civil liberties, particularly as federal agents reportedly identify and track individuals who observe the actions of Immigration and Customs Enforcement (ICE).[3] As the ACLU recently declared, "This is a very dangerous tool in the hands of an out-of-control agency."[4]

DHS's acquisition of Penlink's surveillance technology comes shortly after DHS awarded a contract to the foreign spyware company Paragon, which operates a software that can reportedly gain full access to all information on a mobile device without the device owner's

[1] *Inside ICE's Tool to Monitor Phones in Entire Neighborhoods*, 404 Media (Jan. 8, 2026) (online at www.404media.co/inside-ices-tool-to-monitor-phones-in-entire-neighborhoods/).

[2] *Id*.

[3] *See, e.g.*, *Privacy Advocates: ICE Using Private Data to Intimidate Observers and Activists*, MPR News (Jan. 13, 2026) (online at www.mprnews.org/story/2026/01/13/ice-using-private-data-to-intimidate-observers-and-activists-advocates-say).

[4] *Security News This Week: ICE Can Now Spy on Every Phone in Your Neighborhood*, Wired (Jan. 10, 2026) (online at www.wired.com/story/security-news-this-week-ice-can-now-spy-on-every-phone-in-your-neighborhood/).

knowledge or consent. Using this technology, DHS can potentially access encrypted applications, the phone's location data, and messages and photographs saved to the phone.[5] The continued acquisition of such spyware technology suggests DHS is relying on mass data-collection techniques that the Department can use without cell phone users' knowledge and that may operate outside of constitutional guardrails.

Americans should be able to trust their government to uphold the Constitution and respect fundamental rights. Instead, DHS appears to be engaging in broad surveillance practices to monitor entire communities, violating Americans' fundamental civil rights and civil liberties to punish dissent and advance the President's cruel and unconstitutional mass deportation agenda.

Given these profound implications, I ask that you provide a briefing for committee staff on the following topics by March 5th, 2026:

1. Internal DHS communications and messaging regarding DHS acquisition of location-based electronics surveillance, including Penlink and other technologies that monitor electronic devices via location data;

2. Any legal justification DHS has identified that would justify mass electronic surveillance of individuals without a judicial or administrative warrant;

3. How DHS intends to store, use, and dispose of data collected through the Penlink system; and

4. Who will be granted access to data collected using Penlink technologies, the processes for granting access, and the process for monitoring for any abuses of such access.

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,

---

[5] 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 Government Reform, and Congresswoman Yassamin Ansari to Secretary Kristi Noem, Department of Homeland Security (Oct. 6, 2025) (online at https://oversightdemocrats.house.gov/imo/media/doc/2025-10-06.lee-brown-ansari-to-dhs-re-spyware.pdf).

Shontel M. Brown
Member of Congress

Eleanor Holmes Norton
Member of Congress

Stephen F. Lynch
Member of Congress

Raja Krishnamoorthi
Member of Congress

Ro Khanna
Member of Congress

Greg Casar
Member of Congress

Jasmine Crockett
Member of Congress

Emily Randall
Member of Congress

Yassamin Ansari
Member of Congress

Lateefah Simon
Member of Congress

Dave Min
Member of Congress

James R. Walkinshaw
Member of Congress

Rashida Tlaib
Member of Congress

cc: The Honorable James Comer, Chairman