ANDREW R. GARBARINO, NEW YORK
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

One Hundred Nineteenth Congress
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

February 27, 2026

The Honorable Kristi Noem
Secretary
U.S. Department of Homeland Security
Washington, D.C. 20528

Dear Secretary Noem:

We write to demand details on how the Department of Homeland Security (DHS or Department) is using dragnet surveillance tools to spy on and target the American populace.

At your direction, DHS has established new programs and watchlists to collect, store, share, and utilize data on U.S. citizens and non-citizens alike, without notice to Congress or the public. We are deeply concerned DHS is using these surveillance programs to monitor and investigate Americans and stifle dissent among those who oppose the Trump administration's agenda. You and your underlings appear to be labeling untold numbers of people as "domestic terrorists" or individuals of concern at will without evidence, operating wildly invasive spy tools to identify targets—and then using such labels as an excuse for yet more surveillance. This self-reinforcing spiral of civil liberties violations ratchets in only one direction: toward an authoritarian surveillance state that punishes dissent and inflicts state violence.

The following is a non-exhaustive list of surveillance, data collection, and watchlisting activities DHS and its component agencies have reportedly undertaken since you entered office:

- DHS shared a memo with employees operating in Minneapolis, directing them to "capture all images, license plates, identifications, and general information on hotels, agitators, protestors, etc., so we can capture it all in one consolidated form."[1]

- Immigration and Customs Enforcement (ICE) tasked Palantir with developing an expansive tool "that populates a map with potential deportation targets, brings up a dossier on each person, and provides a 'confidence score' on the person's current address."[2]

---

[1] Jeff Winter & Priscilla Alvarez, *Alex Pretti Broke Rib in Confrontation with Federal Agents a Week Before Death, Sources Say*, CNN (Jan. 27, 2026), https://www.cnn.com/2026/01/27/us/alex-pretti-protesters-minneapolis-invs.
[2] Joseph Cox, *'ELITE': The Palantir App ICE Uses to Find Neighborhoods to Raid*, 404 MEDIA (Jan. 15, 2026), https://www.404media.co/elite-the-palantir-app-ice-uses-to-find-neighborhoods-to-raid/.

- ICE purchased mobile license plate readers, cellphone location tracking devices, and access to private databases of license plate scans, surveillance video feeds, and cellphone location histories.[3]

- ICE signed contracts with spyware and forensic technology companies to allow the agency to hack into phones remotely, access locked phones, recover deleted data, and read information in encrypted chats.[4]

- DHS subpoenaed data from social media companies about individuals critical of ICE.[5]

- DHS authorized employees to engage in online "masked engagement," allowing a previously banned form of undercover operations that uses false digital identities to collect intelligence and target internet users.[6]

- DHS purchased drones, equipped them with unknown surveillance technologies, and in at least one instance, flew a military-grade Predator drone over anti-ICE protests.[7]

- ICE agents told protesters and observers they were identifying them with facial recognition technology[8] which was deployed while still in beta testing, raising concerns about its accuracy.[9]

- DHS collected protesters' personally identifiable information—including photos, addresses, and social security and passport numbers—and added such information into databases.[10]

- DHS ordered immigration officers to gather identifying information about anyone filming them and to "send that information to Intel who will do a 'work-up' on them…meaning, trying to identify them via social media, running their license plates if available, and running a criminal history check"; one agent in Portland, Maine, was captured on video taking pictures of a car belonging to a woman who had been recording him, telling her it was "because we have a nice little database, and now you're considered a domestic terrorist."[11]

---

[3] Eva Dou, et al., *The Powerful Tools in ICE's Arsenal to Track Suspects—and Protesters*, WASHINGTON POST (Jan. 29, 2026), https://www.washingtonpost.com/technology/interactive/2026/ice-surveillance-immigrants-protesters/.
[4] *Id*.
[5] Sheera Frenkel & Mike Isaac, *Homeland Security Wants Social Media Sites to Expose Anti-ICE Accounts,* N.Y. TIMES (Feb. 13, 2026), https://www.nytimes.com/2026/02/13/technology/dhs-anti-ice-social-media.html.
[6] Ken Klippenstein, *Exclusive: ICE Masks Up in More Ways Than One*, KEN KLIPPENSTEIN (Feb. 12, 2026), https://www.kenklippenstein.com/p/exclusive-ice-masks-up-in-more-ways.
[7] Dou, *supra* note 5.
[8] Sheera Frenkel & Aaron Krolik, *How ICE Already Knows Who Minneapolis Protesters Are*, N.Y. TIMES (Jan. 30, 2026), https://www.nytimes.com/2026/01/30/technology/tech-ice-facial-recognition-palantir.html.
[9] *Ranking Member Thompson Introduces Legislation to Curb Unchecked DHS Mobile Biometric Surveillance and Protect Privacy of American Citizens*, COMMITTEE ON HOMELAND SECURITY PRESS RELEASE (Jan. 15, 2026), https://democrats-homeland.house.gov/news/legislation/ranking-member-thompson-introduces-legislation-to-curb-unchecked-dhs-mobile-biometric-surveillance-and-protect-privacy-of-american-citizens
[10] Ken Klippenstein, *Feds Identify "Leader of Antifa"*, KEN KLIPPENSTEIN (Feb. 2, 2026), https://www.kenklippenstein.com/p/feds-identify-leader-of-antifa.

- You labeled Renée Good and Alex Pretti as "domestic terrorists" without any evidence—bold-faced lies clearly intended to sanction state violence toward protesters and raising questions on how DHS is otherwise identifying, surveilling, or watchlisting supposed "domestic terrorists."[12]

- ICE purchased aviation industry data on airline passengers, including "full flight itineraries, passenger name records, and financial details."[13]

- The Transportation Security Administration (TSA) began checking domestic commercial flight passenger information on ICE's behalf to flag individuals who may be the subjects of deportation orders and sharing the results with ICE to facilitate deportations.[14]

- DHS provided unvetted and unqualified employees of the so-called Department of Government Efficiency (DOGE) with unrestricted access to Cybersecurity and Infrastructure Security Agency (CISA) and Federal Emergency Management Agency (FEMA) systems which house sensitive data, including the personal information of disaster aid recipients.[15]

DHS's dragnet effort to weaponize surveillance tools against the American people was enabled by Republicans' One Big Ugly Bill, which provided ICE and Customs and Border Protection (CBP) with combined funding exceeding the budget of most countries' militaries, while neglecting to establish any meaningful safeguards. The negative consequences of this blank check have been exacerbated by your dismantling of internal DHS oversight mechanisms, including the Office for Civil Rights and Civil Liberties.[16]

The Department's opaque, mass expansion of spy tools and framing of protesters, photographers, political opponents, and passersby as enemies of the state leans into people's worst fears of a surveillance state. Your weaponization of DHS undercuts decades of effort to develop a Department that responsibly balances security with privacy and civil liberties protections and transparency.

---

[11] Ken Klippenstein, *ICE Making List of Anyone Who Films Them*, KEN KLIPPENSTEIN (Jan. 23, 2026), https://www.kenklippenstein.com/p/ice-making-list-of-anyone-who-films.

[12] Jude Joffe-Block, et al., *DHS Keeps Making False Claims About People. It's Part of a Broader Pattern*, NPR (Jan. 31, 2026), https://www.npr.org/2026/01/31/nx-s1-5690124/ice-alex-pretti-immigration-unproven-claims-dhs-enforcement-arrests.

[13] Katya Schwenk, *Airlines Are Collecting Your Data and Selling It to ICE*, THE LEVER (May 8, 2025), https://www.levernews.com/airlines-are-collecting-your-data-and-selling-it-to-ice/.

[14] Hamed Aleaziz, *Immigration Agents Are Using Air Passenger Data for Deportation Effort*, N.Y. TIMES (Dec. 12, 2025), https://www.nytimes.com/2025/12/12/us/politics/immigration-tsa-passenger-data.html.

[15] Aileen Graef & Veronica Stracqualursi, *Homeland Security Secretary Noem Says DOGE Team Has Access to Agency Data*, CNN (Feb. 9, 2025), https://www.cnn.com/2025/02/09/politics/noem-homeland-security-doge-musk-cnntv/index.html.

[16] José Olivares, *Gutting of Key US Watchdog Could Pave Way for Grave Immigration Abuses, Experts Warn*, THE GUARDIAN (Nov. 30, 2025), https://www.theguardian.com/us-news/2025/nov/30/us-watchdog-human-rights-department-homeland-security.

Your actions are abhorrent, blatantly unconstitutional, and corrosive to the functioning of a peaceful society. They cannot stand. Accountability is coming. As such, we demand the following information no later than March 13, 2026:

1. A copy of all DHS policies and directives pertaining to data collection, storage, retention, security, sharing, use, deletion, and destruction, including the use of surveillance and intelligence collection technologies.

2. A description and documentation of each DHS program involving surveillance or data collection, storage, retention, sharing, use, deletion, or destruction. For each program, provide the following:
    a. A description of what data is being collected and the standards for its collection, storage, retention, security, sharing, use, deletion, and destruction.
    b. A description and documentation of the standards for determining the entities and individuals subject to having their data collected.
    c. A description of costs incurred since January 20, 2025.
    d. A copy of all relevant Privacy Threshold Analyses (PTAs), privacy impact assessments (PIAs), and System of Record Notices (SORNs).

3. A description of each watchlist or database of biographic and biometric information of individuals—regardless of the nomenclature DHS uses to refer to it internally (system, list, record, file, etc.)—maintained, accessed, or used by DHS and its components. For each watchlist or database, provide the following:
    a. A description and copy of policies and directives pertaining to standards and protocols for the nomination and confirmation of the placement of individuals on the watchlist or in the database.
    b. A description and copy of policies and directives for notifying individuals of placement on the watchlist or in the database and allowing for redress.
    c. The date of origination and purpose for each watchlist or database.
    d. The current number of U.S. citizens and non-citizens in each watchlist or database.

4. Documentation of the Department's definition of the term "domestic terrorist," a copy of the policies in place that permit Departmental designations of United States persons as a "domestic terrorist," and a description of the consequences of such a designation.

5. Documentation of the Department's definition of "Antifa," a copy of the policies in place for designating an individual as a member of Antifa, and a description of the consequences of such a designation.

6. A copy of all DHS policies and directives pertaining to collecting, storing, retaining, securing, sharing, using, deleting, and destroying data pertaining to individuals deemed to be domestic terrorists, members of Antifa, protesters, agitators, political opponents, journalists, photographers, or people in the vicinity of immigration enforcement activities.

7. A description and documentation of TSA's activities to check passenger data for immigration enforcement purposes and all data shared with ICE or CBP, including a description of TSA's legal authorities to conduct such activities.

8. A description and documentation of how TSA has complied with each statutory requirement related to the vetting of passenger data, including requirements to carry out the following:
    a. "Establish an internal oversight board to oversee and monitor the manner in which the system is being implemented;
    b. "Establish sufficient operational safeguards to reduce the opportunities for abuse;
    c. "Implement substantial security measures to protect the system from unauthorized access;
    d. "Adopt policies establishing effective oversight of the use and operation of the system; and
    e. "Ensure that there are no specific privacy concerns with the technological architecture of the system."[17]

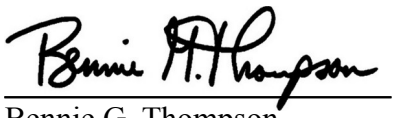
9. A description and documentation of each DHS or component program involving the sharing of data within or outside DHS to aid immigration enforcement.

10. A description and documentation of DOGE's access to DHS systems and DHS data supplied to DOGE, including the following:
    a. A description and documentation of each DHS system accessed by DOGE, including a description of the data held within each system.
    b. A description and documentation of all data shared by DHS to DOGE, or exfiltrated from DHS systems by DOGE, including a description of who exfiltrated such data and each recipient of such data.
    c. A description of measures taken to secure any DHS data exfiltrated by DOGE.
    d. Information on each DOGE worker who has accessed DHS systems or data, including the following:
        i. Full name.
        ii. Current employment status.
        iii. Dates of government employment.
        iv. Title(s) and description of role(s) while employed by the government.
        v. Dates and description of outside employment since January 20, 2025.
        vi. Any financial disclosure filed with the government.
        vii. A description of vetting conducted on such worker prior to their access to any DHS system.
        viii. Their level of security clearance, if any, and the date upon which such clearance was granted.
        ix. A description of each DHS system such worker accessed and activities conducted within such system.
        x. A description of user access and permissions for each system.

[17] 49 U.S.C. §44903(j)(2)(C)(iii)(III)-(VII).

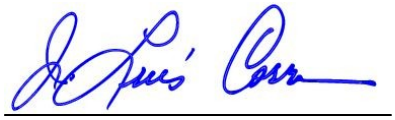
Responses to these requests should be provided in an unclassified format to the greatest extent possible but may be supplemented by a classified addendum.

Sincerely,



Bennie G. Thompson
Ranking Member

Eric Swalwell
Member of Congress



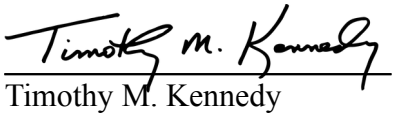
J. Luis Correa
Member of Congress

Shri Thanedar
Member of Congress

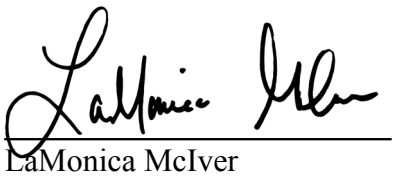
Seth Magaziner
Member of Congress

Dan Goldman
Member of Congress

Delia C. Ramirez
Member of Congress



Timothy M. Kennedy
Member of Congress



LaMonica McIver
Member of Congress

Julie Johnson
Member of Congress

Pablo José Hernández
Member of Congress

Nellie Pou
Member of Congress

James R. Walkinshaw
Member of Congress

Troy A. Carter, Sr.
Member of Congress

Al Green
Member of Congress

cc: The Honorable Andrew R. Garbarino, Chairman, Committee on Homeland Security