

# United States Senate

May 14, 2026

The Honorable Markwayne Mullin  
Secretary  
U.S. Department of Homeland Security  
2707 Martin Luther King Jr. Ave, S.E.  
Washington, DC 20528

Dear Secretary Mullin,

The Department of Homeland Security's (DHS) 2027 budget proposal to develop "smart glasses" for biometric identification presents a grave threat to the privacy and civil rights of people across the United States. DHS's proposed smart glasses could allow its agents to identify individuals, including U.S. citizens, in real time by covertly collecting their biometric information — for example, through a facial scan — without their knowledge or consent. Given the Trump Administration's record of abusing surveillance technologies, DHS would be able to weaponize smart glasses and turn them into an authoritarian tool against anyone who speaks out against President Trump. DHS should immediately abandon any plans it has to develop this technology.

The Trump administration's proposal to develop smart glasses represents a chilling expansion of its surveillance state. According to DHS's own budget documents, the Department seeks \$7.5 million to develop new technologies and analytics tools for U.S. Immigration and Customs Enforcement (ICE) and U.S. Customs and Border Protection (CBP), including smart glasses to "equip agents with real-time access to information and biometric identification capabilities in the field."<sup>1</sup> Smart glasses are designed to be indistinguishable from regular glasses but include small cameras, which would enable ICE and CBP officers to capture thousands of images of faces each day — without the subjects' knowledge or consent — and identify them with biometric recognition technology. Furthermore, there is no guarantee that data collected would only be used for immigration enforcement. In essence, DHS wants to provide its officers with a tool to quickly and covertly identify members of the public, a breathtaking expansion of its technological capacity to surveil the American people.

The dangers here are obvious. This technology can easily be co-opted to support the wrongful arrest, detainment, and deportation of U.S. citizens or other lawful residents and immigrants, as the Department has already done since the start of the second Trump administration.<sup>2</sup> An ICE officer could use smart glasses to identify and later target peaceful

---

<sup>1</sup> Science and Technology Directorate Budget Overview, Fiscal Year 2027, Department of Homeland Security, [https://www.dhs.gov/sites/default/files/2026-04/26\\_0403\\_ocfo\\_fy27-budget-science-and-technology-directorate.pdf](https://www.dhs.gov/sites/default/files/2026-04/26_0403_ocfo_fy27-budget-science-and-technology-directorate.pdf).

<sup>2</sup> Nicole Foy, *We Found That More Than 170 U.S. Citizens Have Been Held by Immigration Agents. They've Been Kicked, Dragged and Detained for Days.*, ProPublica (Oct. 16, 2025), <https://www.propublica.org/article/immigration-dhs-american-citizens-arrested-detained-against-will>; María Luisa Paúl, *As Trump cracks down on immigration, U.S. citizens are among those snared*, The Washington Post (Apr. 5, 2025), <https://www.washingtonpost.com/immigration/2025/04/05/us-citizens-deported-immigration/>.

protesters, even exploiting that information to create a database of President Trump's political opponents. A CBP officer wearing smart glasses in the field could covertly scan thousands of faces a day, cross referencing them against social media and government databases to flag journalists, activists or critics for detention. Meanwhile, immigration enforcement officers continue to use face coverings to avoid being identified in public, underscoring the irony of agents' desire for privacy while simultaneously using privacy invasive technology. Such frictionless, real-time surveillance is un-American. Every person in the United States has the right to move through daily life without fear that the federal government is tracking, scanning, and cataloging their every step.

Given DHS's record during the Trump administration of exploiting surveillance technologies, we are deeply concerned that smart glasses will be abused by this administration. Over the past year, DHS has deployed biometric identification tools — including facial recognition technologies — to identify individuals engaged in protest activity, intimidate them, and deter lawful dissent. For example, in Portland, Maine, an ICE officer recorded a protester on video and told her that her information would go into a so-called “domestic terrorist” database.<sup>3</sup> In a separate incident, an ICE agent, without consent, photographed a Minneapolis woman documenting ICE activity in her neighborhood and then recited her personal information to her, including her address — a clear intimidation tactic.<sup>4</sup> The woman later described being terrified by the encounter. The Trump administration seems to relish these practices, which endanger the core democratic right to challenge the government without fear of punishment. Smart glasses would provide yet another opportunity for DHS to extend its surveillance capabilities and intimidate individuals across the country.

DHS's funding request for smart glasses continues the Administration's unaccountable expansion of its surveillance infrastructure under the banner of national security. Since the start of President Trump's second term, we have repeatedly sounded the alarm on DHS's abuses of its growing arsenal of surveillance tools. We, individually or as a group, have written oversight letters requesting detailed information about ICE's “Mobile Fortify” facial recognition application; CBP's nationwide network of license plate readers; DHS's use of predictive algorithms to identify national security threats; DHS's monitoring of social media information; and DHS's deployment of Predator drones to observe protesters. DHS or its subcomponents have refused to provide a meaningful response to any of these inquiries. The pattern is unmistakable: DHS continues to introduce powerful new surveillance technologies while stonewalling legitimate congressional oversight. That is unacceptable.

Given the serious risk to the privacy and civil liberties of Americans, DHS should abandon its plans to develop and deploy smart glasses. In the meantime, the Department owes the American people answers about its plans to deploy such an invasive and dangerous technology. Please respond to the following questions in writing by June 4, 2026:

---

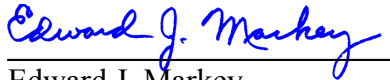
<sup>3</sup> Nathan Bernard (@nathanTbernard), X (Jan. 23, 2026 10:11 AM), <https://x.com/nathanTbernard/status/2014717658323665399>.

<sup>4</sup> Kat Lonsdorf et al., *ICE is using mass surveillance on American citizens, activists*, NPR (Mar. 5, 2026), <https://www.npr.org/2026/03/04/nx-s1-5717031/ice-dhs-immigrants-surveillance-confrontation-deportation-mobile-fortify>.

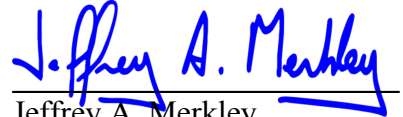
1. Please describe all evaluations DHS has conducted regarding the civil rights and privacy implications of deploying smart-glasses technologies. In your response:
  - a. Identify and describe any assessments of how such technologies would affect the privacy rights of individuals whose images or data may be captured, including bystanders and other non-targets.
  - b. Describe any analysis of whether biometric identification through smart glasses could chill lawful activity protected by the First Amendment.
  - c. State whether DHS has evaluated the risks of misidentification, disparate impact, or other discriminatory outcomes associated with these technologies, and provide any findings.
  - d. Describe any safeguards DHS has considered or adopted to prevent misuse by DHS personnel or contractors.
  - e. Identify any Privacy Threshold Analyses, Privacy Impact Assessments, or third-party audits conducted or commissioned in connection with smart-glasses technologies, and provide copies. If none have been conducted, state whether DHS intends to do so and provide a timeline for completion and public release.
2. Please describe DHS's anticipated practices regarding the collection, use, and retention of biometric data in connection with any deployment of smart glasses. In your response:
  - a. Identify the categories of biometric data that would be collected and the legal authorities supporting such collection.
  - b. Describe how DHS would provide meaningful notice and obtain consent from individuals whose biometric data may be captured, including bystanders and non-targets.
  - c. Specify applicable retention periods and the policies governing data minimization, deletion, and access controls.
  - d. State whether individuals will be able to request deletion of their biometric data and, if so, describe the procedures that will govern such requests and ensure timely and complete compliance.
  - e. Explain how DHS will ensure compliance with applicable state biometric privacy laws, including requirements related to notice, consent, retention, and restrictions on data sharing.
3. Please identify any third parties with which DHS has contracted or otherwise partnered to develop, test, or deploy smart-glasses technologies, and describe the scope and terms of those engagements.

Thank you for your attention to this important matter.

Sincerely,



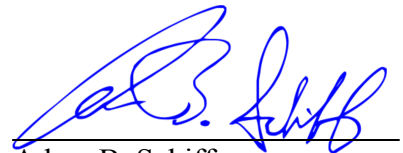
Edward J. Markey  
United States Senator



Jeffrey A. Merkley  
United States Senator



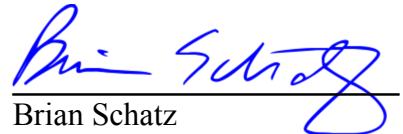
Cory A. Booker  
United States Senator



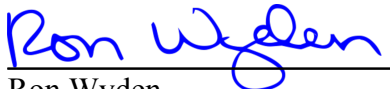
Adam B. Schiff  
United States Senator



Alex Padilla  
United States Senator



Brian Schatz  
United States Senator



Ron Wyden  
United States Senator



Christopher S. Murphy  
United States Senator



Chris Van Hollen  
United States Senator



Richard Blumenthal  
United States Senator