Submitted via email

February 9, 2026

To: Seth D. Renkema,
Branch Chief, Economic Impact Analysis Branch
U.S. Customs and Border Protection
Email: CBP_PRA@cbp.dhs.gov

From: The Cybersecurity Coalition and the Fast Identity Online (FIDO) Alliance

Re: **OMB Control Number 1651-0111**

The Cybersecurity Coalition (the "Coalition") and the FIDO Alliance submit the following comments in response to the Notice on Agency Information Collection Activities; Revision; Arrival and Departure Record (Form I-94) and Electronic System for Travel Authorization (ESTA) (OMB Control Number 1651-0111) (hereinafter "Notice"). *See* 90 FR 57208 (Dec. 10, 2025).

Our comments focus on the proposed collection of five years of social media and multiple other new data elements – including DNA, iris scans, personal and business telephone numbers and emails from the past five years, and extensive details about family members – from travelers that seek to participate in the visa waiver program. These proposed collections raise significant security concerns, have unintended consequences for American technology companies, and risk harming American competitiveness.

We urge that these requirements be removed, or, at a minimum, reevaluated and adjusted to fully account for the significant burden and risks that they create on American companies.

Background

The visa waiver program is a statutorily authorized program, administered by the Department of Homeland Security, that authorizes eligible nationals of specified countries to enter the United States for business and tourism purposes for up to 90 days without a visa. *See* 8 U.S.C. § 1187. American tech companies rely extensively on the visa waiver program to bring in eligible business partners and workers for meetings, trainings, and other business reasons.

There are currently 42 "visa waiver" countries, including most European countries, Australia, Chile, New Zealand, South Korea, and Taiwan. To qualify, countries must, among other things, provide reciprocal travel privileges to American travelers; issue tamper-resistant visa documents that incorporate biometric identifiers; report information about passport loss within 24 hours; accept the repatriation of any citizen, former citizen, or national against whom a final order of removal is issued; and commit to engage in other information-sharing provisions regarding potential threats. *See* 8 U.S.C. §1187(c).

To participate in the program, individuals must obtain advance authorization via Electronic System for Travel Authorization (ESTA), a system that checks the individual's biographic information against relevant law enforcement and security databases before they can board a plane to the United States. Participants must meet certain criteria, including restrictions on past travel to specified countries of concern; use an e-passport with an embedded data chip that includes a biometric identifier (and are harder to alter than other kinds of passports); and are subject to additional screening upon entry at a port of entry. In other words, participation in the visa waiver program does not guarantee admission to the United States; to the contrary, admissibility is determined by Customs and Border Protection officials upon arrival at a port of entry.

Of note, participants in the visa waiver program tend to be more compliant with immigration rules than others – as indicated by their lower overstay rates. In fiscal year 2024, the last year for which such data is available, visa waiver program countries had estimated average overstay rate of 0.43 %, as compared to non-VWP countries overstay rate of 2.2%; in fiscal year 2023 visa waiver program countries had estimated average overstay rate of 0.62%, as compared to non-VWP countries overstay rate of 3.2%.[1]

Proposal

The Notice seeks to make several changes to process and information by which foreigners can become eligible to participate in the foreign waiver program. Our comments focus on two of the proposed changes: (i) the requirement that ESTA applicants provide "their social media from the past 5 years"; and (ii) the inclusion of several new data fields to the ESTA application, to include: biometrics (face, fingerprint, DNA, and iris); business and personal emails and telephone numbers for the past five years; and family member names, dates of birth, places of birth, residences, and telephone numbers for the past five years.

Our organizations fully share the underlying goal of robust screening and vetting to protect against national security and public safety threats. We are concerned, however, that the proposed collections are excessive and overbroad, do not sufficiently account for the significant cybersecurity and related privacy concerns, and will have detrimental effects on American businesses, workforce development programs, and competitiveness.

Cybersecurity Concerns

The proposed new collections include significant amounts of sensitive personal data, without any corresponding accounting for how that data will be stored, secured, or used. Of particular concern, the visa waiver program is a reciprocal program – requiring significant engagement with foreign partners to ensure they meet the specified criteria, to include the granting of

[1] Department of Homeland Security (DHS) *Fiscal Year 2024 Entry/Exit Overstay Report,* https://www.dhs.gov/sites/default/files/2025-09/25_0912_cbp_entry-exit-overstay-report-fiscal-year-2024.pdf; DHS, *Fiscal Year 2023 Entry/Exit Overstay Report,* https://www.dhs.gov/sites/default/files/2024-10/24_1011_CBP-Entry-Exit-Overstay-Report-FY23-Data.pdf.

"reciprocal privileges to citizens and nationals of the United States." *See* 8 U.S.C. §1187(a)(2)(A).

There is a meaningful risk that, were the United States to move forward with the proposed new collections, partner countries would require equivalent reporting by United States citizens as a prerequisite to visa-free business and tourism travel. If adopted broadly, millions of Americans would be required to disclose what has, in the Department of Justice *Rule on Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons,* 90 FR 1636 (Jan. 8, 2025), been defined as "sensitive personal data," and thus subject to a series of restrictions and prohibitions on international transfer, in order to protect against the "unacceptable risk to U.S. national security" that such data might be accessed by foreign countries and persons of concern. *See* id. at 1637; 28 C.F.R. § 202.239 (defining "sensitive personal data"). Of particular concern, there is no guarantee that countries would store such data securely, place appropriate limits on its dissemination, and otherwise protect Americans from the significant surveillance concerns, misuse by cybercriminals for identity theft and other related crimes, and other security risks that could arise.

Moreover, even if foreign countries decline follow suit, the data being sought by the proposed collection will undoubtedly also include Americans' data – including private communications on closed social media accounts, and data about any American family members' phone numbers, residences, and places of birth. This is a treasure trove of information for cyber criminals and foreign adversaries alike. But there is nothing in the proposal that specifies how the United States would secure the sought-after data, protect it from unwarranted intrusion, or otherwise ensure the security and privacy of travelers and their families.

The proposal also does not define "social media" or specify the medium in which such data would need to be provided, leaving significant ambiguity as to the scope of the collection and the types of platforms and communications it would encompass. Nor does the proposal address what recourse would be available to individuals—including American family members whose data is captured—in the event of a data breach or unauthorized disclosure.

Business and Competitiveness Concerns

This proposal is almost certain to have a chilling effect on international business travel, with negative repercussions for an American tech industry that relies on foreign markets, business partners, and workers.

A survey of international travelers from visa waiver countries (Australia, EU, Japan, South Korea, UK) conducted by the World Travel & Tourism Council indicated that over 1/3 of those surveyed would be less likely to visit the U.S. due to this policy change.[2] Those still willing to travel may be unwilling to participate in the visa waiver program – and instead be routed into the more time-consuming and unpredictable process of obtaining a visa.

[2] World Travel & Tourism Council, *Planned U.S. Border Social Media Changes Could Reduce Visitor Spend By USD $15.7 Billion and Impact 157,000 American Jobs, According To New WTTC Research,* Jan. 28, 2026. https://wttc.org/news/planned-u-s-border-social-media-changes-could-reduce-visitor-spend.

This will harm American companies' ability to bring business partners and international workers to the United States for key meetings, roundtables, and trainings. It is also likely to hurt recruitment of top talent in foreign countries – talent that is essential for effective global engagement. And it risks making American tech companies less competitive as a result.

These concerns are heightened for U.S. technology companies that operate across multiple jurisdictions. The proposal also does not address implementation timelines or the status of existing ESTA authorizations during any transition period. Given that companies routinely coordinate international business travel months in advance across multiple jurisdictions, we encourage a phased implementation approach, including sufficient advance notice, with respect to any new collections that are ultimately adopted.

Conclusion

The Coalition and the FIDO Alliance urge CBP to reevaluate this proposal and instead consider more targeted screening and vetting measures that account for the full set of security and business interests at stake.