International Biometrics + Identity Association
1455 Pennsylvania Avenue, NW
Suite 400
Washington, DC 20004

www.ibia.org

Robert A. Tappan
Executive Director

October 7, 2026

The Honorable Rick Crawford
Chairman
House Permanent Select Committee on Intelligence
U.S. House of Representatives HVC-304
Washington, D.C. 20515-6415

The Honorable Jim Himes
Ranking Member
House Permanent Select Committee on Intelligence
U.S. House of Representatives HVC-304
Washington, D.C. 20515-6415

Re: Support for the Committee's Findings on Biometric Entry-Exit, and Recommendations for Implementation at the Land Border

Dear Chairman Crawford and Ranking Member Himes:

The International Biometrics + Identity Association (IBIA) writes to express its support for the Committee's recent *Review of the 9/11 Commission Report* and, in particular, for the Committee's finding that a comprehensive biometric entry-exit system remains one of the major unfinished elements of the post-9/11 security architecture.

IBIA is an advocacy and educational organization representing the developers, manufacturers and systems integrators of biometric and identity technologies and services. Our member companies build and field the systems at the center of the Committee's recommendations, including those in use today by U.S. Customs and Border Protection (CBP), the Transportation Security Administration (TSA), and DHS's Office of Biometric Identity Management (OBIM). We offer these comments in this advisory capacity, and we offer these recommendations earnestly and constructively. The Committee's objectives, overall, are sound. Our purpose here in this letter is to describe what meeting them will actually require and suggest additional steps to achieve the Committee's underlying goals.

I. Where We Agree

- **The Committee is correct that the mandate is unfinished.** Congress first required an automated arrival and departure matching system in 1996 and reinforced that requirement with biometric-specific provisions in the PATRIOT Act, the Border Security Act of 2002,

the Enhanced Border Security and Visa Entry Reform Act of 2002, and the Intelligence Reform and Terrorism Prevention Act of 2004. Biometric entry has been operational since 2004 and has performed admirably—CBP's facial comparison system has processed more than 971 million travelers and has prevented over 2,316 imposters from entering the country using genuine travel documents. As the report states, air, sea, and pedestrian land points of entry have all fully implemented biometric entry systems, challenges remain in collecting biometrics from travelers arriving in vehicles, and the United States "has not fully implemented a biometric exit screening system at any point of entry category." (We would respectfully note that the status table on page 21 rests on sources dated between 2018 and 2023—its "nearly complete" entry for biometric air exit reflects approximately 80 percent implementation as of July 2022—and the Committee may wish to refresh those figures with CBP before any follow-on product.) Only biometric verification can conclusively tie a travel credential to the person physically present; biographic data alone cannot.

- **The Committee is also correct to frame this as an <u>intelligence</u> function rather than a <u>logistics</u> function.** Biometrics establish who a person is. Intelligence establishes whether that person warrants further scrutiny. The two have to be anchored to each other, and connecting them has always been the harder portion of the 9/11 Commission's recommendation.

- **We support the Committee's call to professionalize open-source intelligence collection and analysis** as a primary intelligence discipline, including a dedicated OSINT line item in each agency's budget, formal training standards, and a formalized job code for OSINT practitioners.

- **We likewise endorse the Committee's admonition** that the United States "need not—and must not—replicate the surveillance architectures employed by totalitarian and authoritarian regimes," and that any recommendation intended to reduce barriers between intelligence collection and law-enforcement "must be accompanied by rigorous oversight, appropriate safeguards, and a heightened sensitivity to the privacy, rights and civil liberties of Americans." We note in particular that the Committee identifies the shared belief of all HPSCI Members in safeguarding privacy and civil liberties as "perhaps the most important principle" guiding its recommendations. We address below what we believe those safeguards must consist of (in context).

II. Recommendations for Implementation at the Land Border

Recommendation 3 observes that "technological advancements make collecting biometric data at points of entry relatively quick and easy." At air and sea points of entry, and in pedestrian lanes at land ports, that is now true, and the Committee's own completion data bears it out. In vehicle lanes, however, this objective is not yet true. The distance between those two facts is where the remaining appropriations, policy changes, and capital work reside, and it is the subject of most of

what follows. The land border is the most technically, logistically and politically difficult part of this problem, and the objective—completing biometric entry and exit without significantly impeding the flow of lawful commerce—cannot be met with technology alone. We would also note that the report does not address non-intrusive inspection, cargo screening, or coordination with Mexico and Canada. Several recommendations below are offered to fill those silences rather than to take particular issue with anything the Committee has written.

- **Fund 100 percent non-intrusive inspection (NII) capability at land ports of entry.** As the report notes, CBP is currently piloting facial recognition for travelers entering in personally owned and commercial vehicles. That work has advanced considerably, though individuals in a vehicle are still sometimes missed, and officers can compensate with handheld devices such as Biometric Exit Mobile when a vehicle reaches the primary inspection booth. But neither approach addresses people concealed in trunks or sewn into seats. Only NII—low-energy portals or x-ray systems—reliably detects concealed persons. In passenger vehicles, NII imaging can count the occupants. When that count doesn't match the number of faces captured by the camera or seen by the officer at primary, the mismatch is an objective reason to send the vehicle to secondary inspection. NII and biometric capture work together; neither replaces the other. In containers and semi-trailers, NII detects concealed people as well as contraband and cargo that does not match its declared bill of lading. That capability saves lives: people have died in sealed trailers and containers left by smugglers in extreme heat. Yet funding has never been appropriated for full NII coverage at U.S. land borders.

- **Make non-intrusive inspection mandatory.** Travelers may currently opt out of NII. We recommend that this policy be revisited and inspection made mandatory at land ports of entry. An inspection regime that can be declined by the people most motivated to decline it does not produce the accountability the Committee's recommendation contemplates.

- **Treat cross-border cooperation as an alternative to domestic reconstruction.** Several land ports lack the physical real estate to site NII equipment ahead of the primary inspection booths. Re-architecting those ports would be expensive and highly disruptive. A more cost-effective path may lie in agreements—and, where warranted, U.S. funding—that allow the required inspections to occur on the other side of the border before vehicles approach U.S. primary booths.

    - The United States already exchanges entry-exit data with both neighbors. With Canada, each country's entry records serve as the other's exit records. Because Canada operates border systems comparable to our own, that coverage is nearly complete. Under the U.S.-Mexico Entry/Exit Data Sharing Initiative, Mexico's National Migration Institute likewise shares records of entry into Mexico, which CBP uses to create U.S. exit records. But Mexican collection at the land border is uneven, so those exit records are incomplete.
    - We recommend that Congress consider funding upgrades to Mexican immigration and customs control points opposite U.S. land ports as part of a reciprocal

arrangement. The United States would inspect southbound traffic, which serves Mexico's interest in stopping weapons and currency. In exchange, Mexico would host NII of northbound traffic on its side before vehicles reach U.S. primary booths. Properly structured, this would make outbound records, including biometrics, more complete, and it could reduce or remove the need to reconfigure U.S. ports to fit inbound NII. Any such arrangement would need enforceable maintenance and service agreements to keep the equipment on the Mexican side working.

- **Address outbound traffic flows as a distinct engineering problem.** At the southern border, traffic generally flows into Mexico without inspection, interrupted only by periodic "pulse and surge" operations. If capturing a usable face image in a vehicle moving slowly through primary inspection is difficult, capturing one at speed on departure is substantially harder—and absent outbound NII, concealment remains straightforward. We also note that our Mexican counterparts observe, not unreasonably, that while the United States works to interdict drugs and terrorists moving north, comparatively little is done about the weapons and money moving south that fuel violence on their side of the border. Outbound capability would serve both governments' interests, and it is the natural U.S. contribution to the reciprocal arrangement described above.

- **Build on analytic architecture that already exists.** The Committee's recommendation regarding profiles and intelligence integration is, technically, the easier part of this undertaking, and it sits well beside Recommendation 4 on interoperable platforms incorporating AI from trusted vendors. CBP already performs predictive intelligence and pattern-of-life analysis at vehicle crossings: license plate readers feed analytic systems that assess route, origin and destination, flagging anomalies such as a pattern shift during a surge operation or apparent avoidance of a checkpoint. Arrival and departure records support similar questions—whether a daily crossing reflects work or school, or something else, and whether the pattern aligns with other openly available information. The model is well established on the cargo side, which the report's entry-exit discussion does not take up. CBP's Automated Commercial Environment (ACE) draws information from 47 Partner Government Agencies to determine whether a shipment represents a threat or a violation of import law. We recommend that the Committee direct attention to applying that same multi-agency fusion approach to foreign travelers, and to the cargo threat vector itself.

- **Attach explicit limits and enforcement to any profiling capability.** Recommendation 3's call for U.S. borders to be secured so that CBP "can collect biometrics and build profiles" has drawn more public attention than anything else in the report, and we believe the industry should speak to it directly rather than defensively. Recent public reaction to automated license plate reader deployments illustrates the governing principle: the public supports law-enforcement and border security so long as the technology does not injure

law-abiding people. Consistent with the Committee's own statement that safeguarding the privacy and civil liberties of Americans is imperative, we recommend that any authorization or appropriation implementing these recommendations carry the following conditions:

- Use of intelligence to inform profiles must be limited to foreign travelers, known and suspected terrorists, and criminals;
- Audit records must be maintained and subject to periodic independent review;
- Access controls must be strong and selective, with authorization limited to personnel with a demonstrated need;
- Training must be mandatory for all users; and
- There must be severe penalties for misuse—including by law-enforcement—such as querying systems to locate, stalk, or harass individuals.

These conditions reflect IBIA's published *Identification Technology and Privacy Policy Principles* — not concessions to the technology's critics. They are the reason the industry can support the Committee's recommendations without qualification, and they are what will allow these programs to survive serious scrutiny.

- **Address the talent pipeline.** One IBIA priority the report does not reach is the development of the next generation of technical talent. The report's treatment of China's "whole-of-society" approach addresses influence operations and public-private partnership; we would respectfully add education to that frame. The CCP's approach includes the deliberate cultivation of young people with the required technical skills. On raw output, the United States will not match it; China now graduates roughly 1.3 million engineers a year to about 130,000 in the United States. Our output has grown, but so has China's, and the ten-to-one ratio has held. No amount of analytic sophistication closes that gap. We have to be more focused, we have to value these professions, and we have to start earlier than college. To that end, the Israeli model merits the Committee's study. The Israel Defense Forces' Unit 8200, roughly the counterpart to NSA and CISA, identifies and recruits promising candidates in high school or earlier. Recruits can enter directly from secondary school and are trained within the unit, which deliberately draws on the unconstrained thinking of the very young to solve problems others had judged intractable. They discharge their national service obligation and emerge prepared for careers in intelligence or cybersecurity, with university an option afterward rather than a prerequisite. We recommend that the Committee consider analogous pathways in the intelligence and cybersecurity workforce provisions within its jurisdiction.

III. Conclusion

The objectives of the Committee's report are good — as far as they go. The Committee identifies whole-of-government cooperation as an overriding principle of its recommendations, and we agree. Achieving these particular objectives will require appropriations, policy changes, cooperation between countries and among agencies, capital improvements at the ports of entry,

rigorous privacy and access controls, and sustained investment in training and skills development —a set of problems that no single agency and no single vendor can solve.

IBIA and its Member companies possess the technical expertise to support the design, development, and deployment of the capabilities the Committee describes, and we are committed to facilitating open dialogue among government agencies, Congress, and the public on how they should be governed. We would welcome the opportunity to brief the Committee or its staff on any of the matters raised in this letter, and to serve as a technical resource as the Committee's recommendations move toward implementation.

Thank you for your attention to this longstanding national security gap, and for the Committee's care in addressing the civil liberties questions that accompany it.

Sincerely,

Robert Tappan
Executive Director
International Biometrics + Identity Association
robert@ibia.org

cc: The Honorable Elise Stefanik, Co-Chair, HPSCI 9/11 Review Task Force
The Honorable Josh Gottheimer, Co-Chair, HPSCI 9/11 Review Task Force
Members, House Permanent Select Committee on Intelligence