Closing the Loop:

Completing Biometric U.S. Entry-Exit

International Biometrics+Identity Association

Overview:
Leaving No Stone Unturned

IBIA and its membership strongly support the utilization of biometrics as visitors leave the U.S. Doing so will secure our borders, ensure enforcement of immigration law, and prevent wanted criminals from escaping. Creation of a biometric exit system at U.S. ports of entry is a necessary security enhancement whose implementation is long overdue. Biometric use at entry for over a decade, by US-VISIT and later OBIM, has significantly increased America's security and counter-terrorism efforts and underscores the value for the mandated counterpart system at exit.

The necessity of a biometric exit system only continues to grow. As terrorist and criminal networks grow ever more sophisticated, the tools we use to identify and interdict them must be nimble and adaptive. The evolving and challenging threat environment as shown by the Paris and the San Bernardino attacks, the rise of ISIS, and the resurgence of al Qaeda and its various offshoots requires a new approach—one which adds the power of a biometric to identify bad actors through all available means.

Apprehending terrorists, visa violators, and criminals before they leave U.S. jurisdictional boundaries is an essential part of bringing them to justice and a biometric exit is critical to this. There is little rationale for outsourcing further harm and expending energy and resources to pursue extradition for terrorists and criminals who are hiding abroad. Capturing those people before they depart the United States provides a considerable benefit to counter-terrorism efforts, immigration authorities, and to prosecutors throughout the country.

The worldwide efforts to bolster existing exit systems by adding biometric components is an intrinsic recognition that counter-terrorism efforts and law enforcement must use all of the tools in its arsenal to combat terrorists and criminals. Leveraging the information we already have is but the first step toward a comprehensive and effective border system.

This briefing paper starts with a review of the mandate for biometric entry/exit and then analyzes the several possible factors contributing to the delay, including concerns about cost, uncertainties about logistical implementation, and erroneous beliefs that biographical data is sufficient.

Biometrics technology and solutions expertise are available from many sources and biometric entry has been fully operational for over a decade. It is time to move forward to close the loop and complete the biometric entry-exit mandate. To accomplish this, IBIA believes that a strong DHS—industry partnership is essential and looks forward to working with DHS to implement this important program.

Mandate

Congress first mandated the creation of a system to match arrival and departure information back in 1996 as part of the **Illegal Immigration Reform and Immigrant Responsibility Act**. That act required that the Department of Justice (which held responsibility for immigration at the time) implement an automated arrival and departure system within two years. The mandate went unfulfilled.

> Visa overstays are not the only reason to have an exit system. Beneficiaries for various uses of such a capability include over 10 federal agencies or departments, 18,000 state, tribal and local law enforcement entities, and international partners—in addition to the law-abiding travelers themselves.

In the wake of the 9/11 terrorist attacks, the mandate was reiterated and strengthened to include biometrics in the **Intelligence Reform and Terrorism Prevention Act of 2004** (PL 108-458). The new mandate was then incorporated into the **Implementing Recommendations of the 9/11 Commission Act of 2007** (the 9/11 Act), which required the Department of Homeland Security to implement biometric exit controls within one year of the act's passage. Over a decade after the original mandate for a biometric exit, it remains unfulfilled.

Biographic vs. Biometric Identity Data

Biometrics are the only form of identity authentication that tie people to their credentials. As such, the accuracy and value of biometric data are fundamentally different from those used in current biographic systems. The critical advantage is that biometrics can foil an attempt to use false or misleading biographic information to avoid detection.

Biographical data are subject to errors (whether innocent or intentional) such as misspellings and typos, changed names and previous addresses. By contrast, biometric solutions have the unique capability to expose a false biographic history or a false identity claim.

Misspellings of names in a biographic-only system can be a serious problem, either because of entry errors or intended subterfuge. Boston bomber Tamerlan Tsarnaev's record of transit to Russia was obscured by a misspelling of his name—a fact that ultimately affected the associated investigation by the FBI.

While a biographic exit system may be able to verify the documents of individuals who overstayed their visas or violated their immigration status, it cannot verify the identity of the person presenting those documents. Ironically, the increasingly sophisticated security features in modern documents have resulted in the increased use of legitimate documents by impostors — those who strongly resemble the individual pictured in a real document. Often these impostors can be **detected** only through biometrics.

Furthermore, a biographic solution alone cannot provide the national security benefits that are the primary reason for a biometric exit system. Biometric data are the common threads that run through criminal records and watch lists held by multiple US government and international agencies. Many latent prints left at crime scenes and terrorist attacks are not associated with any biographic information. In the most critical cases for national security and law enforcement, biometric data are often the only link we have to perpetrators and suspects. An exit system based solely on biographic information does not enhance security in these cases.

Members of Congress and executive agencies agree that biographic information is not enough—biometrics are necessary to have the complete set of data for matching. In the words of Senator Chuck Schumer, "Knowing who is coming into the country, and knowing who is going out, is a matter of national security, plain and simple." As CBP's John Wagner noted in a recent hearing, "There is

The accuracy of biometric systems continues to rise. For fingerprints today, the true biometric match rate is in excess of 99.6%

law enforcement value in collecting fingerprints, and we are catching records which we would not have caught through just the biographical alone. We are able to close out records when somebody flies into the country on one passport and flies out on a different passport. The biometrics help us."

Biometric entry systems have already proven their value, delivering both accurate data and strong match rates with information in biometric holdings across the U.S. government. IBIA believes that claims about the accuracy of biographic exit ignore the concrete security and immigration enforcement benefits available from biometrics and are therefore not a sufficient reason to override the mandate for biometric exit.

Cost

In 2008, DHS conducted a study that produced a cost estimate for biometric exit and several administrations have used the significant cost estimates in that study as a barrier to implementation. However, this regularly cited cost estimate was based on policy and operational assumptions that were subsequently **declared inaccurate and inadequate by the Government Accountability Office.**

The 2008 study's cost estimate was designated as a "Class 5" cost estimate as defined by the Association for the Advancement of Cost Engineering International (AACEI). **According to the AACEI**, "Class 5 estimates are generally prepared based on very limited information, and subsequently have wide accuracy ranges." Accuracy ranges for Class 5 estimates are 20% to 50% on the low side, and 30% to 100% on the high side. Consequently, a very high risk multiplier was applied to the analysis because the requirements for a biometric exit and the effort it would take to build an effective system were not defined at the time.

Unfortunately, the faulty cost estimate numbers have continued to circulate and are used to justify delays in implementation. Even worse, those numbers are now over eight years old. In the intervening years, ***the price of biometric solutions has decreased substantially*** and many products are readily available off the shelf. At the same time, the

quality of biometric equipment has increased, and there are many more technological options that could be applied to biometric exit. Furthermore, we believe these cost estimates were inflated by an out-of-date assumption that all biometric exit processing will be attended, requiring the labor of agents.

The Department of Homeland Security's requirements for a biometric exit solution remain undefined. Thus, while IBIA believes that the early estimates are extremely high, the true cost of a complete biometric exit system cannot be accurately estimated until there is an updated concept of operations (con-ops). The biometrics industry continues to urge the Department to define its requirements, and remains available to assist in the creation of a reasonable, data-driven cost estimate based on solid con-ops requirements.

Debating the merit of a biometric exit system solely on cost also fails to account for the significant benefits to America's security, immigration policy, and apprehension of criminals. Once the technical and policy requirements for biometric exit are defined and a cost estimate can be produced, a more informed cost/benefit analysis can finally take place.

Logistics

Some stakeholders presuppose that the operating concept of biometric exit will mirror the operating concept of biometric entry—Customs and Border Protection officers in booths, processing long lines of people, resulting in delays in passenger throughput and require costly new additions or similarly expensive reconfigurations of existing space

This concern is based on an assumption that is not necessarily true. There are many options by which both passenger throughput and the footprint of biometric exit could be greatly minimized, or even integrated into existing processes to the point where it has ***no discernible impact on throughput and space requirements.***

The operating concept for biometric exit can be defined in a way that does not impede passenger throughput or preclude an efficient use of space. IBIA members welcome the opportunity to demonstrate how new innovative solutions involving multiple biometric modalities (iris, contactless fingerprints, facial recognition, etc) can address concerns about both throughput and the deployment footprint. This is reflected by the systems that many European countries have implemented that use biometrics and maintain throughput.

A Global Trend

Building on the success of biometric entry in the United States, countries around the world are now implementing comprehensive biometric systems to confirm identities at the border,using a wide variety of technological solutions. Through the combined use of fingerprints, irises, facial recognition, and document authentication, border officials around the world now have a series of sophisticated tools to identify travelers of interest. The use of automated biometric technologies and e-gates allows for a process with fewer border officers and a smaller physical footprint while actually speeding the flow of passengers.

Biometric technologies are being used for entry and exit in the UK, Germany, Sweden, Austria, France, the Netherlands, Australia, New Zealand, Hong Kong, and the Gulf States. Many others are in the process of formulating and implementing biometric solutions.

The global trend toward the use of biometrics to enhance border security has accelerated dramatically in the past year, driven by the growing numbers of refugees, the rise of ISIS, and attacks in Paris, San Bernardino, and elsewhere in the world. The increasing use of biometrics has also sparked new information sharing initiatives designed to reveal the travel patterns and criminal histories held in disconnected systems around the world.

The cost-benefit analyses that counties are making reflect this new threat environment. Security needs have expanded. The benefits of biometrics are more apparent than ever. At the same time, costs have decreased substantially.

Partnership with Industry

In 2014, the Department of Homeland Security formally launched the **Apex Entry/Exit Re-engineering (AEER) program.** This effort is designed to bridge the gap between the current biographic and future biometric exit systems, define operating concepts, and lay the groundwork for a procurement strategy. In support of this effort, the Department stood up a program office dedicated to exit programs and constructed a test facility outside of Washington DC to evaluate equipment and operating concepts.

The biometrics industry sees this as a promising development in the quest for a biometric exit program. Robust conversations about operating concepts, policy choices, and technological capabilities are needed to ensure the successful deployment of an exit solution.

DHS should consider the industry standpoint on research and development decisions to ensure that its needs are met. To the extent that DHS can make clear statements of needs and requirements early enough, it is easier for industry to make decisions to fund associated R&D and pursuits in support of those objectives. In an era where investment money is under constant pressure, this is a serious consideration. If DHS cannot articulate clear requirements early enough, the quality of the support that industry can provide will be reduced.

IBIA believes that if DHS begins a more open process of exploring operating concepts and defining requirements, it will ensure that companies will have the lead time and market intelligence necessary to anticipate the Department's future needs. The biometrics industry applauds DHS for its willingness to contemplate the technical and policy requirements necessary to move forward with biometric exit. Yet if biometric exit is to become a concrete reality, DHS must engage in a more substantive and open dialogue with the biometrics industry — an industry on which it will depend to bring an operational concept to life.

A clear and concise DHS requirements definition (including industry input), appropriate staging, and disciplined, professional project management are keys to building and implementing a successful biometric Exit program. This will offset the uncertainties associated with current estimates.

Next Steps

To fulfill this long-standing legislative mandate and at last begin the process of tightening border security, IBIA recommends the following actions:

1. DHS should begin a formal partnership with the biometrics industry to turn its operating concept into technical requirements. Using the newly created Joint Requirements Council, DHS should engage with biometrics companies in a process that is open to all, ensuring the creation of technical standards that are rigorous, promoting active competition and innovation.

2. DHS should initiate a continuing public and open dialog on its tests, trials and plans, such as the sessions planned for connect:ID. This will ensure an informed industry with the lead time and market intelligence for research and development activities that will enable the industry to provide the best tools, technologies, and solutions to meet DHS needs and plans.

3. Using jointly developed requirements, DHS and the industry should agree on a budget estimate. A cost estimate created by both DHS and the industry will prove far more realistic than those developed in the past, and will have a broader base of support.

Sources and Additional Reading

AACE International Recommended Practice No. 18R-97, "Cost Estimate Classification System — As Applied in Engineering, Procurement, and Construction for the Process Industries", November 29, 2011, **http://www.aacei.org/toc/toc_18R-97.pdf**

Customs and Border Protection, "CBP Arrests Impostor at the Peace Bridge", (February 2014, **http://www.cbp.gov/news-room/local-media-release/2014-02-03-000000/cbp-arrests-impostor-peace-bridge**)

Department of Homeland Security Inspector General, "US-VISIT Faces Challenges in Identifying and Reporting Multiple Biographic Identities" (OIG-12-111, August 2012, **https://www.oig.dhs.gov/assets/Mgmt/2012/OIG_12-111_Aug12.pdf**)

Department of Homeland Security, "USVISIT Air Exit Pilots Evaluation Report," (2009, **http://www.fairus.org/DocServer/US_Visit_Air_Exit_Pilots.pdf**)

Government Accountability Office, "Border Security: Additional Actions Needed to Improve Planning for a Biometric Air Exit System", (September 2013, GAO-13-853T, **http://gao.gov/products/GAO-13-853T**)

Government Accountability Office, "Overstay Enforcement: Additional Actions Needed to Assess DHS's Data and Improve Planning for a Biometric Exit Program", (July 2013, GAO-13-683, **http://www.gao.gov/assets/660/656316.pdf**)

Government Accountability Office, "Immigration Enforcement: Preliminary Observations on DHS's Overstay Enforcement Efforts", (May 2013, GAO-13-602T, **http://gao.gov/products/GAO-13-602T**)

Government Accountability Office, "Homeland Security: US-VISIT Pilot Evaluations Offer Limited Understanding of Air Exit Options", (August 2010, GAO-10-860, **http://gao.gov/products/GAO-10-860**)

Government Accountability Office, "Homeland Security: Prospects For Biometric US-VISIT Exit Capability Remain Unclear" (June 2007, GAO-07-1044T, **http://gao.gov/products/GAO-07-1044T**)

Government Accountability office, "Technology Assessment: Using Biometrics for Border Security", (November 2012, GAO-03-174**,** **http://gao.gov/products/GAO-03-174**)

U.S. House of Representatives, "Fulfilling a Key 9/11 Commission Recommendation: Implementing Biometric Exit", Hearing before the Subcommittee on Border and Maritime Security, 113th Congress, **https://www.gpo.gov/fdsys/pkg/CHRG-113hhrg86486/html/CHRG-113hhrg86486.htm**

U.S. Senate Judiciary Committee, "Why is a Biometric Exit Tracking System Still Not in Place?" (January 20, 2016, **http://www.judiciary.senate.gov/meetings/why-is-the-biometric-exit-tracking-system-still-not-in-place)**

Identity Matters.

International Biometrics+Identity Association

1090 VERMONT AVENUE, NW • 6TH FLOOR
WASHINGTON, DC 20005
202.789.4452 x1309 • IBIA.ORG