

IBIA Response to the Department of Homeland Security's Biometrics Strategic Framework

Overview

The International Biometrics Industry Association (IBIA) congratulates the Department of Homeland Security (DHS) on the release of its [Biometrics Strategic Framework](#). The Joint Requirements Council and its Information Based Screening and Vetting team produced a thoughtful, meaningful document that addresses many of the ongoing challenges and issues surrounding the use of biometrics in the Department's operations.

In response to the framework, IBIA strongly encourages DHS to establish a regular forum for communication with the biometrics industry. As the framework repeatedly notes, challenges in maintaining a coordinated dialogue has led to inefficient and duplicative procurements which lead to overlapping expenditures, underinvestment in critical technologies, and the creation of systems that inhibit information sharing. Ongoing discussions about DHS's challenges and requirements are the first step in creating a valuable partnership that will benefit both the Department and the companies that serve its needs.

IBIA and its members also encourage DHS collaboration with industry and interagency partners to provide a standardized platform that serves the community with the most biometric intelligence, enabling swift response and action at the forefront of any homeland security mission.

IBIA appreciates the Department's increasing willingness to use a wide range of biometric technologies, and hopes that the vision demonstrated in this framework will extend across new modalities and use cases. Fingerprint, iris, and face are all mentioned in the framework document – IBIA recommends that DHS include DNA and voice in the scope of its discussions.

IBIA agrees with the Department's analysis of its approach to biometrics. IBIA agrees that moving away from the stove-piped, component driven approach to biometrics can greatly help reduce system costs. IBIA agrees that improved coordination between DHS components and other agencies on standards and requirements can prevent the creation of incompatible system architectures. IBIA also agrees that more effective communication around future requirements across the DHS enterprise will lead to more balanced investment by industry in future technologies.

IBIA is one of the leading trade associations focused on the effective and responsible use of technology to determine identity and enhance security, privacy, productivity, and convenience for individuals, organizations, and governments. After the release of the DHS

document, IBIA consulted with its members to develop actionable feedback to the stated objectives.

Comments on Objectives

Below are comments on each of the strategic objectives outlined in the framework document:

Objective 1.1: Refresh outdated biometric collection systems

IBIA agrees, and urges DHS to establish an open forum for dialogue with industry about requirements and capabilities. The biometrics industry is eager to meet the Department's needs for the next generation of biometrics systems, but frequent communication will be critical to realizing that goal. In particular, IBIA hopes that the Department will provide greater insight into proposed technical upgrades associated with the IDENT database and the Apex Entry-Exit Re-engineering (AEER) project.

Objective 1.2: Centralize access to federal and international biometric databases

IBIA agrees, and is excited by the possibility of further interagency cooperation on the formats and standards that are used for processing biometric information. The current approach of agency specific information fields and data formats raises the cost of system development and operations considerably. IBIA recommends that DHS use established forums such as those at NIST to leverage existing interactions with industry on standards.

Objective 1.3: Improve real-time access from field locations

IBIA agrees, and is prepared with a variety of solutions to improve field connectivity. IBIA also encourages DHS to consider adopting a Department-wide stance on the use of device-level biometric watch lists, which would eliminate the need for field connectivity in many instances. Some DHS components use device-level biometric watch lists, but their policies and application are inconsistent. IBIA acknowledges that the use of device-level biometric watch lists still requires regular synchronization of the device-level biometrics watch lists.

Objective 1.4: Expand use of multi-modal biometrics to identify threats

IBIA strongly agrees, and again encourages DHS to engage in a dialogue with industry about its requirements. The wide variety of biometric technology options and processing applications presents the Department with the luxury of choice. Leveraging that choice to full advantage will require the Department to be specific about the results it wants to achieve. Multi-modal biometrics can be configured to be utilized in full or in part

depending on the overall confidence level or match probability of a single, dual or more biometrics.

Objective 2.1: Automate resource intensive identity processes

IBIA agrees, and stands ready to provide the automated solutions required to reduce human resources costs across the DHS enterprise.

Objective 2.2: Implement person-centric biometric processing

IBIA agrees – a truly federated architecture would allow DHS and partner agencies to adjudicate encounters in an efficient and timely manner. IBIA cautions, however, that implementing a “person-centric” approach to biometric processing cannot be accomplished in a vacuum. The interoperability of biometric information and the ability to process biometrics at the interagency level requires a common approach. If DHS alters its processing regime, it should ensure that its model remains compatible with those of partner agencies.

Objective 2.3: Expedite security processes using identity verification capabilities

IBIA agrees, and salutes the progress DHS has already made in implementing this objective. IBIA also recognizes that biometrics can be used in combination with documents to enhance security processes. The increasing use of biometric indicators in identity documents around the world testifies to the utility of that strong combination.

Objective 3.1: Institutionalize joint requirements efforts

IBIA strongly agrees, and asks the Department to consider formalizing its dialogue with industry as a part of this institutionalization effort. Adding industry representation on the JRC and/or IBSV, hosting regular open forums through IBIA members for discussion and debate, using existing NIST working groups to leverage ongoing work on standards, and publication of regular reports on the Department’s thought processes are all ways in which DHS can take advantage of industry knowledge and improve communication.

Objective 3.2: Establish DHS-wide biometrics authorities

IBIA agrees. Having a broad range of experience in implementing a wide variety of information sharing models around the world, IBIA members can provide comparative insight to DHS as it considers the operational impact of policy changes.

Objective 3.3: Develop privacy policies and processes

IBIA applauds DHS's willingness to tackle the complex privacy issues surrounding collection and use of biometric information. IBIA members are strongly committed to ethical use of biometrics and welcome additional dialogue on how the IBIA [ethics statement](#) might be applied to the Department's efforts.

Objective 3.4: Enhance stakeholder communications

IBIA strongly agrees, and sees enhanced communication as the lynchpin of the Department's efforts to enhance its biometric systems. IBIA urges DHS to consider the establishment of a regular Department-wide forum which would allow for ongoing dialogue, efficient communication, and fair access to relevant decision-makers.

Objective 3.5: Implement standardized solutions

IBIA agrees, and even asks the Department to consider expanding its drive for standardization to other agencies as well. As information sharing across the government continues to expand, DHS has an interest in promoting the lower costs and increased efficiency which would come with a whole of government approach to biometric solutions.

Objective 3.6: Establish governance and ensure appropriate oversight

IBIA agrees – an effective oversight mechanism is necessary to ensure public trust in the use of biometrics and protect against misuse. IBIA also asks the Department to consider inclusion of IBIA industry representatives in its oversight efforts as a way to take advantage of the technical expertise that may be necessary to draw conclusions about the proper operation of biometric systems.

Next Steps

Building on the framework's solid foundation, IBIA looks forward to a productive dialogue with DHS and its components. IBIA is also prepared to take the first step by hosting Department officials to launch a dialogue on the framework and how it can be implemented in practice. IBIA will reach out to the authors of the framework in the near future to begin this process in earnest.