Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.
RESPONDENT INFORMATION AND BACKGROUND

a. Organization and Respondent

Respondent Name:

Maria Cardiellos
Executive Director

Respondent Address:

Integrated Justice Information Systems Institute (IJIS)
20110 Ashbrook Place, Ste. 150
Ashburn, Virginia 20147

http://www.ijis.org/

Type of Organization:

Private Nonprofit

b. Organization Overview

The Integrated Justice Information Systems Institute (IJIS) was founded in 2001 as the result of the Department of Justice’s (DOJ) interest in engaging private sector participation in the advancement of national initiatives affecting justice and public safety and more recently homeland security (including school safety) and health and human services. We are a nonprofit alliance working to promote and enable technology in the public sector and expand the use of information to maximize safety, efficiency, and productivity. IJIS is the only national membership organization that brings together the innovative thinking of the private sector and practitioners, national practice associations, and academic organizations that are working to solve public sector information and technology challenges. IJIS advocates for policies,
processes, and information sharing standards that impact our safety and security; build knowledge on behalf of our stakeholder groups; and, connects the organizations and leaders within the communities of interest.

Additionally, IJIS provides a trusted forum within and across our areas of focus where resources are developed, collaboration is encouraged and public sector stakeholders can realize the benefits of technology and the power of information to keep our communities safe, healthy, and thriving. We assist in government sectors by bringing industry to the table in a constructive role and continuing to drive toward achieving high regard for the companies that are dedicated to helping the public sector find high-value solutions. IJIS is funded through a combination of federal grants, industry contributions, and partnership agreements.

Finally, IJIS is an active member of several committees, forums, etc., in support of the public sector mission joining practitioners and providers at the many working tables. Examples include the DOJ Global Advisory Committee, the IACP CJIS Committee, and the many IJIS Advisory Committees that include the IJIS CJIS Committee, the Law Enforcement Advisory Committee, the Court and Corrections Advisory Committees, and the Technical Architecture Committee – all these include practitioners, services providers, academia and research experts nationwide.

c. The State of Biometric Technologies

As industry, practitioners, and policymakers, we all tend to forget the amount of time it takes to perfect certain technologies, even in the field of biometrics. Once a new technology is developed, it takes decades to understand its true effectiveness, develop proper policy, and fully understand proper usage and legal implications. For example, fingerprints were first used in law enforcement in the late 1800s to early 1900s with the first official fingerprint card being developed in 1908. The FBI did not form an identification division for another 16 years in 1924. It took another 56 years for the first Automated Fingerprint
Identification System (AFIS) database to be developed. Currently, there are over 70 million cards with 700 million fingerprints in AFIS. Even today, these computerized generated matches are often followed by human verification in major cases.

Likewise, the first usage of DNA in law enforcement was in 1986. However, it took years of debate, legal policy reviews, ethical discussions, and technology advancements before the courts would accept DNA as evidence. DNA technology has advanced rapidly since its first use in a criminal case 40 years ago. Now many states require DNA collection for sex offenders and felony offenders. There is still much policy work to do in the field of DNA collection to close collection gaps and auditing to ensure that legislation is fully met. Evidence retention policies are a critical need for law enforcement to protect this evidence and retention policies to use DNA technology successfully.

Fingerprints and DNA are just two examples of biometric technologies that took decades to fully develop. Given that technology and research have advanced significantly we should expect newer identification technologies such as facial and retina recognition to take time to mature and perfect much quicker than fingerprints, but perfection requires the use, testing, policy development, ethical review, and clear governance.

d. IJIS Differentiators / Uniqueness

IJIS recently celebrated the milestones and all of the accomplishments in our 20-year history. Our success is built on our community of collaboration that represents our public and private sector members; our practitioner community nationwide as well as our subject matter experts that balance operational realities with proven results; our research and academic partners that contribute innate skills that assess and evaluate value; national membership organizations that represent public sector domains spanning justice, health and wellness, school safety, technology, and so many others; and, proven leaders in their fields demonstrating initiative management and implementation skills nationwide with so many success stories.
Given this array of talent that IJIS can offer in support of the DHS OSTP effort, our community organization is such that we engage the best resources from the different communities nationally to best respond to the goals and objectives of the given request for service. Such is the case with this RFI – we could recruit and/or issue a call for participation from our membership to support any of the defined topic areas. Understanding the critical value of governance in the constitution, vision definition, buy-in and support, policy adherence as well as long term implementation and support – “governance programs, practices, and procedures (applicable to the context, scope, and data use of a specific use case).” is that topic area upon which the IJIS response will focus.

d. Governance Programs, Practices, or Procedures

Law enforcement, courts, corrections, and policymakers require clear guidance and policy when implementing new technologies. This can only be achieved with proper governance. Governance is important to evaluate technologies and to establish standard operating procedures within legal limits that govern how and when technology should be used. Users of these technologies must be provided a strict set of rules by which they must operate. Those rules, often referred to as Standard Operating Procedures (SOPs), guide the use of the technology, how it is conducted, and to ensure its success. These policies and practices provide clear guidance, manage expectations, and reduce frustrations.

As part of the RFI, the following are the stated priorities that must be considered when proposing a governance methodology. Though not a one-to-one correlation, the IJIS proposed governance model addresses the intent of each concern.

i. Stakeholder engagement practices for systems design, procurement, ethical deliberations, approval of use, human or civil rights frameworks, assessments, or strategies, to mitigate the potential harm or risk of biometric technologies;
ii. Best practices or insights regarding the design and execution of pilots or trials to inform further policy developments;

iii. Practices regarding data collection (including disclosure and consent), review, management (including data security and sharing), storage (including timeframes for holding data), and monitoring practices;

iv. Safeguards or limitations regarding approved use (including policy and technical safeguards), and mechanisms for preventing unapproved use;

v. Performance auditing and post-deployment impact assessment (including benefits relative to current benchmarks and harms);

vi. Practices regarding the use of biometric technologies in conjunction with other surveillance technologies (e.g., via record linkage);

vii. Practices or precedents for the admissibility in court of biometric information generated or augmented by AI systems; and,

viii. Practices for public transparency regarding the use (including notice of use), impacts, opportunities for contestation, and redress, as appropriate.

The stated purpose of the RFI is to understand the extent and variety of biometric technologies in past, current, or planned use; the domains in which these technologies are being used; the entities making use of them; current principles, practices, or policies governing their use; and the stakeholders that are, or might be, impacted by their use or regulation. To ensure the comprehensive review, assessment, adherence to and implementation, and support of a solution that will meet the policy, operational and technical needs of a user community (relative to defined use cases), a proven governance model is critical to success. IJIS has successfully used a proven governance model that founded the success of over twenty (20) national programs across the nation in support of information sharing (several funded by DHS, DOJ OJP, BJA,
This **proven model/methodology is comprised of four (4) pillars of success** that will effectively respond to supporting any implementation or advances made in the usage of biometric technologies to support specific use cases within the public safety domain. They include the following:

**Policy and Governance** ensures the gathering and analyzing of information on the missions, goals, strategies, policies, and operational challenges reflected of the participating domains, agencies, stakeholders, etc.;

**Business Processes and Operations** ensures alignment of business processes and operations with existing and/or new policies and governance models. It will also support the definition and address the priorities of the proposed Steering Committee depicted in the provided graphic.

**Systems and Technologies** will focus on determining what solutions are in place, how they can be improved or enhanced, and providing guidance related to the development and implementations of biometric technologies and data access across agencies, domains, etc. to ensure alignment with operation and policies; and,

**Outreach and Communications** (O&C) will ensure that – as progress is realized on the policy, operational, and technical fronts – proper messaging is developed to support education, engagement, participation, and ultimately new technologies that might otherwise cause consternation to any constituent groups. The proper education and socialization plan is so critical to the success of these efforts that IJIS will engage expert practitioners, partner organizations, and other resources including those from the field as needed. Each messaging tool (in the format of training, TA, or other support interactions) will build upon—new knowledge, current and emerging best practices, developed toolkits, and other resources that are integrated and replicable—helping the program remain at the forefront in providing critical services to all stakeholders.

Though specific goals and objectives would be developed to support a successful governance model in
support of advancing the proper usage of any new biometric technology, IJIS’ experience has shown high-level goals should address no less than the following intentions:

1) Ensure engagement of the key constituencies to be directly or indirectly impacted by the new technology implementation. Commitment or buy-in of executives from each of the participating domains/organizations (as part of the proposed Executive Steering Committee depicted) will ensure the support of supporting members of those agencies (to comprise the Subject Matter Expertise (SME) Council, as well as the Policy, Operational and Technical Working Groups also depicted.

2) Ensure the successful alignment of mission needs with existing and newly developed processes, policies, and technologies.

3) Ensure the constitution of both an Audit and Evaluation program components to measure the progress, impact, and necessary improvements warranted over time.

4) Given the progress that is sought during the initiative, ensure the proper and timely communication is delivered consistently and effectively to all participating domains, agencies, practitioner groups nationally, and the public that will benefit from the overall educational impact.

The overarching “steps” – and services available to support same from the IJIS Institute – to constitute the proposed governance model include the following:

**Standup a National Public and Private Sector Biometrics Technologies Steering Committee**

Success requires a multidisciplinary approach led by stakeholders that represent the landscape of services offered, as well as the populations to be served. Leadership, vision, buy-in, engagement, and even education are all critical aspects of a successful governance model to address emerging solutions, be that on a local level let alone a national perspective. Leaders in each of these fields or domains should
constitute the Executive Steering Committee, as well as provide Subject Matter Expertise (SMEs) to support other aspects of the governance model and program implementation if necessary.

A representation of the proposed governance model is provided below. The graphic depicts the critical components to include the Steering Committee as discussed above, along with the supporting SME Council that will be organized into three subgroups to address Policy and Governance, Business and Operational issues, as well as Technology and Architecture needs. It is important to note that this governance body is not a transitional entity to address any specific project alone. It is a governance structure that should be codified to address the critical needs of Public and Private Sector Usage of Biometric Technologies nationwide.

**Support the Development of Priorities for the National Public and Private Sector Biometrics**

**Technologies Steering Committee**

The IJIS Team proposes to work with the National Public and Private Sector Biometrics Technologies
Steering Committee to develop a comprehensive assessment, review, implementation (if appropriate), and evaluation of biometric technologies used in the public and private sectors. Though one can anticipate the challenges that are evident in responding to such an effort, the proposed working sessions with the Steering Committee will not only identify the priorities as they exist today but will enable us the dialogue to identify and address operational efficiency opportunities, and policy guidelines that will impact the outcomes in the future. Each of the intended Committee members will bring a vast array of diverse experiences that collectively represent national trends, challenges, and gaps to be addressed. The IJIS Team proposes to work with Steering Committee members to

a) convene critical players that make up the participating members;

b) facilitate a dialogue to identify the common gaps that members experience when trying to implement and/or consider such technologies;

c) assess the operational and policy implications that impact a common solution;

d) design a solution that meets the collective needs of the community, and

e) outline a plan for implementation of a pilot to validate its effectiveness.

Subsequent support/activities that can be provided – but exceed the direct constitution of the governance model (though the committees would be engaged) - including the design and development of minimum guidance to be made available to both public and private sectors on the implementation and use of biometric technologies; the constitution of a national model repository to server as a resource bank for future implementations; the development of model policies to be used by participating implementation agencies; the assembly of a training and technical assistance resources that can guide agencies in the development of related programs; and the possible development of web-based resource center providing actionable resources, templates, and relevant content around research, policy, and governance, business process and operations, best practices, lessons learned, voices from the field, and systems and
technologies, as well as serve as a library of comprehensive training.

e. Conclusion

IJIS Institute has a proven success record of employing a methodology that constitutes the engagement of disparate user groups/domains, etc. on the federal/state/local levels, the facilitation of same to arrive at a design/development (with our private sector partners) / implementation/support of a solution that will meet the needs of the champion agency/domain. Critical success factors will always be founded on a governance structure that supports policy assessment/development/adherence at all levels of participation (FSLT). Our record of over twenty years delivering solutions nationwide that remain in operation today is proof of our success.

Though there is much more detail to provide and/or suggestions to offer in the evaluation of responses to this DHS OSTP RFI, the page limitation mandates that this narrative be brought to a conclusion. IJIS has successfully supported DHS and other federal partners with numerous national initiatives that include the Nationwide Suspicious Activity (SAR) Initiative (NSI), the National Fusion Center Initiative, the current CAD to CAD Interoperability initiative and so many others. We look forward to the opportunity to support this valuable effort and to tailor a solution-set that meets the priorities of the public and private sectors' use of biometric technologies properly and successfully nationwide.