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.
January 14, 2022

Subject: Dignari Response to the Office of Science and Technology Policy (OSTP) Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies

Name of person(s) or organization(s) filing the comment: Dignari, LLC

Respondent type: Industry

Dignari is pleased to submit our response to the OSTP RFI. Dignari is a Women-Owned Small Business (WOSB) that specializes in program strategy, emerging technology, data science, and human-centered design. Our personnel have built and deployed numerous biometrics solutions successfully over the last 25 years, including for key U.S. Federal Government programs including the TSA Transportation Worker Identity Credential (TWIC), TSA Registered Traveler, Department of Homeland Security (DHS) Homeland Security Presidential Directive 12 (HSPD-12), U.S. Customs and Border Protection (CBP) Biometric Entry-Exit Program, General Services Administration (GSA) USAccess, and the DoD Common Access Card (CAC). We continue to provide a full suite of biometric services to our clients and look forward to published results from this RFI and OSTP’s continued role in the advancement of policy relevant to biometric technology.

The table below provides our company and GSA MAS contract information for acquiring Dignari services and solutions. We welcome the opportunity to discuss these options in more detail. Dignari’s point of contact is Adnan Malik, who can be reached at [redacted] or

<table>
<thead>
<tr>
<th>Dignari Company Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Name</td>
</tr>
<tr>
<td>DUNS</td>
</tr>
<tr>
<td>Contact Name</td>
</tr>
<tr>
<td>Email</td>
</tr>
<tr>
<td>Phone &amp; Fax</td>
</tr>
<tr>
<td>Business Address</td>
</tr>
<tr>
<td>Contract Vehicles:</td>
</tr>
</tbody>
</table>

Sincerely,

Gena C. Alexa
President
Dignari, LLC
**Topic 1: Descriptions of use of biometric information for recognition and inference**

Dignari personnel have over 25 years of experience with biometric technologies and have found that the use of biometric information falls into two broad categories: (a) for foundational use; and (b) for functional use. In effect, this aligns to the traditional access control constructs of authentication and authorization respectively.

Foundational biometric use most often determines “are you who you claim to be.” (e.g., biometrics associated with passports). These systems incorporate varying levels of identity proofing appropriate to operational requirements prior to storage of biometric data. Functional biometric use (e.g., Apple Face ID) is based on some level of established foundational biometric data and is used to determine “are you eligible for a specific service” (e.g., to use an iPhone, to travel, to access a facility, to operate a vehicle), and is offered by both the public and the private sectors. When it comes to establishing root foundational identity within a society, government entities are most often relied upon as the authoritative source of biometric data. These foundational biometrics are in turn often used as seed inputs for derived systems. For example, using a passport photo for identity proofing during employment or benefit program issuance processes.

Each category has challenges and limitations in terms of use. Foundational biometric data, especially in the U.S., is often associated with breeder documents (e.g., birth certificates), however, the lack of universality of documents within a population (e.g., not every citizen owns a passport, lost birth certificates) creates challenges when trying to link biometrics with established industry or enterprise-wide rulesets. Functional biometric use has challenges such as a general mistrust of how the biometric data is used, how it is secured, and how it is obtained by both public and private sector entities. For example, utilizing PII to gain access to a resource, misuse of biometric data, and unknown collection such as automatically tagging people in photos.

Functional use of biometrics has grown rapidly over the last decade and touch almost every sphere of economic and social life, including banking, e-commerce, mobile phones, immigration, and travel. Recent advancements in biometrics, and artificial intelligence in general, have extended the functional use of biometric information to include behavioral or cognitive use. Notable examples include the use of facial biometrics in automobiles to assess the weariness and attentiveness of a driver or sentiment analysis for advertising. Dignari’s work has spanned the full spectrum of foundational and functional use-cases of biometric information, crisscrossing the public and private sectors.

### Foundational Biometric Use

Dignari has vast experience across multiple U.S. Federal Government clients in the use of foundational biometric information. Many of the systems that we have developed and delivered consist of an enrollment capability where breeder documents and other information is used for identity proofing prior to user account creation and biometric collection.

<table>
<thead>
<tr>
<th>Planned, developed, or deployed uses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our developed and deployed uses of foundational biometric data include enrollment systems where users gain access to program benefits or are issued credentials (e.g., federal employee and</td>
</tr>
</tbody>
</table>
contractor badges). Planned use includes referencing or using foundational biometric data to establish identity or to issue derived credentials for expedited and trusted travel use cases.

**Goals of use**

Goals of use include initial identity proofing as well as the establishment of foundational biometric data which is authoritative in terms of the given program. This foundational biometric data may then serve as an enabler for functional use later. Foundational biometric data may be collected and stored in the system and serve as foundational for that program or the system may simply reference other authoritative source biometric data repositories at time of use.

**Nature and source of the data used**

Foundational biometric data typically involves attended collection between an operator and the individual who has opted in to be enrolled. This is to ensure the data is of high quality and trusted at the point of origination into the system. Some of these systems may collect a combination of biometric modalities. For example, ten prints for background investigations, face images for duplicate checks, and iris images for future system flexibility. Foundational biometrics should remain as close to single-sourced as possible. Distribution of copies or different versions of the biometric information may introduce challenges and increase privacy and security risks.

**Deployment status (e.g., past, current, or planned deployment)**

Dignari personnel have assisted with the implementation of numerous State/Federal/International foundational government biometric systems in the past and continue to support similar implementations today.

**Impacted communities**

Most of the foundational biometric systems we’ve implemented have been focused on providing a trusted population with the opportunity to voluntarily provide biometrics to gain access to specific program benefits, such as expedited processing.

**Functional Biometric Use**

Our experience working with the U.S. Federal government in the functional use of biometrics, includes traveler screening and identity management to improve citizen services and national security. In most cases, functional biometric use is limited to trusted populations or for frequent lower risk travelers who opt-in for added benefits and convenience of expedited processing.

**Planned, developed, or deployed uses**

Our developed and deployed use of functional biometric data includes several traveler processing systems where users gained access to dedicated lanes and expedited processing. Efficient and frictionless travel experiences are currently being implemented that allow touchless and more sterile biometric processing while improving overall security posture.

**Goals of use**

The functional biometric systems we’ve implemented have attempted to make the user experience faster, easier, and less intrusive while also making the system more secure and trustworthy.

**Nature and source of the data used**
The user experience is varied during functional biometric use. Technologies such as face and iris allow at-a-distance and on-the-move biometric collection while fingerprint typically requires direct contact with devices. Recent advances in contactless fingerprint technology reinforce the idea that industry continues to pursue a balance between convenience and utility. In many cases, sharing benefits across biometric system boundaries enhances the collective ecosystem. As a result, interoperability remains a central tenet with national and international standards bodies continuing to refine relevant standards. Some of our clients have used these industry standards to develop program specific requirements for functional biometric use. For example, establishing face image capture guidelines to include image requirements (e.g., dimensions, quality metrics) and camera placement.

**Table 1: Foundational and Functional Biometric Data Use**

<table>
<thead>
<tr>
<th>Deployment status (e.g., past, current, or planned deployment)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dignari personnel have assisted with the implementation of numerous State/Federal/International functional government biometric systems in the past and continue to support similar implementations today.</td>
</tr>
</tbody>
</table>

**Impacted communities**

Most of the functional biometric systems we’ve implemented have focused on providing a trusted population with dedicated areas for expedited processing. Impacted communities include travelers and operators of the system, as well as the larger community that relies on the security implemented by the system. Additionally, those who choose not to enroll or who are ineligible to participate are also impacted by their inability to realize potential benefits.

**Topic 2: Procedures for and results of data-driven and scientific validation of biometric technologies**

The procedures for and results of data-driven and scientific validation of biometric technologies requires more than just algorithm analysis—it requires an examination across the full spectrum of people, process, and technology. While there is great value in laboratory analysis of algorithms using standardized data sets, normalized procedures, and scientific methods, it is also important to understand the interplay between people, process, and technology in a holistic operational analysis. How does the technology perform given the unique and often unconstrained environments in which it is deployed and how do individuals interact with it? Unfortunately, biometric systems may excel in the lab yet fall flat in production. For example, we recently analyzed face Presentation Attack Detection (PAD) capabilities on mobile phones and our client’s unique operational environment (e.g., time of day, indoors/outdoors) was central to our testing. One of the top performing solutions, which could not be spoofed in our lab, failed miserably once it was used outdoors. Understanding real-world scenarios such as this exposed the technology as unusable.

Human factors need to be analyzed when validating biometric technologies. How a biometric sample is collected, and the resultant quality of that sample, is directly related to the experience of the user during capture and the performance of the system. For example, will users know when a biometric collection process has started and ended? Will they clearly understand their role in the process? Will they perform the expected action adequately enough for the collection of a quality sample? For one of our clients, we helped assess multimodal biometric systems deployed in a harsh outdoor environment. The analysis included weekly test increments with configurations that analyzed user behavior while interacting with unique biometric hardware devices across varied
pedestrian traffic flows. The overall experiment ran for 3 months with weekly biometric capture modes (e.g., face only, iris only, face and iris) and a rotation of vendor solutions to ensure data coverage and fairness. These weekly cycles assessed numerous aspects of biometric technology including but not limited to population statistics, traveler demographics, time of day data, weather conditions, device timings, impacts of habituation, subject gaze, occlusions, background faces, image attributes, placement and orientation of hardware, and queue management.

Many of our clients continuously monitor biometric matching performance to not only improve operations but to also improve the underlying algorithm. This has led to a substantial reduction in initial gaps in matching across age, gender, and nationality. Consistent statistical testing bolsters performance thresholds and minimizes the impact of racial or gender bias. There is also a need to conduct manual reviews of data to confirm algorithm performance and to better understand false match and false non-match results.

Participants in the biometrics space should also be encouraged to share data analysis and scientific research to collectively improve the biometrics industry. For example, CBP is partnering with NIST to perform independent analyses of face matching performance including the potential impact of traveler demographics and image quality. In addition, CBP is working with the DHS Science and Technology Directorate to evaluate overall effectiveness of facial algorithms.

**Topic 3: Security considerations associated with a particular biometric technology**

Unlike other forms of sensitive information (e.g., financial information, health information, login information) that travels the web, biometric information is rather immutable and limited in options and entropy. In addition, in today’s age of cloud and edge computing, personal information may be distributed widely and outside the control of the end user. The use of biometric information in today’s age requires stronger safeguards in all stages of the data lifecycle (i.e., collection, storage, distribution, in motion, and at rest) to maintain privacy and security. In many instances, biometric data is protected using proven industry data protection methods such as secure transport technologies and encrypted data formats.

Even with these traditional controls, biometric technology poses unique challenges for security. This includes the advent of synthetic identity, spoofing techniques against recognition, and other approaches to defeat the deduplication algorithm commonly used by biometric technology. For example, a common spoofing technique is utilizing someone else’s biometric data to perform actions on their behalf or to gain access to systems or facilities. These use cases are not just rudimentary exploits such as the infamous gummy bear fingerprint hack. As AI technology advances, the threats within the biometric space increases exponentially. New attacks may use deep fake video for authentication or employ photo morphing techniques to inject fraudulent root identity data, posing new challenges that traditional IT security approaches can’t easily solve. For Presentation Attack Detection (PAD) on mobile devices, there are solutions utilizing both active and passive analysis of the user and their environment. This includes approaches such as eye tracking of dynamic content, background movement analysis, reflectivity, multispectral analysis of the face, and other technologies to determine if the user is live and in person. Traditional biometric systems have required users to perform actions in attended modes (i.e., an operator directly assisting the user during biometric capture), either for security reasons or simply because
the process was unfamiliar. As mobile phones have advanced, biometric operations are now in the hands of the user (i.e., unattended) and evolving into the wild. Remote enrollment systems and similar unattended use cases introduce new attack vectors that will need to be tracked and mitigated. As commercial entities such as Apple, Samsung, and Google embrace biometric use cases, will their implementations be trusted and leveraged for official government business?

Dignari’s long-standing work in biometrics across clients has focused on building robust safeguards for security and privacy, using instruments of policy, technology design, data protection, and operational control. We have been involved in several significant technical security and policy roles since CBP inherited the biometric entry/exit mission in 2013. When CBP began testing biometrics at airports in 2016, the Dignari team opened the lines of communication to engage with both internal and external biometric entry/exit stakeholders in cybersecurity, civil liberties, and information privacy to seek input from the community and share facts about the program. Supported by Dignari privacy Subject-Matter Experts (SMEs), CBP coordinated several outreach events with privacy and civil liberties advocates as well as the Privacy and Civil Liberties Oversight Board. In addition, our SMEs engaged Privacy Offices within CBP and DHS Headquarters in drafting multiple Privacy Threshold Assessments (PTA), Privacy Impact Assessments (PIA), Privacy Notices through Privacy Act Statements (PAS), signage at affected facilities, verbal announcements, and tear sheets with frequently asked questions, as well as language for the relevant public websites.

**Topic 4: Exhibited and potential harms of a particular biometric technology**

One harm that may not garner as much attention is participatory bias. This is where technical, environmental, and/or operational limitations may unintentionally exclude certain populations from taking advantage of biometric technology benefits or worse, introduce extraneous processing or negative experiences for the participant. For example, elderly individuals may not be able to perform necessary capture operations such as placing arthritic fingers on a flat platen. Operational or environmental constraints such as fixed infrastructure, may prevent exceptionally short or tall people from having an optimized facial image captured. Physical disabilities or accessibility issues may prevent someone from interacting with a particular biometric device. Many issues can largely be overcome by solution design and thoughtful analysis in the pilot stage, but awareness is key.

**Topic 5: Exhibited and potential benefits of a particular biometric technology**

There are many potential benefits of utilizing biometric technology. This section will explore those benefits by user, covering system implementers, government system owners, and end users. By examining the benefits by user, we can identify the success of biometric technology use cases.

For system implementers such as airlines and airports, they have the potential to modernize their processes without unduly burdening their customer. Current processes and infrastructure may be unable to sustain air-travel given the projected increases in the quantity of passengers. A facial biometric system can minimize the burden on existing processes and systems while increasing convenience for the passenger. Unlike fingerprinting or other more intrusive biometric modalities, a facial capture is all that is required to verify one’s identity and create a better user experience for
all parties. Additional benefits at the airport could also be enabled for a full curb-to-gate touchless experience while maintaining a more secure and sterile environment for travelers.

For government system owners, overall security can be improved by automatically confirming known identities using biometrics. This minimizes an operator’s time spent verifying individuals and increases their time to focus efforts on higher risk populations, edge cases, and exceptions. For example, a biometric entry-exit system can effectively combat attempts by foreign national terrorists to circumvent border checkpoints. This is done by providing an accurate way to verify an individual’s identity using biometrics and minimizing the unlawful entry using false identity documents. Establishing such a system is crucial to our efforts to respond to the continuing threat of global terrorism. The increasingly sophisticated features in modern passports have led to the increased use of legitimate documents by imposters. Today, those seeking to evade detection by CBP, or other border security services frequently use a non-altered travel document legitimately issued to another person. The best tool to combat this fraud is to biometrically verify that a person who presents a travel document is the true bearer of that document. Using a biometric verification system, CBP can update the border crossing records of foreign nationals and provide greater assurance that the government will be able to identify imposters during future encounters.

For end users there are also benefits of particular biometric technologies. Face recognition systems provide an easy-to-use, more convenient interface that expedites interactions between an individual and the system. As biometrics continue to gain momentum in the private sector, additional benefits are realized such as paying for mobile food orders using Apple Face ID. There are also additional use cases across sectors that open the possibility of benefits for face recognition. From detecting mental stress and depression to helping those with Alzheimer’s recognize photos of friends and family, face recognition offers new and innovative ways to interact with the world around us.

Topic 6: Governance programs, practices, or procedures applicable to the context, scope, and data use of a specific use case

(a) 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;

Stakeholder engagement is critical for any emerging technology implementation, especially biometric technologies. Stakeholders should be viewed across a wide swath of communities, both internal and external. External stakeholders should include those with direct domain knowledge such as industry consortiums, national and international standards bodies, academia, as well as technology product and service providers. It should also include indirect communities who may be impacted or play a role in system implementation such as the public at large, privacy advocates, and the media. Internal stakeholders should cover the gamut of support operations needed to field successful biometric implementations. This includes business/mission owners, program management, acquisition, budgeting, technology implementers, infrastructure and hosting providers, UI/UX designers, security and privacy groups, public affairs, testing
organizations, application developers, and many more. Each must understand the unique aspects of biometric implementations and adhere to overarching security and privacy requirements. Leaning more toward a transparent and collaborative stakeholder engagement model not only keeps everyone informed but also allows each entity to feel invested in the success of the project. Stakeholders should be engaged at the onset of biometric technology implementation and work together with the delivery team from initial proof of concept, through field pilots, into production, and throughout scaled enterprise operations and maintenance.

(b) Best practices or insights regarding the design and execution of pilots or trials to inform further policy developments

Dignari has significant experience in planning, conducting, and analyzing biometric pilot studies across a range of government sponsors. When conducting pilots or trials it is important to define goals and objectives and to identify measures of success. Understanding what is being tested, and what is hoped to be gained because of the test, should inform how you plan, design, and ultimately conduct each pilot. With this baseline understanding of what is being evaluated, it is then possible to work backwards to define the minutiae of the pilot including evaluation criteria, target populations, deployment locations, pilot phases and duration, and overarching test methodologies to collect relevant data. When utilizing biometric technologies, pilots should be as close to real operations as possible. Users should be representative of a diverse user population and interact with the system consistent with the expected end state. While it may not be possible to fully mimic the end state for each pilot, the goal should remain to be as close as possible. Pilots may be conducted one at a time or incrementally with adjustments to functionality analyzed after each iteration. Regardless of the frequency or duration, each pilot should feed into a larger vision of the organization’s biometric operations and inform future work. Additionally, output and findings from the pilots should be shared with relevant stakeholders throughout the process and tracked over time in a centralized and open repository so they may be referenced and used as inputs for future projects.

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

Data collection should include processes and procedures related to individual participation. For example, U.S. Citizens who do not wish to have their photos taken during international travel can request alternative processing through government officials or other stakeholders. It’s common for most government biometric systems, especially pilot systems, to employ opt-in procedures and alternative processing for those who do not want to participate in the system. These alternate processing guidelines are typically published in standard operating procedures.

To help inform these decisions, biometric system owners should document and publicize intended use of biometric data including retention policies. Many U.S. Federal government biometric programs notify the public using PIAs, System of Record Notifications (SORNs), and through program information such as Frequently Asked Questions readily available via public websites. For example, DHS has published more than 10 PIAs on their Biometric Entry/Exit program to explain all aspects of the program including policies and procedures for the collection, storage, analysis, use, dissemination, retention, and deletion of data.
Data storage and retention should be minimal and focused solely on time frames of valid use within the system and for particular use cases. Foundational biometric data should have documented procedures for data lifecycle management from initial identity creation through deprovisioning and account termination. Functional biometric data, collected at the time of an encounter with the system, should only be stored for specific purposes such as ongoing system performance analysis or evidentiary reasons. For one-to-many identification scenarios, biometric galleries should be limited to the specific target population and ideally remain ephemeral for that particular use.

As an example of proper and tailored data processes and storage, an organization may reduce the retention period of certain protected populations to no more than 12 hours after identity verification and only for continuity of operations purposes. Facial images of other populations within the system may be retained for up to 14 days in secure systems to support system audits and to evaluate facial recognition performance. Longer term storage to comply with relevant laws and regulations may also be implemented and socialized using SORNs.

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

Safeguards and limitations of approved use should be specifically documented and agreed upon by all stakeholders. For example, business requirements should not allow approved partners or biometric vendors to retain the photos they collect under a government process for their own business purposes. The partners must immediately purge the images following transmission to government systems, and the partner must allow audits to ensure compliance. If there are stipulations where images may be used for ongoing analysis, those should be identified, documented, and publicized accordingly with controls in place to anonymize the data as much as possible. If data is to be shared between government organizations for research and analysis, Memorandums of Understanding (MOUs) and Interconnection Security Agreements (ISAs) may be necessary to safeguard the data. Strong encryption should be used to transfer the data between the capture device, local or backend matching services, and relying systems, as well as for data at rest. Image data should be minimally stored due to security and privacy reasons. When possible, biometric templates instead of images should be used to limit the possibility of reuse or theft of root biometric data. Only authorized government personnel and authorized representatives of approved government partners should have access to physical devices like cameras. Separation of duties and role-based access control should also be defined for each system component including central data repositories.

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

Performance auditing and post-deployment impact assessments should be standard practice that provide maintenance activities of biometric system implementations. Beyond performance analysis of biometric matching algorithms, it's important to also audit processes and user behavior. This includes analyzing the effects of habituation over time to determine if users are effectively interacting with the system or if something needs to be tweaked before abandonment becomes an issue. System timing metrics should be reviewed at a granular level to understand how long each event takes to identify gaps in performance and opportunities for optimization.
Metrics should be compared to baseline numbers captured prior to deployment and tracked over time to identify anomalies and issues. These analyses should not be performed in a vacuum rather they should be socialized with relevant stakeholders and collectively assessed for future configuration changes or modifications. Additionally, the relevant privacy offices should continually evaluate programs to ensure that all parties maintain required privacy protections.

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

Dignari has performed preliminary research and analysis of potential surveillance camera-based face recognition solutions. This includes using face biometrics to detect and identify individuals as they move through a secure space. While there have been studies in the past such as the NIST Face In Video Evaluation (FIVE)\(^1\), questions remain as to the accuracy of these systems given substandard cameras, suboptimal mounting locations, prevalence of occlusions, and overall poor biometric capture environments. Biometric technologies used in conjunction with surveillance systems also introduces a unique conundrum—if a match isn’t detected does that mean the system isn’t working or just that a targeted individual wasn’t present? For example, a system may be deployed in a public area to check live faces against a watchlist of known criminals. If at the end of a period no criminals are detected, how do you know whether the system malfunctioned or if no criminals happened to walk through the capture zone? There continues to be significant academic research into surveillance-based face recognition capabilities and more generally of face recognition in challenging environments.

(g) Practices or precedents for the admissibility in court of biometric information generated or augmented by AI systems

Dignari does not have relevant experience to add for this item.

(h) Practices for public transparency regarding: Use (including notice of use), impacts, opportunities for contestation and for redress, as appropriate

In all biometric systems that Dignari has supported, public transparency and notice of use have been central to the ultimate success and acceptance of the biometric technologies. Identification and documentation of how the biometrics of system users will be utilized should be conducted early in the project/program lifecycle and revisited throughout. Many times, this is addressed in PIAs, SORNs, and other open publications. As solutions mature and near piloting or production deployment, public relations efforts should be used to further inform the public of how the biometrics will be used as well as their opportunities for contestation and redress. Signage, tear sheets, and other communication methods should be deployed to areas where biometrics are being actively captured. These should be easy to understand, accessible, and offer information regarding alternate processes available.

\(^{1}\) https://www.nist.gov/programs-projects/face-video-evaluation-five