MITRE Response to the Office of Science and Technology Policy's Request for Information on Public and Private Sector Uses of Biometric Technologies

January 14, 2022

For additional information about this response, please contact:
Duane Blackburn
Center for Data-Driven Policy
The MITRE Corporation
7596 Colshire Drive
McLean, VA 22102-7539

policy@mitre.org
(434) 964-5023

<<This page is intentionally blank.>>

About MITRE

The MITRE Corporation is a not-for-profit company that works in the public interest to tackle difficult problems that challenge the safety, stability, security, and well-being of our nation. We operate multiple federally funded research and development centers, participate in public-private partnerships across national security and civilian agency missions, and maintain an independent technology research program. Working across federal, state, and local governments—as well as industry and academia—gives MITRE a unique vantage point. MITRE works in the public interest to discover new possibilities, create unexpected opportunities, and lead by pioneering together for public good to bring innovative ideas into existence in areas such as artificial intelligence, intuitive data science, quantum information science, health informatics, policy and economic expertise, trustworthy autonomy, cyber threat sharing, and cyber resilience.

MITRE does not produce or sell biometric technologies, nor competes to operate systems, but does have a long history of providing data- and evidence-driven support to federal agencies in the areas of biometric research, development, testing, and evaluation; system prototyping and design; acquisition guidance; and operational policies. We focus on providing accurate, unbiased, information and guidance without attempting to influence decisions to any particular outcome. MITRE also occasionally performs independent research on priority biometric issues that lack private sector motivation or ability. MITRE's Duane Blackburn also previously worked at the Office of Science and Technology Policy (OSTP) for eight years, across two administrations, where one of his duties was coordinating interagency activities on biometric technologies.

Introduction and Overarching Recommendations

Biometric technology is a powerful tool that can be used to achieve many positive outcomes or could also lead to harms if used incorrectly—this has led to much debate within the policy community. Biometrics are also incredibly complex and nuanced, which has led to a staggering volume of mis- and disinformation from those seeking to influence the policy community. Effective biometrics policies and regulations must be based on data, evidence, and experience. Yet, many of the nation's policy actions and proposals on biometric technologies have been driven by advocate messaging (both for and against) or inaccurate analyses that mistakenly conflate biometrics with other technologies, fail to differentiate between algorithms and systems, or fail to recognize the breadth and depth of existing technical and operational analyses, evidence-based policies, and national and international standards and best practices. Within this response, MITRE provides unbiased recommendations and insights on biometric technology and policy considerations so that OSTP has an accurate, unbiased, foundation on which to review Request for Information (RFI) responses and determine their subsequent actions. MITRE stands ready and willing to assist and advise going forward, as OSTP deems appropriate.

OSTP and the National Science and Technology Council (NSTC) have a long and distinguished history leading federal and national efforts on biometric technology. The NSTC Subcommittee on Biometrics and Identity Management (BIdM) led efforts far beyond the NSTC norm of coordinating research and development activities by also tackling other important issues such as terminology, standards development, privacy practices, public education, and public-private collaboration.[1] Even though this Subcommittee expired approximately ten years ago, its interagency members continue to gather throughout the year to exchange information and provide mutual mentoring, to host the government's annual identity conference, and to collaborate on special projects. Going forward, MITRE strongly recommends that OSTP leverage these prior and ongoing activities, existing policies, and experienced interagency personnel within their biometrics efforts.

Overarching Recommendation #1: Follow NSTC policy and international vocabulary standards. This RFI's definition of biometrics does not align with existing NSTC policy or international standards, which will create confusion, complicate policy analyses, and likely lead to incorrect policy decisions.[2] It intermingles (identity) biometrics with inference of emotion/intent and in a couple of occasions also folds in the biological and medical community's use of the word "biometrics" (to generically describe any biological-based data). Those are three different categories of technologies/issues that have different backgrounds, uses, and operational considerations and should have distinct policy analyses. To ensure clarity and to promote proper analysis, all references to biometrics in this MITRE response are limited to identity matters and discussion of other topics will specifically state so without using that term.

Policy matters for biometric technologies was also a focus for OSTP in the years following the 9/11 terrorist attacks. Complicating factors at that time were insufficient knowledge about these then-new technologies and inconsistent use of terms, which led to conflating different technologies and risks. NSTC BIdM attacked this problem, in part, by developing a *Glossary* document, and an aspect of its approval by parent NSTC Committees included direction to federal entities to consistently align with these definitions within their future activities and materials.[3,4] For the most part, federal agencies have done so for the past fifteen years, and the NSTC's *Glossary* document later served as a reference input in the development and updates of international biometric vocabulary standards.[5]

Overarching Recommendation #2: Ensure policy decisions are evidence- and science-based. MITRE strongly recommends that OSTP's biometric activities be based on reasoned analysis of data and evidence, as intended by the *Foundations of Evidence-Based Policymaking Act of 2018* (P.L. 115-435) and called for in the NSTC's *Protecting the Integrity of Government Science*.[6,7]

Much of the national conversation today *against* biometrics resembles the conversations *for* them twenty years ago: driven not by data and evidence but rather on misguided assumptions of their capabilities and Hollywood-inspired visions of operational systems that use them. A large

[1] Blackburn, Duane and Garris, Michael. A National Science and Technology Council for the 21st Century. 2021. MITRE, https://www.mitre.org/sites/default/files/publications/pr-21-2388-national-science-technology-council.pdf.

[2] ISO/IEC 2382-37:2017 Information technology — Vocabulary — Part 37: Biometrics. 2017. ISO, https://www.iso.org/standard/66693.html. Last accessed January 8, 2022.

[3] This Glossary is available within the Subcommittee's compendium document Biometrics "Foundation Documents" at https://apps.dtic.mil/sti/pdfs/ADA505048.pdf, page 24.

[4] At the time this Subcommittee reported to both the NSTC Committee on Technology and the NSTC Committee on Homeland and National Security. The Subcommittee was shortly thereafter rechartered as the Subcommittee on Biometrics and Identity Management, reporting solely to the NSTC Committee on Technology.

[5] ISO/IEC 2017.

[6] Foundations for Evidence-Based Policymaking Act of 2018. 2018. United States Congress, https://www.congress.gov/115/plaws/publ435/PLAW-115publ435.pdf.

[7] Protecting the Integrity of Government Science. 2022. The White House, https://www.whitehouse.gov/wp-content/uploads/2022/01/01-22-Protecting_the_Integrity_of_Government_Science.pdf.

portion of current policy analyses and news articles on this topic are not accurate, rendering subsequent recommendations or actions based on them to be flawed. Unfortunately, it appears that some of the discussion and questions in this RFI have been influenced by these faulty analyses. "When bad information becomes as prevalent, persuasive, and persistent as good information, it creates a chain reaction of harm."[8]

Biometric technologies and the systems that use them are very complex and nuanced, making it difficult for well-meaning but inexperienced entities to develop accurate analyses. There are also several entities that appear to be much more driven to *influence* audiences (both for and against biometrics) rather than to *inform* them in an accurate and non-biased manner.[9] While this has disappointingly become commonplace for many debatable topics within the current national environment, these works are in many cases driving the modern policy dialogue on biometrics. Reasoned analysis and policy decisions, based on data and evidence, prevailed twenty years ago. It must similarly prevail today as well.

Overarching Recommendation #3: Biometric policy decisions need to be specifically focused and nuanced. There are multiple biometric modalities (face, finger, and iris recognition being those predominantly used by federal agencies, with rapid DNA growing) and several existing and potential use cases—with all having unique technical, operational, and policy considerations. Analyses or policy decisions that are proper for one modality and one use-case are most likely inaccurate for others. OSTP's future work must therefore be specifically focused to be accurate. Relatedly, policy analysis on attribute and cognitive or emotional state inference technologies will be decidedly different than for biometrics, and the same holds true for biological and medical data. There will be some overlap of concerns, and maybe even a few aligned best practices, but wholesale conflation of the different capabilities must be avoided.

Questions Posed in the RFI

2. Procedures for and results of data-driven and scientific validation of biometric technologies...

Biometric technologies have a long history of being subjected to scientific evaluation and held to high academic rigor.[10,11] There are several active academic conferences and journals dedicated to the development and testing of biometric systems.[12,13] Biometric examiners can also achieve

[8] Commission on Information Disorder Final Report. 2021. Aspen Institute, https://www.aspeninstitute.org/wp-content/uploads/2021/11/Aspen-Institute_Commission-on-Information-Disorder_Final-Report.pdf.

[9] D. Blackburn, Two National Academies Recs for NIST Have Value for Wider R&D Community. 2021. https://www.linkedin.com/pulse/two-national-academies-recs-nist-have-value-wider-rd-duane-blackburn/. Last accessed December 7, 2021.

[10] Overview of the NIST Face Recognition Vendor Test, from 1994 to present. https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt Last accessed December 22, 2021.

[11] For instance, the IEEE Biometrics Council, https://ieee-biometrics.org. Last accessed December 22, 2021.

[12] For instance, the IEEE Biometrics: Theory, Applications, and Systems conference. Last accessed January 6, 2022.

[13] For instance, the IEEE Transactions on Information Forensics and Security routinely accepts biometrics papers. https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=10206 Last accessed January 6, 2022.

professional certification.[14], One can even earn accredited academic engineering degrees in biometrics.[15]

Properly designed and implemented evaluations have played significant roles in the further development of multiple biometric modalities and in planning their use in federal (and other) operations. The two largest current issues in biometric evaluations are below:

- A community-wide lack of explaining evaluations to non-expert audiences so that the results and their relevancies are generally understandable. This results in external entities picking up the slack to explain the findings, even if they do not have the knowledge, insights, or desire to do so accurately.
- An increasing number of biometric evaluations (usually performed by entities advocating for or against the technology) that do not follow international biometric evaluation standards and/or fail to meet minimum statistical significance requirements, yet nonetheless are embraced and promoted in news articles or policy analyses and recommendations as providing "scientific evidence" about biometric technology.[16]

The NSTC BIdM previously produced a paper, *Biometric Testing and Statistics,* to explain key concepts, procedures, and metrics to the public.[17] More recently, the FedID document *Biometric Face Recognition: References for Policymakers* similarly provides introductory and intermediate overviews of testing and evaluating biometric technologies specifically for legislators and policymakers.[18] The NSTC BIdM also drove U.S. engagement with the international community to develop and refine international standards for biometric testing, which includes principles and frameworks, methodologies for the three types of performance evaluations, modality-specific testing, and quantifying performance variation across some demographic groups.[19] MITRE strongly recommends that OSTP, and others interested in this topic, study these papers and standards. Summaries of key takeaways are described below.

Biometric Evaluation Axiom: Different types of evaluations provide different insights.
Corollary: Improperly taken "insights" are usually inaccurate.

Biometric algorithms and other system components, as well as human-system interaction, must be extensively tested to identify necessary future research, to inform decisions while planning operational systems, and to monitor operational performance. The international biometrics community has long coalesced around three types of evaluations, with each serving a different purpose. It is critical for policymakers to understand the differences among the three and how to properly consider their results.

[14] For instance, the Latent Print Certification from the International Association for Identification, https://theiai.org/latent_requirements.php, Last accessed December 22, 2021.

[15] For instance, West Virginia University Biometric System Engineering: https://admissions.wvu.edu/academics/majors/biometric-systems-engineering.

[16] ISO/IEC 19795-1:2021, Information technology — Biometric performance testing and reporting — Part 1: Principles and framework. 2021. International Organization for Standardization, https://www.iso.org/standard/73515.html. Last accessed December 7, 2021.

[17] This document is available within the Subcommittee's compendium document Biometrics "Foundation Documents" at https://apps.dtic.mil/sti/pdfs/ADA505048.pdf, page 149.

[18] Biometric Face Recognition: References for Policymakers. 2020. FedID, https://www.mitre.org/sites/default/files/publications/biometric-face-recognition-references-for-policymakers.pdf.

[19] Standards by ISO/IEC JTC 1/SC 37. 2021. ISO, https://www.iso.org/committee/313770/x/catalogue/. Last accessed December 21, 2021.

- Technology Evaluations assess the abilities of biometric recognition algorithms only; they do not evaluate other components that are necessary in operational systems. They typically involve massive numbers of subjects in standard data sets so that performance variation across different algorithms can be measured and compared. Results from these evaluations are used to identify areas that require additional research or as a first step in selecting an algorithm for operational use. Highlighting any result from a technology evaluation and claiming that to be the expected outcome within an operational system will almost always be incorrect.
    - The National Institute of Standards and Technology's (NIST) biometric technology evaluations are considered the gold standard of biometric technology evaluations.
    - Testing organizations must carefully consider the makeup of test data to ensure it can provide accurate and useful evaluation results. Reproducibility requires datasets that are publicly available and/or available via data sharing agreements. Results from evaluations that use vendor or advocate datasets that are not openly shared are suspect.
- Scenario Evaluations enable initial assessments of how a full biometric system (which includes a biometric recognition algorithm as one of several of its components) will perform in a *specific* use case. A mock-up of the anticipated operational environment is created, and humans are used as live subjects throughout the evaluations. Scenario evaluations involving multiple different systems would have the same environment and subjects, but they would receive their own input data from the live subjects.
    - Results from scenario evaluations offer a good understanding of how an individual system will operate in the real world for that one specific use case and population, thus providing potential operators input on selecting systems and establishing operational procedures. Different systems will likely have different results for the same use case and results for one system will vary from one use case or population to another; assumptions that other systems will perform the same as the tested system, or that the tested system will perform similarly in different use cases, will usually be inaccurate. The DHS-sponsored Maryland Test Facility's Biometric Technology Rallies are examples of scenario evaluations.[20]
- Operational Evaluations are evaluations of a specific system in a specific use case while it is in use. They do not usually measure accuracy directly (though it can sometimes be feasible), but rather analyze other factors such as cost, workflow impact and user experience. Results from operational evaluations are typically used to enhance procedures within the operational system. Annual reports on usage and timing from the major biometrics systems are examples of operational evaluations that are performed continually. U.S. Customs and Border Protection has performed several operational evaluations, for example.[21]

[20] Biometric Technology Rally. 2021. Department of Homeland Security, https://www.dhs.gov/science-and-technology/biometric-technology-rally. Last accessed December 13, 2021.

[21] M. Mason. Biometric Breakthrough - How CBP is Meeting its Mandate and Keeping America Safe. 2021. U.S. Customs and Border Protection, https://www.cbp.gov/frontline/cbp-biometric-testing. Last accessed December 13, 2021.

Biometric Evaluation Axiom: Evaluations must meet statistical significance requirements and be sufficiently documented to be repeatable. *Corollary: Evaluations that do not meet these requirements should be ignored.*

Properly measuring the accuracy of a biometric recognition algorithm or system in a nonbiased and statistically significant manner is complicated, time-consuming, and costly. Parameters that may at first seem inconsequential can have significant ramifications, leading to incorrect results. National and international standards for biometric performance testing and reporting should be followed with any deviation from the standard being documented in detail. The reliability of results from evaluations that do not follow these standards are highly suspect.

Evaluation protocols must be precisely designed to ensure accurate and nonbiased results. One major consideration is the makeup of the test database, which must be studiously developed to produce accurate evaluation results. (A dishonest evaluator can produce whatever result desired by improperly modifying the makeup of the database and system parameters.) Evaluations must also be thoroughly documented so that external entities can repeat the evaluation and receive statistically similar results. There have unfortunately been a few widely-referenced evaluations that failed these requirements—anyone with biometric knowledge could easily tweak their parameters in ways that nonexperts wouldn't see to produce wildly better or worse outcomes.

All evaluations, including those of biometric technologies, must follow common statistical significance requirements. Otherwise, the results may not be trustworthy. For biometric evaluations, the fidelity of the accuracy measures depends on the numbers of individuals used and comparisons made. Evaluations with higher numbers of individuals and comparisons will provide more precise results. Evaluations with only a few dozen individuals or comparisons often have high error variances, making their measurements (and any analyses based on them) suspect. Biometric modalities used in major federal government systems (such as fingerprint, face, iris, or DNA) now have such low error rates that evaluations must have massive numbers of test subjects and comparisons to reach statistical significance.

Biometric Evaluation Axiom: Evaluation metrics will vary based on the type of evaluation (technology, scenario, and operational) AND the operating mode of the biometric. *Corollary: The metrics for each are not interchangeable, and trends seen in one metric do not always hold for others.*

Biometric systems function in one of three different modes, as discussed below:

Verification, where there is a 1:1 comparison of the live subject to their claimed identity in the system. A conceptual example is when a foreign national enters the United States, his or her face may be compared against a visa photo to verify that the traveler is indeed who he or she claims to be in their travel document.

- There are a few different acceptable metrics for verification (based on evaluator's preference), though all are mathematically linked and can be derived from one another.
- Any test reporting a true match rate must also report a corresponding false match rate (or false accept and false reject rates). It is trivial to adjust system parameters to produce a desired outcome for only one rate but doing so also usually causes the corresponding rate to fall into unacceptable ranges. Any statement that only lists one such metric, without its corresponding metric, is completely useless information.

Closed-set identification (1:many), where all potential subjects are known to be in the database and the system works to properly find them. A conceptual example is checking identities within a confined facility such as a correctional institution. An issue for awareness is that while this is the easiest evaluation to perform (and does provide useful insights), there are relatively few operational activities that function in this mode.

- In some closed-set applications, systems are setup without a threshold setting so systems will return the ‘best’ candidate, regardless of how confident the system is in this match.

Open-set identification (1:many), where the system attempts to see if a subject is in the database. Conceptual examples include checking for duplicate drivers’ licenses or to identify a criminal suspect. An issue for awareness is that this is the most complex mode to evaluate, as it contains considerations and issues found while evaluating both verification and closed-set identification.

- Note that there is no “biometric surveillance” function, despite how often it is discussed in policy advocacy materials. Widespread surveillance is a use-case, much more discussed in theory than found in actual operation, which leverages multiple interconnected biometric systems performing open-set identification functions.

Acceptable accuracy metrics for each function are different, and measured accuracy trends within one function do not necessarily show up similarly for the other two functions. This is both a statistical issue as well as one of terminology, with non-experts incorrectly conflating statistical metric nomenclature across the functions. The previously mentioned NSTC BIdM and FedID documents explain proper metrics for each in detail.

3. Security considerations associated with a particular biometric technology…

The IT security implications of the collection, storage, and utilization of biometrics data have been well understood by the community for many years. MITRE is therefore instead predominantly focusing on the new risks associated with genomics data at the intersection with modern medical practice in answering this question.

In general, the deployment of computational artificial intelligence has highlighted deficiencies in consideration of the ethical applications of the technologies utilizing them. In many cases, fundamental principles of the ethical treatment of persons were not considered, which was originally described as the principles of “respect for persons” and “do no harm” in the Belmont Report.[22] MITRE recommends the implementation of a holistic ethics assurance approach that prevents the violation of ethical rights and requires the development of a lifecycle ethical analysis process to achieve equitable and actionable ethics within AI applications.

In recent years, various technologies have expanded the depth and breadth of analyses that can be applied to personal information, presenting means to collect and extract more useful information while diminishing the anonymity and privacy that once existed within the data. The expansion of technologies for evaluating identity, ancestry, and health come with the downstream concerns of the equitable and protected collection, storage, and transmission of this data. Differential privacy considerations and tradeoffs should be reviewed with each technological advance to ensure balance of information privacy and information utility. The

[22] The Belmont Report. 1979, Department of Health, Education, and Welfare, https://www.hhs.gov/ohrp/sites/default/files/the-belmont-report-508c_FINAL.pdf.

utility of genomic information with current technologies could pose potential for longitudinal privacy leakage as new technologies come online and leverage the data in unanticipated ways. An example is the identification of individuals thorough the genetic markers of related individuals, extending to multiple generations of relatives beyond the originating genome.

The development of mechanisms and technologies to safeguard these types of sensitive information must be considered and preemptively developed in parallel to the emerging technologies, assuring the protection of the rights and privacy of individuals. Expansion of technologies to leverage advances in genomics and molecular biology have opened the use of these data for identification of individuals and provides an example of exposure risk for personally identifiable information (PII). The collection of genomics data for precision medicine techniques provides a risk for the use of these data in a changed context. The same genomics data collected for medical applications such as cancer detection and characterization contain identifiable genomic markers of identity. While these data are expanding in popularity and utility in the commercial and healthcare spaces for determining ancestry and evaluating health risks, the individual is often required to weigh those benefits of precision medicine against the risks of forfeiting their privacy; moreover, the individual may not even be aware of these privacy risks.

The security of digital genomic data poses a long-term sensitivity for the information contained within it. Unlike most types of PII, the genome of an individual is relatively immutable, remains uniquely identifiable over the lifespan of the individual, and maintains sensitivity beyond the individual due to intrinsic linkages to relatives and offspring via heredity. Innovative applications for protecting these data largely remain at the academic level and are not yet realized for implementation by commercial entities, the healthcare industry, non-profit organizations, and government agencies.

Within biometric technologies, new advances in contactless fingerprint technologies allow faster and higher-throughput collection but also removes the human operator. This in turn makes operational security more difficult. The *Biometric Presentation Attack Detection Framework* has been developed as a general framework for detecting attack mechanisms for biometric technologies such as spoofing.[23] Additionally, several of the top performing face recognition algorithms have been developed by foreign entities, raising national security concerns.

4. Exhibited and potential harms of a particular biometric technology…

Oversimplified analyses. Many harms often discussed in biometric policy analyses have been based on inaccurate projections. A common example is taking a result from a technology evaluation of an algorithm and assuming the same error rates will occur in an operational system. It is important to realize that biometric systems are *emergent* systems, "where the system's behavior is a consequence of the interactions and relationships amongst its components, rather than the independent behavior of individual elements. Evaluating an operational system's performance thus requires an end-to-end (full system) analysis."[24] Measured algorithm traits from a technology evaluation don't necessarily show up in operational systems (due to actions taken

[23] ISO/IEC 30107-1:2016 Information technology — Biometric presentation attack detection — Part 1: Framework. 2016. ISO, https://www.iso.org/standard/53227.html. Accessed January 7, 2022.

[24] Biometric Face Recognition…, FedID 2020.

from other system components), and if they do, their impact will vary by use case and the algorithms (and other system components) selected.

Bias. One of the most-discussed concerns within policy analyses of biometrics is bias, with nomenclature issues again creating significant confusion. Technical/evaluation bias, operational bias, and prejudicial bias are different things but they are often incorrectly intermingled, which creates misinformation that significantly muddles public debate. For example: a knowledgeable individual could use a biometric algorithm with significant demographic technical/evaluation biases and develop systems that lack prejudicial bias. The same individual could also use an algorithm without measurable demographic technical/evaluation biases and develop a system with significant prejudicial bias. The two biases are not the same, even though they are commonly (and inaccurately) discussed as such in advocacy materials. This issue has been especially profound within third-party analyses of NIST's *Face Recognition Vendor Test Part 3: Demographic Effects* technology evaluation results, leading to inaccurate discussions about the report's results and what they mean for operational systems and policy considerations.[25] Additional discussion on the differences across these types of biases can be found in the MITRE document *When and How Should we "Trust the Science?"*[26] This incorrect conflation of bias terminology is not unique to biometrics, as many artificial intelligence discussions encounter similar issues, for example. MITRE recommends developing explanatory reference material and specific guidance on how to minimize all three forms of bias in biometric (and other) systems and related decision-making processes.

Privacy. The First Amendment includes free speech and free association protections, and the Fourth Amendment protects persons from unreasonable search and seizure. Critics claim biometric systems have the potential to violate First Amendment and Fourth Amendment constitutional protections because they may be used to improperly conduct surveillance activities on law-abiding persons. Legal, privacy, and civil liberties subject matter experts should advise executives, project managers, and developers, about potential risks and how to comply with constitutional, statutory, and regulatory requirements. By providing guidance through the entire project lifecycle, the risk of violating constitutional protections, privacy rights, and civil liberties can be substantially minimized. For additional discussion of privacy considerations of biometrics, please review the NSTC document, *Privacy & Biometrics: Building a Conceptual Foundation*.[27]

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

MITRE is not aware of existing stakeholder engagement best practices that are specific to biometric system design. The Organisation for Economic Co-operation and Development (OECD) recently released a report with numerous issue-agnostic models to consider for policy

[25] P. Grother, M. Ngan and K. Hanaoka. Face Recognition Vendor Test Part 3: Demographic Effects. 2019. National Institute of Standards and Technology, https://doi.org/10.6028/NIST.IR.8280. Last accessed November 23, 2021.

[26] D. Blackburn. "When and How Should We 'Trust the Science'?". 2021. MITRE, https://www.mitre.org/sites/default/files/publications/pr-21-1187-when-and-how-should-we-trust-the-science_0.pdf.

[27] Privacy & Biometrics: Building a Conceptual Foundation. 2006. National Science and Technology Council, https://www.hsdl.org/?view&did=463913.

and public officials to engage with citizens to shape best practices for utilization.[28] MITRE's observation of OSTP's public "listening sessions" supporting this RFI is that the sessions were beneficial in understanding concerns and emotions surrounding these technologies but were lacking accurate and nuanced insights necessary for proper policymaking.

Biometric data is PII and should be collected, stored, and shared in accordance with federal, department, and agency-specific privacy policies and procedures. Biometric specific nuances should be further discussed and will often need to be specific to individual modalities and use cases to be beneficial. Existing reference material to build from include the NSTC's Privacy and Biometrics document, International Biometrics + Identity Association (IBIA) Ethics document, Biometrics Institute's Ethical Principles, and existing international biometric standards from ISO/IEC.[29,30,31]

One of the activities within the NSTC BIdM was to establish a formal interagency process to collectively analyze national and international standards and to select those that will be used in federal biometric systems and processes. As part of this work, the NSTC issued the *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards* (which was later further reinforced by *National Security Presidential Directive 59*) and created the *Registry of US Recommended Biometric Standards.* [32,33,34] Upon expiration of the Subcommittee, the NSTC delegated the responsibility of maintaining the registry to NIST.

Court admissibility of biometric information in courts is dependent on meeting Daubert standard (*Daubert v. Merrell Dow Pharmaceuticals, Inc*., 509 U.S. 579).[35] The Daubert ruling established basic criteria for courts determining whether methodologies are valid to the court (pp. 592-595). MITRE recommends that the OSTP reach out to the Department of Justice, Federal Bureau of Investigation, as they frequently deploy the Daubert standard for court proceedings and have training programs for expert witnesses.

MITRE notes that the use cases and associated usability of biometrics with individuals having disabilities remains a growing and needed area of research to enable the development of mitigation and inclusion strategies.[36]

[28] Chwalisz, Claudia. Eight Ways to Institutionalize Deliberative Democracy. 2021. OECD, https://doi.org/10.1787/4fcf1da5-en. Last accessed December 21, 2021.

[29] Ethics. 2021. IBIA, https://www.ibia.org/policy-advocacy/ethics. Last accessed December 21, 2021.

[30] Ethical Principles for Biometrics. 2019. Biometrics Institute, https://www.biometricsinstitute.org/ethical-principles-for-biometrics/. Last accessed December 21, 2021.

[31] Standards by ISO/IEC… ISO, 2021.

[32] NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards. 2007. White House Office of Science and Technology Policy, https://www.nist.gov/system/files/documents/2017/04/12/nstc_policy_bio_standards.pdf.

[33]Directive on Biometrics for Identification and Screening to Enhance National Security. https://www.govinfo.gov/content/pkg/PPP-2008-book1/pdf/PPP-2008-book1-doc-pg757.pdf. Last Accessed January 07, 2022.

[34] More info available at https://www.nist.gov/itl/iad/image-group/support-registry-us-recommended-biometric-standards. Last accessed January 9, 2022.

[35] Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993). https://supreme.justia.com/cases/federal/us/509/579/. Last Accessed January 07, 2022.

[36] Brink, R and Scollan, R. Usability of Biometric Authentication Methods for Citizens with Disabilities. 2019. MITRE, https://www.mitre.org/sites/default/files/publications/pr19-1396-usability-biometrics-for-disabilities.pdf.