

**Lisa J. Sotro**  
**Chair, DHS Data Privacy and Integrity Advisory Committee**

November 19, 2012

The Honorable Janet Napolitano  
Secretary of the Department of Homeland Security  
U.S. Department of Homeland Security  
Washington, DC 20528

Mr. Jonathan R. Cantor  
Acting Chief Privacy Officer  
U.S. Department of Homeland Security  
Washington, DC 20528

**Re: DHS Data Privacy and Integrity Advisory Committee Recommendations on Privacy in the Department's Collection and Use of Biometrics (Report 2012-02)**

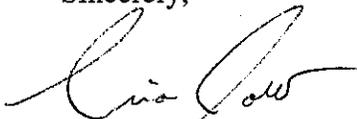
Dear Secretary Napolitano and Mr. Cantor:

It is my pleasure to convey to you the enclosed report that sets forth privacy recommendations for DHS to consider when determining whether the collection and use of a biometric is warranted. The report also contains recommendations for specific privacy protections for DHS to consider when using biometrics for identification purposes. Although the members of the Data Privacy and Integrity Advisory Committee are aware that US-VISIT is DHS's primary provider of biometric identification and analysis services and we are familiar with US-VISIT's robust privacy practices, this tasking allowed us to consider possible ways to improve or expand these privacy practices as additional biometric identifiers are considered by the Department. We are grateful for the Department's cooperation in providing access to important programmatic information and the officials with direct knowledge and expertise on the matter.

We hope you will agree that implementing these privacy recommendations in connection with the Department's collection and use of biometrics will enhance the protection of personal information while supporting the Department's mission.

Please do not hesitate to contact me if you have any questions regarding these recommendations.

Sincerely,



Lisa J. Sotro

Enclosure

cc: Members of the DHS Data Privacy and Integrity Advisory Committee

**REPORT 2012-02 OF THE DATA PRIVACY AND  
INTEGRITY ADVISORY COMMITTEE (DPIAC)  
ON PRIVACY AND THE DEPARTMENT'S  
COLLECTION AND USE OF BIOMETRICS**

**As approved in public session  
NOVEMBER 7, 2012**

In view of the Department of Homeland Security's (DHS or the Department) use of biometric identifiers in certain national security program activities, the Data Privacy and Integrity Advisory Committee (DPIAC) was asked to provide written guidance on privacy best practices associated with the use of biometrics for mission purposes. Specifically, the Committee was asked to consider the following two questions regarding the collection, use, and disclosure of biometric information:

1. What privacy considerations should DHS include in determining if the collection and use of a biometric is warranted?
2. What specific privacy protections should DHS consider when using biometrics for identification purposes?

In developing the Committee's written guidance, members of the Technology Subcommittee heard from representatives from various components within the Department already using biometric identifiers for mission purposes. These include the United States Visitor and Immigrant Status Indicator Technology (US-VISIT), the Directorate for Science and Technology, and the United States Coast Guard.

The following guidance details privacy best practices from across private industry as well as the robust privacy protections already in effect within the Department. This document does not attempt to present a gap analysis for the Department's use of biometrics. Instead, it is our sincere hope that as the Department's use of the technology increases, this report will serve as a practical guidance document for program managers and Department leadership alike as they consider when and how to implement the technology.

## I. Introduction

"Biometrics" refers generally to the science of measuring, recording, and analyzing a person's unique physical attributes. Unique physical attributes, also called "biometric data," can include fingerprints, hand geometry, retina and iris patterns, voice waves, signatures, and facial patterns. In information technology, biometrics typically refers to those technologies using a person's unique physical attributes for identification and/or authentication purposes. Biometric technology has matured significantly since it was conceived, and it is now almost as easy to use a biometric as an identifier as a username and password combination. Because biometric data captures a person's unique and generally unchanging physical characteristics, unauthorized access to biometric data has more potential to cause harm to the individual (as they cannot, in most instances, change those biometric characteristics of themselves like they would change a password). This high level of uniqueness and the immutability of the information cause most privacy experts to consider biometrics as sensitive forms of personally identifiable information (PII). Due to the sensitivity of the data, understanding the need for using biometrics, and protecting the privacy of persons required to submit to biometric technologies, ensuring the security of this data is important.

## II. Privacy Considerations for Biometrics Collection and Use

*Tasking question: What privacy considerations should DHS include in determining if the collection and use of a biometric is warranted?*

When considering the use of biometrics in a specific situation, DHS should take a selective and cautious approach and:

1. Evaluate the usefulness and utility of a biometric method
2. Recognize the potential privacy impacts of biometric use
3. Review program requirements and biometric use
4. Consider the risks and benefits of deploying biometrics

A careful review of the utility of biometrics coupled with their privacy implications can assist DHS in determining whether it is reasonable and cost-effective to use biometrics for a specific system or program. By taking a “hard look” at program requirements and systematically assessing the risks and benefits of biometrics, decision-makers are better positioned to apply them in an appropriate manner.

### Evaluating the Usefulness and Utility of Biometrics

A biometric is a collection of unique distinguishing biological characteristics of a person that can be used to identify them. Some of these characteristics are more generally reliable for identification purposes than others, such as fingerprints (more reliable) and hairstyle (less reliable). Current systems generally employ physiological biometrics, such as fingerprints, iris scans, facial recognition, and DNA profile, so this paper applies primarily to their use.<sup>1</sup> A biometric is most often chosen for a particular application based upon its reliability, cost, community acceptance, and a risk assessment of the collection and storage of the biometric.

Effective biometrics must have five properties: Universality, Uniqueness, Permanence, Collectability, and Acceptability.<sup>2</sup> Various situations may make some of these properties hard to achieve. For example, a biometric that has a slow collection time might be a poor choice at a busy border crossing, or a requirement for face recognition biometrics for international flights might be at odds with some religious customs requiring face covering. The utility of a biometric depends not only on how well it can reliably and uniquely identify an individual (considering whether there are unacceptably high rates of false positives or false negatives), but also on how difficult it is to capture the original sample (e.g., a fingerprint) and the difficulty, reliability, and repeatability of capturing test samples for comparison.

---

<sup>1</sup> There are two basic kinds of biometrics. Physiological biometrics, such as fingerprint, iris scan, DNA, and face recognition, employ a single sample for both capture and verification. Behavioral biometrics, such as signature, gait, and typing, have been in use for centuries and rely on ongoing samples for their continued accuracy.

<sup>2</sup> R. Clarke, “Human identification in information systems: Management challenges and public policy issues,” *Information Technology & People*, 7(4):6-37, December 1994.

The collection and use of biometrics is not a perfect science. Different biometrics and systems have varying rates of success in authentication and identification applications. In their *Guide to Biometrics*, Bolle and others provide two examples that may be helpful.<sup>3</sup> First, suppose airline passengers submit a fingerprint to a database to verify their identity before boarding a plane. If the biometric system has a false reject rate of 3% and 5,000 people every hour request access over a 14-hour day, roughly 2,100 people will require additional screening due to the failure of their biometric to match. Next, suppose a face biometric is used for screening (identifying) people on the no-fly list. If the system has a false positive rate of 0.1% and a database of 25 persons on the no-fly list, then 7 of the 300 people attempting to board a jumbo jet will be falsely matched with one of those 25 persons. The assessment of biometrics' utility for a given application must take their success and failure rates into consideration and include contingencies to handle failures.

Finally, there have always been concerns about the protection of biometric samples from theft or abuse. Due to each person's uniqueness, the use of biometric data and biometric technologies can greatly enhance security.

### Recognizing the Potential Privacy Impacts of Biometrics

Like all other identifiers, biometrics pose a risk to privacy because they facilitate linkage of disparate pieces of data. Perhaps uniquely, biometrics link that data to a person in a way that the person cannot easily break. Some collections and uses of biometrics may create a greater risk to civil liberties than do others. The risks to individual privacy vary according to factors that include:

- Intrusiveness of the collection (DNA swab vs. facial recognition)
- Whether the subject is given notice at the time of collection
- Whether the collection is consensual, mandatory, or effectively mandatory
- Impact on religious tenets against revealing facial and other features
- Uses to which collected biometrics are to be put, and the impact on one's liberty or other activities that results (exclusion from the U.S. vs. secondary inspection in airport vs. denial of a job or other economic benefit)
- Uses to which a collected biometric may be put in the future inadmissibility
- Extent to which the subject can control use of the biometric
- Retention policies, particularly, whether the biometric is retained or whether a numerical rendition or template of the biometric is retained instead
- Protection policies that will be employed to secure the collected biometric sample from modification, replacement, or unauthorized copying
- The chance of error in connection with the use of the biometric, and the opportunity of the subject to correct such errors

Macro considerations also come into play. A database with biometric identifiers of a large class of individuals – say, every person who crosses the border into the United States – can be put to many uses. Interest in such a database would be broad, and managing appropriate access to avoid mission creep would be difficult. As the usefulness of such a database

---

<sup>3</sup> R. M. Bolle, J. H. Connell, S. Pankanti, N. K. Ratha, and A. W. Senior. *Guide to Biometrics*. Springer-Verlag, New York. 2004.

became clear, increasing demands for broadening its application would surely follow. As a result, the scale of a biometrics database can also affect civil liberties on a macro level, suggesting a preference for more limited classes of data subjects wherever feasible.

To the extent they permit a person to distinguish herself from another by authenticating her identity, biometrics can also enhance privacy and civil liberties. Use of biometric identifiers can reduce identity theft that can result in the denial of benefits to a person rightfully entitled to them. Because some biometrics are difficult to forge and cannot be lost or forgotten, many may, in some contexts, prefer their judicious use over other more easily compromised identifiers.

However, researchers have found ways to reconstruct a fingerprint image from the data that is typically stored from processing a fingerprint. They can use that data to create a means of “faking” that fingerprint to obtain a match when presented to a commercial biometric verification system. The research suggests that similar attacks could be mounted using iris scan data and other biometrics. Thus, the long-term protection of biometric samples is now a key part of any biometrics system that must be considered when evaluating the utility of biometrics in any specific application. As discussed above, the immutable aspect of some biometrics, can actually increase security and privacy risks when those biometrics are forged or stolen.

#### Review Program Requirements and Biometric Use

Given context specific success/failure rates, and their inherent privacy impacts, those contemplating the use of biometrics should closely review specific program or system requirements prior to making a decision of whether to use biometrics. The key question is: What is being protected? While the implementation expense and privacy risks associated with biometrics may be rationalized where mission critical or highly valuable assets are to be protected or individual identification may otherwise be especially challenging (e.g., in immigrant, refugee, or transient populations), such a fit is less likely in low-to-medium risk or highly controlled operational situations. Further, the risks associated with the use of biometrics may be lessened where they are used for simple identity verification only, especially when the biometrics data is stored on a card or other device held by the target individual. The context of the program use, the type of the biometric, and the extent to which implementation risks can be mitigated, will help determine whether the benefits are enough to warrant use of biometrics.

A review of program requirements and objectives is necessary to avoid unnecessary cost and risk to both individuals and program missions. In addition to the assets or systems to be secured, decision-makers should also be mindful of cultural factors within their target user community. Generational differences may also have an impact, according to the target community’s comfort with technology and sensitivities regarding privacy. If the use of biometrics will be viewed as unnecessary or intrusive, some alternate means of identification, verification, or authentication should be considered.

Also, because biometrics collection and use require still evolving technologies, any system deployed needs to be able to fail well, in that there must be a contingency plan if it turns

out that the biometric identifier is not as reliable, or the identification technology is not as reliable, as previously expected.

### Consider the Risks and Benefits of Deploying Biometrics

The Department's decision to deploy biometrics should be driven by careful consideration of the long and short-term risks and benefits for both data integrity and privacy, as discerned through a careful evaluation of the potential privacy impacts, the specific program requirements and objectives at hand, and the usefulness and utility of biometrics for the given application. This evaluation should be done in coordination with the Privacy Office, as well as the Office of General Counsel, in order to ensure a thorough review of the privacy impacts and a consistent weighting of those costs across use cases.

The following risk-benefit model is offered to help DHS analyze these factors. In this model, the risk-benefit balance may point to a clear decision of "deploy" or "don't deploy" in some cases. However, other situations demand further review and diligence regarding specific program requirements and objectives and the potential privacy impacts of using biometrics to meet those requirements and objectives. Decision-making for these "gray area" deployments should also consider the potential benefits offered by a scheme involving multiple identifiers, and whether the benefits can be efficiently obtained by using non-biometric identifiers. The analysis should also look for reasonable mechanisms to mitigate risk, prior to making any implementation decision. For example, if a program's requirements can be accomplished with one-to-one matching (e.g., matching of a photo to another specific photo for authentication purposes), instead of one-to-many matching (e.g., matching a photo to a database of photos to identify an individual), then DHS should pursue the one-to-one approach.

In choosing to use and deploy biometrics, the benefits of biometric use (called "Integrity Benefit" and "Privacy Benefit") should typically outweigh the risks ("Integrity Risk" and "Privacy Risk") to that use. Specifically:

$$\textit{Integrity Benefit} + \textit{Privacy Benefit} > \textit{Risk to Integrity} + \textit{Risk to Privacy}$$

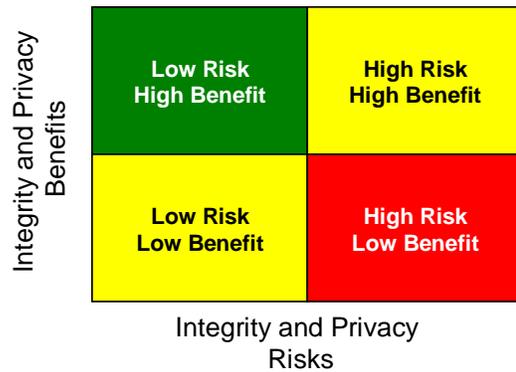
The benefits of biometric use are described as follows:

- Integrity Benefit: The Level of Assurance (LoA) offered by collected biometric, including success/failure rates.
- Privacy Benefit: The degree of biometric uniqueness resulting in a degree of privacy (degree to which the biometric offers security to keep private a respective transaction) \* value of transactions requiring biometric authentication

The risks of biometric use are described as follows:

- Integrity Risk: Harm done if the incorrect person is allowed access or service being granted at enrollment with biometric

- **Privacy Risk:** Potential privacy impacts/harm if DHS has/knows the collected biometric; and the potential privacy impacts/harm if others have/know this collected biometric
- The risk-benefit proposition for biometrics offers several high-level situations (see figure). The risk-benefit analysis may point to a clear decision of “deploy” or “don’t deploy” in some cases. However, other situations demand further review and diligence regarding specific program requirements and objectives. **Deploy:** Integrity and Privacy Benefits clearly outweigh Integrity and Privacy Risks (green).
- **Don’t Deploy:** Integrity and Privacy Risks clearly outweigh Integrity and Privacy Benefits (red).
- **Questionable Value:** Low benefits and risks for both Integrity and Privacy challenge the decision to use this technology (yellow).
- **Extraordinary Circumstances Required:** High risks and benefits for both Integrity and Privacy mandate differentiating circumstances to assume the risks. If the Integrity Risks far outweigh Privacy Risks, and the Integrity Benefits and Privacy Benefits provide a degree of unique identification, consider LoA and security measures to overcome the probability of incurring the Privacy Risks (yellow).



To summarize, biometrics can be an effective tool, in the right circumstances when all stakeholders (including those whose biometrics will be collected) understand their utility, risks, and benefits. DHS must assess their particular circumstances in light of the characteristics and privacy implications inherent to the use of biometrics. Moreover, the data gathered in such a systematic review can be used to help select and implement proper privacy protections where biometrics are deemed to be a good fit for the problem at hand.

### III. Recommended Privacy Protections for Biometric Use for Identification Purposes

In addressing the privacy protections for the use of biometrics for identifications purposes, the DPIAC Technology Subcommittee drew on a previous DPIAC document entitled, “Framework for Privacy Analysis of Programs, Technologies, and Applications” (the Framework), published in 2006.<sup>4</sup> This Framework sets forth five steps for analyzing DHS technologies in light of their effects on privacy interests. This white paper follows the analysis suggested within Step Four of the Framework: Analyze the privacy interests implicated by the program. In this step, the Subcommittee is to analyze the privacy and related interests implicated by the program under study and how they are affected.

<sup>4</sup> Department of Homeland Security, Data Privacy and Integrity Advisory Committee (DPIAC), Report 2006-01 “Framework for Privacy Analysis of Programs, Technologies, and Applications,” adopted March 7, 2006, available at: [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_advcom\\_03-2006\\_framework.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_03-2006_framework.pdf) . See also Department of Homeland Security “Privacy Policy Guide,” 2008-01, available at: [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_policyguide\\_2008-01.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf)

As described in the Framework, this analysis begins with the values that underlie and inform the Fair Information Practice Principles (FIPPs). The original version of the FIPPs (known as Fair Information Practices or FIPs) was developed by an advisory committee commissioned by the Secretary of Health, Education, and Welfare in 1972 to examine the extent to which limitations should be placed on the application of computer technology to record keeping about people. The committee's final report delineated five principles for protecting the privacy and security of personal information; these principles underlie the major provisions of the Privacy Act of 1974 that was passed the following year. A revised version, expanded to eight principles, was developed by the Organization for Economic Cooperation and Development (OECD) in 1980. This version has been widely adopted and is the basis of many privacy laws and related policies worldwide. The FIPPs are not legal requirements but provide a useful framework for identifying, evaluating, and addressing privacy risks. Importantly, DHS has published its own FIPPs, which form the basis of the Department's privacy compliance policies and procedures governing the use of PII. DHS should be commended for its leadership for embracing a more complete set of the FIPPs than have been accepted previously by U.S. government agencies. Each of the DHS FIPPs and its application to the collection and use of biometrics is discussed below, with specific recommendations from the Committee.

*Transparency: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII).*

Under this principle, DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of biometric data. Individuals should know how and why biometrics are used, including what information is collected and by whom. To meet the transparency principle, DHS should:

- Develop a strategy, policies, and procedures to provide adequate notice
- Provide employees with training to ensure adequate notice
- Deploy written notices in different languages
- Use standard images and icons to communicate the use of biometrics
- Audit operational notice processes regularly to ensure that they are consistent with policy

In addition to providing notice to individuals whose biometrics are being collected, DHS should engage in an education campaign regarding the use of biometrics, including why it is necessary and what rights and protections are afforded to individuals who provide their biometrics. Government entities and the public sector often lack a good understanding of how biometrics technologies work and when and how they are best applied. By allowing the program to be open to public scrutiny, understanding, and participation, many of their concerns regarding the use of biometrics in identity systems may be resolved.

*Individual Participation: DHS should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. DHS should also provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.*

Under this principle, DHS should involve the individual in the process of using biometric data and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of that person's biometric data. DHS should also provide mechanisms for appropriate access, correction, and redress regarding DHS' use of a person's biometric data.

Where possible, individuals should have the option not to participate in a program involving the use of biometrics for identification purposes, while maintaining the rights and privileges of other individuals who are participating in a program involving biometrics. In addition, where appropriate, consideration should be given to allow an individual to withdraw consent for DHS to subsequently collect, use, or retain the biometric. When participation in the biometrics program is mandatory to receive certain rights and privileges, the consequences for the individuals' refusal to participate, or withdrawal of consent, should be clearly communicated, as well as the argument for why such participation is mandatory, such as for national security purposes.

It is critical that the program provides due process through redress mechanisms, especially wherever a person may suffer an adverse action or determination. The notice provided prior to the PII collection should include redress policies. When an adverse determination has been made about an individual's rights, benefits, or privileges, timely redress – the opportunity to contest that determination with an impartial arbiter – is an essential element of the fairness of that process. DHS should develop access, correction, and redress procedures and communicate such procedures to individuals who participate in a biometrics program consistent with the DPIAC's previously issued report, "The Elements of Effective Redress Programs."<sup>5</sup>

*Purpose Specification: DHS should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.*

Under this principle, DHS should disclose the authority under which it is collecting biometric data and it should clearly articulate how that data will be used. The purpose for which biometric data is collected should be clearly described in the notice that is provided to individuals before the collection of their biometric data.

---

<sup>5</sup> See Department of Homeland Security, Data Privacy and Integrity Advisory Committee (DPIAC), Report 2010-01, "The Elements of Effective Redress Programs," adopted March 18, 2010, available at: [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_dpiac\\_report2010\\_01.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_dpiac_report2010_01.pdf)

Inherent in this principle (and in the “use limitation” principle) is the fact that DHS must use the collected biometric data for only the purposes that it specifies in the notice. Any secondary use of biometric data must be carefully considered and be consistent with the reason for which the data was initially collected. In addition, when the purpose for which the biometric data was collected initially is satisfied, DHS should consider whether the continued retention of that data is consistent with its privacy policies and purpose specification.

*Data Minimization: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).*

Under this principle, DHS should collect only the biometric data that is necessary to accomplish program purposes and retain that data only long enough to satisfy program purposes. For the collection of biometric data, the data minimization principle is especially critical. Due to the sensitivity of biometric data and its immutable characteristics, the data minimization principle should be carefully considered when choosing the biometric collection method for a specific program. In particular, DHS should not choose a more invasive biometric collection method (e.g. DNA collection) when a perceived less-invasive method (e.g. fingerprint collection) could be used.

When addressing this principle, DHS should also consider how biometric data is stored, both for operational purposes and for long-term storage. For operational purposes, only that data (and meta data) needed for the program purpose should be stored. For instance, DHS should weigh the efficacy in storing a complete biometric image versus storing a cryptographic hash of the biometric image or simply a value that indicates whether a biometric match against a known database was achieved. Saving a complete biometric image introduces a more urgent need for securing such data. Saving a cryptographic hash of the image or some other matching variable may not introduce the same level of information security concerns.

*Use Limitation: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.*

Under this principle, DHS must carefully consider how it uses collected biometric data for its programmatic purposes and it must carefully consider any sharing of that data or secondary use of that data. As biometric technologies improve and biometric data becomes easier to collect, use, and share, adhering to this principle becomes more important.

Like the “purpose specification” principle, DHS must use the collected biometric data for only the purposes that it specifies in the notice provided to an individual when the biometric is collected. Any secondary use of biometric data or sharing that data outside of the entity that first collected the data must be carefully considered and be consistent with the reason for which the data was initially collected. If DHS has a compelling reason to share the data outside of the Department, then DHS must enter into an information sharing and access agreement with the external agency to ensure that any additional use of the

biometric is consistent with the purposes for which the biometric was initially collected. The provisions contained in these agreements should be consistent with the DPIAC's previously issued white paper, "The Department of Homeland Security Information Sharing and Access Agreements."<sup>6</sup>

*Data Quality and Integrity: DHS should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.*

Under this principle, DHS should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete. When biometrics are collected and used for identification purposes and to make decisions about individuals, the quality and integrity of the data are critical.

DHS should develop a strategy to periodically assess the accuracy of the collection methods/technology over time to ensure that expected accuracy rates (including consideration of false positive/negatives) are being achieved and to investigate any discrepancies. A significant difference in actual versus expected accuracy rates should be grounds for DHS to reconsider the use of biometrics or the technology in use for the particular program or context.

Technology used to collect and maintain biometric information should contain customary integrity checks to ensure accurate and complete capture of information. In addition, systems that maintain biometric information should have appropriate technical controls, such as edit checks, etc., to help ensure accuracy of any related, non-biometric identifying information that is collected and maintained.

*Security: DHS should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.*

Biometrics require enhanced security because they are a highly sensitive form of PII; persons can change their passwords but they cannot change their DNA. Any plan to use biometrics should include at least the following security elements:

- Secured collection devices
- Limiting the transmission and storage of biometric images on collection devices
- Databases used to store biometric data should be secured according to industry best practices for highly sensitive data
- Replication of original biometric data should be avoided

---

<sup>6</sup> See Department of Homeland Security, Data Privacy and Integrity Advisory Committee (DPIAC), "Final White Paper on Department of Homeland Security Information Sharing and Access Agreements," adopted May 14, 2009, available at:

[http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_dpiac\\_issa\\_final\\_recs\\_may2009.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_dpiac_issa_final_recs_may2009.pdf)

Devices used to collect the data need to be secured and to store data securely; in some environments they may need to be tamper-proof. They must be configured to only store data as long as needed onsite, and to only transmit data to authorized clients. Ordinarily collection and transmission of data should be auditable events.

The collection device should not transmit an image of the original biometric, but instead a unique or probabilistically unique, identifier derived from the biometric. If for any reason this is not feasible, it is essential that the biometric be processed promptly on receipt, that the original image be destroyed, and only the derived identifier be saved.

Databases in which any substantial quantity of biometric data is stored should be subject to appropriate, and periodically reviewed, policies for data retention and data sharing. Biometric databases are particularly attractive targets for attackers, and should be secured carefully. As the DPIAC has previously noted:

“People expect organizations that collect personal information about them to protect it from unauthorized access, use, disclosure, modification, or destruction. The steps that an organization must take to protect its assets, processes, and functions include securing servers and computers inside locked and patrolled buildings; checking the background of employees, if appropriate, and training them to use procedures that protect data; and ensuring that software systems are up-to-date and that new vulnerabilities are patched quickly.”<sup>7</sup>

Cards or other tokens on which biometrically derived data is contained must store the information in a manner that does not permit replication of the original. Identifiers derived from a biometric need to be engineered to be tamper- and copy-resistant.

*Accountability and Auditing: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.*

Under this principle, DHS should be accountable for complying with these principles, providing training to all employees and contractors who use biometric data, and auditing the actual use of biometric data to demonstrate compliance with these principles. This principle is especially important when collecting and using sensitive biometric information for identification purposes.

When collecting and using biometrics for identification, employees should be provided role-based training that includes (1) the importance of and reasons for protecting this information, (2) proper handling of the information, and (3) the consequences of failing to comply with handling requirements. In addition, DHS should establish rules of behavior for

---

<sup>7</sup> See note 4, DPIAC Report 2006-1, “Framework for Privacy Analysis of Programs, Technologies, and Applications” at FN 12.

those who interact with this sensitive information. Supervisors and managers must hold employees accountable for complying with these information-handling requirements, according to the Department's established personnel regulations and procedures.

DHS systems that maintain biometric information should log access to this information and other key events. These logs should be proactively reviewed to identify suspicious activity. DHS should take timely action to investigate and resolve any anomalies identified.

It is critical the DHS Privacy Office is involved early in any program consideration of using biometric information. The Privacy Office should make certain the Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA) documents and processes sufficiently call out biometric data to allow for proactive analysis of the benefits and risks at a time when collaboration between the Privacy Office and those creating the program can optimize any implementation.

DHS should place a priority on conducting Privacy Compliance Reviews to (1) ensure that the controls on the collection, use, sharing, and destruction of biometric information that were established in the PIA are, in fact, followed and (2) identify any additional measures that are needed. These compliance reviews should include analysis of requests for redress, if any, and the disposition of those requests to determine any systemic implications for the program. During these reviews, DHS should also assess available technology to identify viable alternatives that are more accurate and/or more privacy protective.

Specific Committee recommendations for DHS consideration of the use of biometrics:

1. Develop a strategy, policies, and procedures to provide adequate notice, including the specific legislative authority for collecting the biometric and the intended purpose for the collection.
2. Provide employees with training to ensure adequate notice.
3. Deploy written notices in different languages.
4. Use standard images and icons to communicate the use of biometrics.
5. Audit operational notice processes regularly to ensure that they are consistent with policy.
6. Engage in a public education campaign to explain the necessity of DHS use of biometrics.
7. Limit use of the biometric to those specific purposes described in the notice.
8. Minimize collection of biometrics to only data that is necessary for the stated purpose, and only retain such data for the period necessary for such purpose.
9. Develop a strategy to periodically assess the accuracy of the collection methods/technology.
10. Technology used to collect and maintain biometric information should contain customary integrity checks to ensure accurate and complete capture of information.

11. Systems that maintain biometric information should have appropriate technical controls to help ensure accuracy.
12. Any plan to use biometrics should include at least the following security elements:
  - Secured collection devices;
  - Limiting the transmission and storage of biometric images on collection devices;
  - Databases used to store biometric data should be secured according to industry best practices for highly sensitive data; and
  - Replication of original biometric data should be avoided.
13. The Privacy Office should be included early on in any consideration of the use of biometrics.
14. The Privacy Office should analyze the PTA and PIA processes to make certain they sufficiently focus on biometric data.
15. The Privacy Office should ensure periodic compliance reviews are conducted to make certain biometrics implementations are operating appropriately.