Supplemental Information in Support of the NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards

August 10, 2009

NSTC Subcommittee on Biometrics and Identity Management

Table of Contents

1 Introduction

1.1 Overview

In 2005, the NSTC Subcommittee on Biometrics & Identity Management established a standards & conformity assessment working group (SCA WG) to facilitate coordination of USG entities that participated in national and international biometric standards bodies. By 2007, the SCA WG members of the NSTC began working at a more systemic level on topics such as conformity assessment and government-wide adoption of appropriate, approved and published standards.

The collaborative efforts of the SCA WG members resulted in the development of a draft comprehensive policy analysis report, which served as a basis to develop the USG policy document on biometric standards entitled "*NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards"*. This policy was drafted by the NSTC Subcommittee on Biometrics and Identity Management and was approved by the NSTC Committee on Technology in September 2007. It identifies policy issues that impact improving USG mission effectiveness, by delivering standards-based biometric technology.

The NSTC Subcommittee on Biometrics & Identity Management has tasked its standards and conformity assessment working group to maintain the *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards*.

This policy builds on the previous work of the NSTC Subcommittee on Biometrics & Identity Management (e.g., the *National Biometrics Challenge*, dated August 2006) to support biometric data exchange and interoperability across USG agencies, as well as the broader NSTC goal of harmonizing policy and guidance for biometric applications throughout the USG. The policy states that the USG should be guided by the following principles:

- ***Continued development of voluntary consensus standards for biometrics is vital to the security of our Nation and the stability of the US-based biometrics community.*** Agencies should support national and international voluntary biometric standards development activities.
- ***Rigorous testing is required to ensure vendor and system compliance with biometric standards.*** Agencies should support the development of harmonized conformance, interoperability, performance, security, human factors, and operational scenario testing programs in support of procurement actions for biometric products, programs and services.
- ***Standards and conformity assessment processes must be identified and adopted across all agencies to ensure full interoperability.*** Agencies should participate in an interagency process led by the Subcommittee to review available standards and develop consensus recommendations regarding which standards should be adopted across the USG.

- ***The biometric standards and conformity assessment processes recommended by the Subcommittee should be promulgated.*** The Subcommittee shall develop a registry of adopted biometric standards at www.standards.gov/biometrics[1].
- ***The biometric standards and conformity assessment processes recommended by the Subcommittee should be integrated into agency plans whenever feasible.*** Agencies should strive to build and operate biometric systems that are based on the Subcommittee's recommended standards.
- ***Timely adoption and use of appropriate standards is critical to achieving biometrics goals.*** Following selection of recommended standards, the Subcommittee should work to advance adoption of standards for use in Federal biometrics programs and services.

1.2 About this Report

The initial draft comprehensive policy analysis report developed by SCA WG members by June 2007 served as a basis for:

- *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards;*
- *Registry of USG Recommended Biometric Standards*;
- *Supplemental Information in Support of the NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards* (this document*);*
- *Catalog of USG Biometric Product Testing Programs* [DRAFT].

These documents are developed and maintained by the NSTC Subcommittee on Biometrics and Identity Management and the Subcommittee's Standards Conformity Assessment Working Group. The latest approved versions of these documents are available on the Federal government's web site for biometric activities at: ***www.biometrics.gov/standards/***.

2 Supplemental Information

To assist Federal agencies support biometric system interoperability, this section provides supplemental standards and testing related information in support of the *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standard* and the *Registry of USG Recommended Biometric Standards*.

2.1 Conformity Assessment

Conformity assessment[2] of products or equipment to a given set of standards and/or operational requirements enhances the user's confidence that the product will perform in

[1] This information is also available on the Federal government's web site for biometric activities at www.biometrics.gov/standards.

[2] Conformity assessment is defined in ISO/IEC 17025:2004 as: "demonstration that specified requirements (3.1) relating to a product (3.3), process, system, person or body are fulfilled."

accordance to the given set of standards and operational requirements. The specification of operational and performance requirements should express the users' expectations of the equipment and products' performance when used in realistic applications. These requirements must include technical operational characteristics that can be effectively tested and evaluated. Conformity assessment can be performed by testing laboratories that may or may not be accredited. Accreditation of laboratories that perform the tests and evaluations of products and equipment increases confidence that test results are developed with competence and integrity.

Currently there are several USG chartered programs for biometric product testing and certification. These programs are as follows:

- GSA's FIPS 201 Evaluation Program for credential and identity management
- FBI's fingerprint scanner certification
- TSA airport access control performance certification
- TSA TWIC product certification (under development)
- DOD biometrics certification program
- NIST NVLAP program (under development)

For further information on the above programs, refer to the *Catalog of Biometric Product Testing Programs.*

2.2 USG Model Criteria for the Adoption/Maintenance of Biometric Standards

The principle driving force for most USG systems is to improve mission effectiveness by delivering the technology required to support specific applications. Over the course of the last two decades and in accordance with US law and policy, many USG agencies (e.g., DHS, DoD, DoJ, NIST) have promulgated policies and procedures for the adoption of Information Technology (IT) standards, for intra-agency or inter-agency use, in order to facilitate interoperability across applications and systems. In support of standards-based USG biometric systems, the following model criteria for the adoption and maintenance of biometric standards for USG use have been developed.

In 2006, the NSTC SC on Biometrics, Working Group on Standards and Conformity Assessment developed an Interagency Coordination Plan, which included model criteria for the adoption of biometric standards. These criteria were based upon two main factors: the maturity of the standards as evaluated by the USG and the USG business need driving adoption. In terms of maturity, it was recommended that the USG categorize biometric standards and develop three categories: Emerging, Stable, and Mature. Building upon that work, the following criteria for categorizing each biometric standard and guidelines for adoption of a biometric standard are:

Criteria for Emerging Standards (E - Emerging)

- **Availability** – The standard is published and publicly available

- **Authoritative** – The standard was developed and is maintained by a recognized Standards-developing organization (SDO), such as INCITS M1, JTC 1 SC37, or NIST, through a process open to participation by the USG.

Criteria for Stable Standards (S - Stable)

- Includes criteria for Emerging standards in addition to the following:
- **Technical Maturity** – The standard is stable and its technical content is mature. No major revisions or amendments are in progress that will affect backward compatibility with the approved standard. If a revision or amendment is in progress that will have a great impact on compatibility with the approved standard, then the standard should be categorized as an emerging standard.
- **Commercial availability –** Several products from different vendors exist on the market to implement this standard.

Criteria for Mature Standards (M - Mature)

Includes criteria for stable standards in addition to the following:

- **Implementability** – Several commercial or government organizations have developed implementations of this standard.
- **Conformance Testing Tool & Certification** – Conformance testing captures the technical description of a specification and measures whether an implementation faithfully implements the specification. A conformance testing methodology and a tool implementing this methodology, and/or conformance testing program that allows preparation of a certified or otherwise approved validated/qualified product list is available.
- **Interoperability Testing** – Interoperability testing tests one implementation (e.g., device, subsystem, system) with another to establish that they can work together properly. A testing methodology and reference implementations or interoperability testing programs are available.
- **Performance Testing** – Performance testing measures one or more characteristics of an implementation under test (e.g., device, subsystem, system) such as its accuracy, human factors, quality, responsiveness, robustness, speed, throughput, etc., under various conditions. Technology, scenario, and operational performance test results based on recognized testing methodologies are available that provide confidence in sufficient performance to meet the requirements of a recognition application.

The NSTC Subcommittee on Biometrics and Identity Management should establish definitions for emerging, mature, and stable biometric standards and, based upon those definitions, establish model criteria for the adoption and maintenance of biometric standards for USG use. The model criteria for USG agencies to mandate and adopt biometric standards should include the following:

The Registry should adopt standards that may be categorized as either stable or mature;

The Registry should not adopt emerging standards the content of which is not stable or for which there is no product that implements it;

The Registry should include migration strategy concerning the adoption and use of new standards. This strategy should provide guidance for agencies to replace existing standards to mitigate the risk of lack of interoperability. This strategy should provide guidance for the adoption and use of new standards that may replace existing standards to mitigate the risk of possible loss of backward compatibility and/or interoperability. The following questions are examples of the questions that should be addressed in the analysis:

- Is the national standard a subset of the international standard?
- Is compatibility required by implementations of the standard?
- Can implementations conform to both the national and international standards?
- Is there an installed/implemented base using the national or international standard?
- Is the national standard already supporting interagency requirements for interoperability?
- Is the international standard sufficient for international (e.g., NATO Interpol) requirements?
- Are there approved national or international biometric profiles (implementation agreements) available?
- Are there sound conformance test methodologies and tools for the national or international standard?
- Are there conformity assessment programs with validated product lists for the national or international standard?

For new applications implementing biometric standards

- Case 1: Stable or Mature ANSI and Emerging ISO standards exist.
- If there is need to migrate to the ISO version in the future, and then perform comparative analysis and future migration plan.
- Based on the complexity of the future migration plan, decide whether to implement the ANSI standards now or work with industry and SDOs to accelerate the maturity of the international standard and implement the international standards.
- Case 2: Stable or Mature ANSI and ISO standards exist
- Absent technical issues, preference is given for implementation and adoption of the ISO standard.

For existing applications implementing biometric standards

- Case 1: Stable or mature ANSI standard exists, and there are no equivalent international standards.
- Continue implementation of ANSI standards.
- Consider sponsoring the development of an international standard while maintaining backward compatibility with the ANSI standard to protect previous investment.
- Case 2: An international standard becomes Stable or Mature, while an already implemented ANSI or government standard exists
- Determine the business need for migration to the international standard.
- If necessary, develop a future migration plan.
- Develop implementation guidelines for each of the approved standards that will assist the USG in its adoption and implementation of the biometric standards for various applications.
- Perform analysis of the relationship between standards and select the appropriate ones for specific applications based on business models or business cases. Select business cases. Then develop appropriate use scenarios for some of the choices available and discuss some emerging items that should be considered for future applications.
- Develop or identify a mechanism to communicate the USG evaluation criteria and adoption guidelines to the vendor community and SDOs to provide clarification concerning USG standards requirements for adoption by biometric systems.

2.3 USG Participation in Biometric Standards Development

In accordance with US law and policy, USG experts are participating in various national and international standards development organizations to ensure the timely development of technically sound biometric standards. The motive for this participation is to improve mission effectiveness by delivering standards-based biometric technology in support of specific agency applications.
Ongoing USG participation will be required in the future so that:

- Timely, technically sound biometric standards continue to be developed and maintained;
- USG has sufficient technical knowledge about these standards to make savvy adoption decisions; and
- USG can develop a testing infrastructure that supports successful procurements and deployments of standards-based biometric systems.

USG leadership in biometric standardization includes:

- FBI Electronic Fingerprint Transmission Specification (EFTS)/Electronic Biometric Transmission Specification (EBTS) standardization activity;

- DoD EBTS standardization activity;
- National Institute of Standards and Technology Information Technology Laboratory (NIST/ITL) development of standards under its American National Standards Institute (ANSI) accreditation, provide:
    - The Chair of InterNational Committee for Information Technology Standards -Technical Committee INCITS M1
    - The Chair and the Secretariat for ISO/IEC Joint Technical Committee 1-Subcommittee 37 (JTC 1 SC 37)
    - Technical editors for many important biometric standards development projects
- The Departments of State and Homeland Security provide USG representation to the UN International Civil Aviation Organization (ICAO) Technical Advisory Group (TAG) New Technologies Working Group (NTWG) dealing with travel identification and use of biometrics;
- Additionally, USG experts are providing substantive technical contributions for many biometric standards development projects, which are of high priority to the USG. USG coordination of agency positions and contributions to biometric standards development projects is successfully occurring through groups such as the FBI's Criminal Justice Information Systems (CJIS) Advisory Policy Board (APB), the DHS Biometrics Coordination Group (BCG), the DoD Biometric Standards Working Group (BSWG), and the NSTC Subcommittee on Biometrics & Identity Management's Standards & Conformity Assessment Working Group.

The USG should continue to provide administrative and technical leadership for national and international biometric standards development, and should coordinate USG positions and contributions to these standards developers.

2.4 Application of Biometric Standards in Procurement Actions

An important aspect of the adoption of biometric standards is the incorporation of applicable standards into procurement actions. To support the data interchange and interoperability goals for USG use of biometrics, agencies should follow USG guidelines and standards for procurement of biometric devices, hardware and software systems.

In procurement actions standards provide several advantages. The major advantages are:

- In equipment purchases, standards can set specifications that give confidence that products will function as intended;
- Data formats and system interfaces developed to standards support data interchange and USG system interoperability goals; and
- Standards widen the vendor base which leads to increased competition which, in turn, can result in reduced costs.

Unfortunately, it is not always obvious in that a standard is available or applicable to a procurement action. Therefore, many USG agencies have developed processes to identify, vet and adopt standards pertinent to their national security and homeland security needs. Those standards that are adopted will be compiled into a central database that program managers, systems developers, procurement officers and all others performing procurement actions will be able to access. The goal of this effort is to create a one-stop-shopping-center for standards related to national security and homeland security requirements.

Within DoD, the DoD Information Technology Standards Registry serves as a central repository for DoD-approved information technology standards, including biometric standards. The standards selection criteria focus on mandating only those items critical to net-centricity and interoperability. Standards must successfully satisfy the following seven criteria for submission and acceptance into DoD Information Technology Standards Registry (DISR): net-centricity, interoperability, maturity, implementability, public availability, and consistency with authoritative sources. Use of the DISR is mandated for the development and acquisition of new or modified fielded IT and National Security Systems throughout the DoD.

In another example, the DHS has developed a two stage adoption process. The first stage is a technology vetting step. When a document is submitted for consideration as a DHS adopted standard a determination is made by a standards coordinator in the DHS S&T Office of Standards as to the need for a review by technical experts in the pertinent field to determine on a technical level if a document has a sufficiently wide or critical application in the homeland security domain that warrants its adoption.

The second stage involves vetting the document at a policy level. The DHS S&T Office of Standards has formed a DHS Standards Council that works jointly with the DHS Biometrics Coordination Group's Standards Working Group. This is a group of DHS component employees who manage standards issues within their component. As such these representatives either are in a position to make policy decisions on standards matters or have access to those within their component who have that authority. Therefore, they are in a position to have standards vetted within their component.

At the policy level, documents are considered for application to the component's responsibilities, including procurement requirements, as well as whether or not they will encumber the activities of the component. Documents that are deemed acceptable at the policy level are then registered into the central database and publicized by the DHS S&T Office of Standards.

Agencies should develop internal procedures to ensure citation of relevant standards from the *Registry of USG Recommended Biometric Standards* (Registry) in all biometric procurement actions.

2.5 Exchange of Proprietary Data Formats

The issue is whether USG applications should allow standardized records to also include additional proprietary data. The hazard is that within one organization or deployment, a single supplier may use entirely proprietary data for matching, and have partial support

for data that may sometime arrive. For example, an employee of one government department visits another and presents an identity credential containing standardized minutia records to a system that is incapable of processing it.

The vast majority of biometric systems currently in use embed proprietary template data. They are either not interoperable at all, or achieve interoperability only at the input image or signal level. For example most current biometric laptop logon systems are purely proprietary. Alternatively while the FBI's IAFIS system uses a proprietary fingerprint template (minutiae plus other commercially-protected feature data) for matching, it achieves interoperability with the outside world (i.e. state and local law enforcement) only via standardized image formats, primarily ANSI-NIST image records.

However, while image based interoperability is common, there are some standardized biometric templates in existence. Some of these include fields for proprietary data. The format of such data is usually unpublished, is known only to the company that provided it, and could even be strongly encrypted. By definition then, such content is not interoperable i.e. it cannot be used by a system unless that system includes the (proprietary) components to handle it.

Some standards exist that address the issue of exchange of data in proprietary formats. They are stable, but some have revisions underway to correct minor errors:

- ISO/IEC 19794-2:2005
- INCITS 378-2004
- ANSI/NIST ITL 1-2007

With INCITS 378-2004 and ISO/IEC 19794-2:2005 the standard fingerprint minutiae data may be accompanied by either standardized ridge count, core and delta information or by fully proprietary data.

An ANSI/NIST ITL 1-2007 minutiae record can contain standardized minutiae data, very similar to INCITS 378-2004 minutiae data, or full proprietary minutiae data from one of six large commercial fingerprint concerns. The presence of standardized data is not required by an ANSI/NIST ITL 1-2007 record itself.

The technical differences between these standards for core minutia data the differences are syntactic. An ANSI/NIST ITL 1-2007 record can encapsulate purely proprietary data. The other standards can serve to add proprietary data to standardized data.

All USG biometric systems should employ standards to achieve interoperability and avoid proprietary formats to the maximum extent possible.

Agencies should use the proprietary data fields in standardized data formats from the registry of USG recommended biometric standards for the exchange of proprietary data.

Agencies with closed systems that do not require system or interagency interoperability should only use proprietary data formats if standardized data formats can be documented to be inadequate.

2.6 Access to Copyrighted Biometric Standards for USG-wide Use

USG planning/procurement/use of standards-based biometric applications would be greatly facilitated if USG persons involved in such activities had ready access to electronic copies of all biometric standards, which are being specified for USG biometric data exchange and interoperability. Biometric standards that are not copyrighted, such as USG developed standards, are most often, freely available for downloading from the Web. Also, some standards developing organizations copyright their standards and make them available at no cost. However, other standards developing organizations rely on the sale of their copyrighted standards to support their operation.

USG employees and contractors require access to biometric standards to design, procure, and implement systems that use biometric technologies. Providing access to these standards will allow a larger community within USG to be aware of standards, their applicability, and recommended best practices.

2.7 Backwards Compatibility of Standards

In the context of biometric systems, backwards compatibility can only be achieved by ensuring interoperability of new systems with legacy data, or new data with legacy systems. Adequate control and documentation of both the biometric data and biometric interfaces are necessary conditions for this, and while proprietary data and interfaces do not necessarily preclude migration to newer systems, these will most often be from the same supplier. Thus formal biometric standards offer benefits in two areas. First the ability to migrate to another vendor supports a competitive marketplace of improving products. Second this supports continuity of operations should the supplier have difficulties.

Biometric systems often achieve interoperability at the unprocessed image or signal level, but the actual identification or verification comparisons involve proprietary template data. In most cases, particularly for identification systems, this is a necessary condition because accuracy available from standardized templates (when they exist), lags that of the proprietary solutions. If an application is to successfully migrate from one supplier to another, there will be a need to re-enroll the raw image or signal data. In very large scale operations this will entail a transitional arrangement.

Not all applications migrate to new standards at the same rate. Historical data may be necessary to be used, therefore, systems should be able to use older data and formats, perhaps recognizing that utility may be reduced for legacy data; or current data captured according to previous benchmarks or standards.

While participating in SDO activities, the USG should promote the concept that voluntary consensus standards be backward compatible to the maximum extent possible to ensure interoperability of new systems with legacy data, or new data with legacy systems.

2.8 Lifecycle Handling of Biometric Samples

When a biometric sample is entered into a data set, its usefulness depends upon how it has been handled since the time of capture. The data sample may pass quality check algorithms and have the proper data storage format and data attributes, but not be reflective anymore of the biometric sample collected from the subject. This can be caused by a variety of factors, to include, but not limited to, multiple compressions/restorations of a data record, or scanning of an original image at an unsuitable resolution.
While the circumstances of data collection (particularly for watch list information) may not be controllable, once the data is captured, care should be taken so as not to unnecessarily degrade the data in handling of it. By following procedures recommended for selecting parameters at all stages of data handling and not employing certain means of data handling or transmission, the watch list data will be more suitable to actually identifying persons of interest.

Known or suspected terrorist (KST) and other watchlist data should be of the best possible quality. Mishandling of the data could produce false matches that would not be recognizable as such (for instance by introduction of artifacts into a fingerprint image with JPEG used to compress the image. Systems should be reviewed to ensure that data handling meets the best practices defined as a result of this issue.

2.9 Collection and Use of Metadata to Accompany Biometric Data

USG agencies often have requirements for metadata to facilitate the use and management of biometric data, and the storage and transmission of biometric records containing biometric data. The required metadata may include descriptive elements affecting the processing of biometric data as well as some operational system capabilities. The metadata may include information on the types of pre-processing done on the sample data, data that supports verification of the authenticity of the biometric data itself, source of the data, time stamping as well as data that support protection of the biometric data and the integrity of the biometric record. USG agencies often have requirements to associate the biometric data with user-defined challenge data and/or published or unpublished payload data. USG agencies often have requirements to efficiently determine whether a particular biometric data record is of interest by using attributes of their biometric-specific data without exposing the biometric data itself to applications. The best way to meet these types of requirements is for USG agencies to use appropriate standard biometric data structures defined in INCITS M1/JTC 1 SC 37 biometric interface standards, in instantiations of the ANSI/NIST ITL 1-2007 standard or in data structures that use a combination of the standards above.

Metadata can be categorized as “processing,” “operational,” or “demographic.” These categories are somewhat arbitrary, especially the first two. As discussed below, a metadata element may fall within one category or the other depending on the processor, the system and the application. Processing metadata is defined as the minimum information related to the biometric data that is required in order to process the captured biometric data. Length, width and resolution of an image are considered processing metadata. Operational metadata could be seen as information that is not required for the processing of a specific biometric record but that could be crucial for the effective system

operation. Information related to the origin of the biometric data, the product identifier, or the validity period of the biometric sample may fall within this category. In some instances, the distinction whether specific metadata is “processing” or “operational” is blurred. A data structure that contains biometric data could include metadata indicating the product (and version) of the software that generated the biometric data. Whether these are “operational” or “processing” metadata may depend on the system design and matcher functionality. The matcher may require these metadata to process the biometric data, or the metadata may be used only to pre-select a subset of records in a database. Finally, demographic metadata includes biographic and descriptive metadata pertaining to a subject but is not required to process the biometric data.

Metadata specified in the biometric data interchange standards developed by INCITS M1 and JTC 1/SC 37 contain processing metadata and also some operational metadata such as the product identifier and the equipment ID. Whether these metadata are sufficient to achieve the requirements depends of the applications, system design and expected functionality. Usually, a system requires more operational metadata elements than generally specified in biometric data interchange standards in order to achieve full data interchange and interoperability. The interface standards developed by INCITS M1 and JTC 1/SC 37 contain additional operational metadata. Therefore, in an open systems environment, both biometric data interchange format standards and these biometric interface standards are necessary to achieve full data interchange and interoperability for biometric recognition. In many cases, application profiles for the data interchange format standards and/or the technical interface standards are also necessary (e.g., Electronic Biometric Transmission Specifications).

Many applications may also need to incorporate in the system design, means of selecting biometric data based only on metadata external to these data. An example is instances where the biometric data is encrypted and a pre-selection of the records that contain these data needs to be made based on privacy-irrelevant information at the pre-decryption processing stage.

INCITS M1 and JTC 1/SC 37 have developed technical interface standards (e.g., Common Biometric Exchange Formats Framework (CBEFF) and Biometrics Application Programming Interface (BioAPI)) that specify self-describing Biometric Information Records(BIRs) that reveal the format and other attributes of their biometric-specific data without exposing the biometric data itself to applications. The metadata contained in these BIRs provide a means for applications to efficiently determine whether a particular biometric data record is of interest, and if so, which biometric services to call to process the biometric-specific data. The ANSI/NIST ITL 1-2007 standard specifies records that define biometric data of several modalities.

Agencies should develop agency-specific guidelines for the collection, maintenance, and use of metadata for USG biometric applications. This is a factor in OMB program review.

This policy does not apply to law enforcement applications and other large-scale identification applications that only require conformance to standards such as DoJ/FBI/CJIS, EBTS V8.0, DoD EBTS V1.2 or ANSI/NIST ITL 1-2007 nor does it apply to applications that can achieve full system requirements with metadata contained

within the biometric data records specified in INCITS M1/JTC 1 SC 37 biometric data interchange format standards, self-describing data such as JPG 2000 images and instantiations of ANSI/NIST ITL 1-2007 data structures that contain the required metadata.

All new USG biometric applications that require plug and play capability without losing functionality and required descriptive "processing", "operational" or "demographic" data that is not contained in standards or biometric data records described in the note above should:

- Require Biometric Information Records (BIRs) conforming to a CBEFF Patron Format (PF) for the processing, exchange, protection, encapsulation, transmission and storage of biometric data. Use existing Patron Formats that permit incorporating in the data structure the required level of additional "processing" and "operational" metadata and data elements that support payload, security/integrity options and creation date/validity period. (Note: Patron Formats specified in INCITS 398-2008, or instantiations of BioAPI BIRs are preferred.). Part 3 of the international version of CBEFF offers other alternatives.
- Require conformance to the CBEFF Patron Formats detailed above for applications that require transmission or storage of BIRs that require clear text biometric headers or making metadata available without processing the record or exposing the biometric data itself to applications (e.g., for the purpose of indexing BIRs).
- Encrypt biometric data within the BIRs and sign BIRs by relying on information in the CBEFF BIR Security Block, unless other system security mechanism are already provided by means external to these biometric data structures.

USG agencies may define data structures that use a combination of the standards above (e.g., CBEFF BIRs containing ANSI/NIST ITL 1-2007 data structures).

USG applications should adhere to the standards detailed in this issue to the maximum extent possible but with the recognition that strict adherence may require agencies to defined their own CBEFF Patron Formats to meet the requirements for metadata not defined in existing Patron Formats. These Patron Formats may be published or unpublished. The goal is to assure interoperability and data interchange using still standardized data structures. A requirement is that the "owner" of the Patron Format be registered with the International Biometric Industry Association who acts as the Registration Authority for CBEFF. The IBIA organization identifier: Hex "FEFE" has been reserved for private use, not uniquely assigned by IBIA. A Patron Format can also be registered.

Note: Embedding these biometric data structures in other encapsulators not defined in the above standards may be needed to meet some system requirements. Their use is application-dependent. These can be published or unpublished data structures.

2.10 Future USG-wide Requirements for Biometric Technologies

The USG consists of many agencies with many different operational environments and business needs. In addition, new requirements may arise over time that will affect the potential use of biometrics by these agencies.
The Registry is focused on biometric technologies that are considered to be high priority for USG-wide use in the near term (i.e., fingerprint, 2D-face, and iris) or may be high priority by 2013 (i.e., voice and DNA modalities). Other biometric technologies (i.e., 3D-face, vascular, hand geometry, signature, etc.) may be included in subsequent revisions of this report.

Voice recognition is an excellent example of an emerging biometric technology that may have potential use in the USG. For example, voice recognition could be used in cases such as a driver of a vehicle on an airport tarmac approaching an airplane. Voice recognition software may be able to determine whether that particular driver has authority to enter a specific restricted zone.

DNA is not traditionally considered a real-time biometric due to the requirements for DNA processing and analysis. However, there is now more acceptance of DNA as a practical biometric tool as the processes for taking DNA samples and the actual 'laboratory' process becomes simplified and less time consuming.

Bibliography

Reports

Report of the Defense Science Board on Defense Biometrics, March 2007
http://www.acq.osd.mil/dsb/reports/2007-03-Biometrics.pdf

NSTC Subcommittee on Biometrics**,** *The National Biometrics Challenge*, August 2006
http://www.biometrics.gov/NSTC/pubs/biochallengedoc.pdf

NSTC Subcommittee on Biometrics**,** *Privacy and Biometrics*, September 2006
http://www.biometrics.gov/docs/privacy.pdf

NSTC Subcommittee on Biometrics, Introduction to Biometrics Web Page
http://www.biometrics.gov/ReferenceRoom/Introduction.aspx

NSTC Subcommittee on Biometrics**,** *Biometrics Glossary*, September 2006
http://www.biometrics.gov/Documents/Glossary.pdf

NSTC Subcommittee on Biometrics, *Biometrics Standards*, August 2006
http://www.biometrics.gov/Documents/BioStandards.pdf

NSTC Subcommittee on Biometrics, *Biometrics Testing and Statistics*, August 2006
http://www.biometrics.gov/docs/biotestingandstats.pdf

NIST, *Guidance on Federal Conformity Assessment Activities*, August 2000
http://ts.nist.gov/Standards/Global/caguidance.cfm

NISTIR 6025, *Metrology for Information Technology (IT)* , May 1997
http://www.itl.nist.gov/lab/nistirs/NISTIR%206025.pdf

INCITS M1, *Report to M1 on Issues for Harmonizing Conformity Assessment to Biometric Standards*, March 2005
http://www.incits.org/tc_home/m1htm/docs/m1050067.pdf

INCITS M1, *Study Report on Biometrics and E-Authentication*, March 2007
http://www.incits.org/tc_home/m1htm/2007docs/m1070185.pdf

U.S. Army Biometrics Task Force, *U.S. Army BTF Technical Contribution to M1.3 - National and International Iris Image Interchange Format Standards: Comparative Analysis Report*, November 2006
http://www.incits.org/tc_home/m1htm/2006docs/m1060977.pdf

U.S. Army Biometrics Task Force, *U.S. Army BTF Technical Contribution to M1.3 - National and International Face Recognition Format for Data Interchange Standards: Comparative Analysis Report*, November 2006

http://www.incits.org/tc_home/m1htm/2006docs/m1060976.pdf

Making the Confidence Connection -- Conformity Assessment System Design, Gordon Gillerman, Standards Engineering, the Journal of the Standards Engineering Society, Vol. 56, No. 6, November/December 2004
http://www.astm.org/SNEWS/DECEMBER_2004/gillerman_dec04.html

USG Laws and Policy

NIST National Technology Transfer and Advancement Act (NTTAA) Web Page
http://ts.nist.gov/Standards/Conformity/nttaa.cfm

OMB Circular A-119; *Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities*, February 1998
http://ts.nist.gov/Standards/Conformity/upload/fr-omba119.pdf

Freely Available Standards and Guidelines

NIST, *ANSI/NIST-ITL 1-2000 Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information*
ftp://sequoyah.nist.gov/pub/nist_internal_reports/sp500-245-a16.pdf

NIST, American National Standard, *ANSI/NIST-ITL 1-2007 Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information - Part 1*
http://fingerprint.nist.gov/standard/

NIST, American National Standard, *ANSI/NIST-ITL 2-2008 Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information - Part 2 -XML*
http://fingerprint.nist.gov/standard/index.html

NIST FIPS 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, June 2006
http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

NIST SP 800-76-1, *Biometric Data Specification for Personal Identity Verification*, January 2007
http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf

NISTIR 6529-A, *Common Biometric Exchange Formats Framework*, April 2004
http://www.itl.nist.gov/div893/biometrics/documents/NISTIR6529A.pdf

DoJ/FBI/CJIS, *Electronic Fingerprint Transmission Specification (EFTS), Version 7.1*, May 2005
http://www.fbi.gov/hq/cjisd/iafis/efts71/efts71.pdf

DoJ/FBI/CJIS, *Electronic Biometric Transmission Specification (EBTS) Version 8.1*, http://www.fbibiospecs.org/fbibiometric/documents/EBTS_v8.1_11-24-08.pdf

DoJ/FBI/CJIS, *IAFIS Wavelet Scalar Quantization (WSQ) Grayscale Fingerprint Image Compression Specification*, December 1997
http://www.fbibiospecs.org/fbibiometric/docs/WSQ_Gray-scale_Specification_Version_3.pdf

Image Quality Specifications for ten-print fingerprint capture systems, Appendix F, EBTS
www.fbibiospecs.org

Personal Identity Verification (PIV) Image Quality Specifications for Single Finger Capture Devices
http://www.fbi.gov/hq/cjisd/iafis/piv/pivspec.pdf

JPEG 2000 Profile for 1000ppi Fingerprint Compression
www.mitre.org/work/tech_papers/tech_papers_04/lepley_fingerprint/

JPEG 2000 and WSQ Image Compression Interoperability
www.mitre.org/work/tech_papers/tech_papers_01/lepley_jpeg2000/

Testing Documents

WSQ Fingerprint Image Compression Encoder/Decoder Certification Guidelines
www.itl.nist.gov/iad/894.03/fing/cert_gui.html

Test Procedures for Verifying IAFIS Image Quality Requirements for Fingerprint Scanners and Printers
http://www.mitre.org/tech/mtf

Test Procedures for Verifying Image Quality Requirements for Personal Identity Verification (PIV) Single Finger Capture Devices
http://www.mitre.org/tech/mtf

Available Test Tools/Reference Data

DoD Conformance Test Suite (CTS) for ANSI INCITS 358-2002 BioAPI Specification (BioAPI 1.1)
http://www.biometrics.dod.mil/CurrentInitiatives/Standards/TestingToolsets.aspx

NIST Conformance Test Suite (CTS) for ANSI INCITS 358-2002 BioAPI Specification (BioAPI 1.1)
http://www.itl.nist.gov/div893/biometrics/BioAPI_CTS/index.htm

NIST Minutiae Exchange Interoperability Test for INCITS 378-2004
http://fingerprint.nist.gov/minex/

NIST Conformance Testing Architecture and Test Tool for CBEFF Patron Format A (specified in INCITS 398-2008)
http://www.itl.nist.gov/div893/biometrics/CBEFF_PFA_CTS/index.htm

Certified Product Lists

GSA FIPS 201-1 certification: http://fips201ep.cio.gov/

TSA Airport Access Control certification:
http://www.tsa.gov/join/business/biometric_qualification.shtm

FBI certification: http://www.fbi.gov/hq/cjisd/iafis/cert.htm

TSA TWIC certification: http://www.tsa.gov/assets/pdf/twic_ice_list.pdf

The information provided in this Annex is a summation of the analyses performed by the SCA WG in the **first part of 2007**. Therefore some of the information below is now out-of-date. These analyses are being provided to give the background on the issues that shaped the subsequent first editions of *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards* and the *Registry of USG Recommended Biometric Standards* (Registry)."

Annex A – History

2007 Analyses by SCA WG

The information provided in this Annex is a summation of the analyses performed by the SCA WG ***in the first part of 2007 and therefore some of the references below are now out-of-date.*** These analyses served as a basis for the subsequent first editions of *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards* and the *Registry of USG Recommended Biometric Standards* (Registry).

A.1 Fingerprint and Palm Image Standard

Issue

USG agencies have ongoing requirements to capture, use, store, and exchange fingerprint and palmprint image biometric data. The best way to meet these requirements is for USG agencies to use the same biometric data interchange format standard for fingerprint images and to use the one voluntary consensus data interchange format standard available for palmprint images. While the standards support data exchange, conformance to them alone is not sufficient to satisfy the USG's high level objective to have the best quality finger images available for watchlists and other applications.

Analysis of Issue

There are three voluntary consensus data interchange format standards for fingerprint images presently available:

- ISO/IEC 19794-4:2005 Fingerprint Image Interchange Format
- ANSI INCITS 381:2004 Fingerprint Image Interchange Format
- ANSI/NIST-ITL 1-2007 Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information - Type-14 fingerprint image record

All three fingerprint image standards are stable and compatible with one another. The Number of Fingers, the capture resolution, compression ratio and the compliance of sensor is specified by each application. At the time of this writing, revision projects are underway for ISO/IEC 19794-4:2005 and INCITS 381-2004, which should result in improved standards.

There is only one voluntary consensus data interchange format standards for palmprint images presently available:

- ANSI/NIST-ITL 1-2007 Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information - Type-15 palmprint image record

There are many options within the standards and these should be rigorously addressed in a dedicated profile of the standards for specific application.

The information provided in this Annex is a summation of the analyses performed by the SCA WG in the **first part of 2007**. Therefore some of the information below is now out-of-date. These analyses are being provided to give the background on the issues that shaped the subsequent first editions of *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards* and the *Registry of USG Recommended Biometric Standards* (Registry)."

Existing or planned USG/other procurements that should result in the deployment of standards-based fingerprint products include the Federal Government Personal Identity Verification (PIV) Program, FBI Next Generation Identification, DHS US-VISIT IDENT, and the DoD Automated Biometric Identification System. The FBI NGI specifies the ANSI/NIST ITL 1-2007 Type-14 fingerprint record and PIV will result in INCITS 381-2004 and ANSI/NIST ITL 1-2007 Type 4 and 14.

Potential Solutions

In all new USG biometric applications in which fingers are imaged for enrollment or registration, the images collected should conform to ANSI/NIST ITL 1-2007 Type-14 fingerprint image record requirements. The resolution should be at least 197 pixels per centimeter.

The Type-14 record, which permits information exchange beyond that of the Type-4 record (e.g., variable resolution images, greater than .8 bits of grayscale), is used for new USG fingerprint applications. The use of the ANSI/NIST ITL Type-4 record is deprecated

In all new USG biometric applications in which the palms of cooperative subjects are imaged for enrollment or registration, the images collected should conform to ANSI/NIST ITL 1-2007 Type-15 palmprint image record requirements.

For all new USG biometric fingerprint and palmprint applications, the image standards should be formally profiled. This should enumerate which of the options are permitted and instantiate minimum and maximum values for variables that the generic base standards do not prescribe. Particularly the profile should establish minimum criteria for the sensor resolution and the sensor area. It should enumerate the allowed compression algorithms and should specify maximum compression ratios.

USG should develop default or candidate profiles for fingerprint image retention and transmission.

USG should develop technical means, including open-source tools, for transcoding fingerprint images between instances of the standards (e.g., fingerprint images conforming to ISO/IEC 19794-4:2005 transcoded to the ANSI/NIST ITL 1-2007 Type-14 fingerprint image record).

USG applications should adhere to the ISO and ANSI standards to the maximum extent possible but with the recognition that strict adherence may not be feasible, advisable, or cost efficient. Therefore, a specific application profile should be developed that deals with the issue of which parts of the standards are not to be adhered to in any particular application. The goal is to assure machine interoperability and accuracy.

USG agencies should reflect this policy in any agency specific adoption processes (e.g., DoD DISR, DHS TRM).

Agency standards registries should harmonize with this policy.

The information provided in this Annex is a summation of the analyses performed by the SCA WG in the **first part of 2007**. Therefore some of the information below is now out-of-date. These analyses are being provided to give the background on the issues that shaped the subsequent first editions of *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards* and the *Registry of USG Recommended Biometric Standards* (Registry)."

A.2 Fingerprint Minutiae Standard

Issue

USG agencies have ongoing requirements to exchange fingerprint minutiae biometric data. The best way to meet these requirements is for USG agencies to use the same biometric data interchange format standard for fingerprint minutia. Minutiae-based exchange has been demonstrated to be less accurate, but faster, than image-based fingerprint interoperability.[3]

Analysis of Issue

There are three data interchange format standards for fingerprint minutiae:

- ISO/IEC 19794-2:2005 Finger minutiae data
- INCITS 378-2004 Finger Minutiae Format for Data Interchange
- ANSI/NIST ITL 1-2007 Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information - Type-9 minutia data record

All three standards are stable. INCITS 378-2004 is being revised to correct minor flaws.

ISO/IEC 19792-4:2005 allows specification of either the record or (smart) card format and requires specification of the format type code to describe the minutia placement specification.

Existing applications allow the use of standardized fingerprint templates. The FBI CJIS, Electronic Biometric Transmission Specification (EBTS) Version 8.0 - requires conformance to the ANSI/NIST ITL 1-2007 Type-9 fingerprint record. NIST Special Publication 800-76-1 requires storage of INCITS 378-2004 fingerprint templates on the PIV credential.

Potential Solutions

All new USG identification applications should only use standardized minutiae records, even if parent images or associated proprietary template data are also available for matching.

All new USG verification applications which specify storage or use of standardized minutia records should use the ISO/IEC 19794-2:2005 formats of type 0001, 0003 or 0005. Such applications should allow inclusion of proprietary data in associated extended data fields.

The use of any of the standardized minutiae records for encoding latent fingerprint minutiae is insufficient, and should only be used as a supplement to the parent latent image.

[3] NISTIR 7296 http://fingerprint.nist.gov/minex04/minex_report.pdf

The information provided in this Annex is a summation of the analyses performed by the SCA WG in the **first part of 2007**. Therefore some of the information below is now out-of-date. These analyses are being provided to give the background on the issues that shaped the subsequent first editions of *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards* and the *Registry of USG Recommended Biometric Standards* (Registry)."

The use of any of the standardized minutiae records for encoding enrollment records to be used in the background or search in civil or criminal searches is insufficient, and the standards may only be used as supplemental material to a fingerprint image.

For all new USG fingerprint minutiae-based applications, the standards should be formally profiled. This will enumerate which of the options are permitted and instantiate minimum and maximum values for variable that the generic base standards do not prescribe.

NIST should coordinate USG positions on the revision of minutiae standards.

USG should develop default or candidate profiles for verification of fingerprint minutiae applications.

NIST should conduct further Minutiae Exchange (MINEX) research, development, test and evaluation rounds to improve minutiae-based accuracy and interoperability. Such work should include extant standardized records and emerging Extended Fingerprint Feature Sets.

USG should develop technical means, including open-source tools, for transcoding minutiae between instances of the standards, e.g. a minutiae record conforming to ISO/IEC 19794-2:2005 transcoded to the ANSI/NIST ITL 1-2007 Type-9 minutia data record.

NIST should conduct further Evaluation of Latent Fingerprint Technologies (ELFT) research, development, test and evaluation rounds to improve accuracy, and to evaluate performance of standardized latent fingerprint feature encodings.

NIST should conduct or otherwise coordinate evaluation of standardized encoding of fingerprint information.

USG applications should adhere to the ISO and ANSI standards to the maximum extent possible but with the recognition that strict adherence may not be feasible, advisable, or cost efficient. Therefore a specific application profile should be developed that deals with the issue of which parts of the standards are not to be adhered to in the particular application. The goal is to assure machine interoperability and accuracy.

USG agencies should reflect this policy in any agency specific adoption processes (e.g., DoD DISR, DHS TRM).

Agency standards registries should harmonize with this policy.

A.3 Latent Fingerprint Standard

Issue

The ability to transmit and process latent fingerprint images is of critical importance in the criminal law enforcement and homeland and national security domains.

The information provided in this Annex is a summation of the analyses performed by the SCA WG in the **first part of 2007**. Therefore some of the information below is now out-of-date. These analyses are being provided to give the background on the issues that shaped the subsequent first editions of *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards* and the *Registry of USG Recommended Biometric Standards* (Registry)."

Analysis of Issue

Performance of latent examiners and automated biometrics system is strongly dependent on the acquisition and transmission of the latent images. The ability of modern latent matching technologies to conduct accurate one-to-many searches remains problematic and a high-end research topic. Two search paradigms are: Search of latent images against massive repositories of ten-print records (the typical criminal case); and comparison of a single ten-print record against a watchlist of latent images (the KST case).

The relevant acquisition and transmission standards may be incomplete in supporting lights-out evaluation of automated latent matching technologies (for example, in connoting mirror-imaging).

Potential Solutions

In all future applications, latent fingerprint and palm images should be stored in Type 13 records of the ANSI/NIST ITL 1-2007 standard. That standard's Type 7, 9 and 14 records should not be used. The INCITS 381 and ISO/IEC 19794-4 standards should not be used.

NIST should continue its ELFT series of performance-based evaluations of latent fingerprint technologies. These evaluations should be extended to include evaluations of standardized feature sets. NIST should propagate successfully evaluate feature data through the international standards community.

NIST should initiate and support formal standardization of one-to-many latent evaluations in SC 37 Working Group 5.

NIST should coordinate an interagency and international collaboration to collect and construct reference latent fingerprint and palm image databases. Such collections should include acquisition of mated ten-print records. These should be made available for research and development. NIST should sequester test data for its ELFT evaluations. NIST should support research and development by allowing testing via its Rapid Evaluation infrastructure.

USG agencies should reflect this policy in any agency specific adoption processes (e.g., DoD DISR, DHS TRM).

Agency standards registries should harmonize with this policy.

A.4 Face Image Standard (2D)

Issue

USG agencies have ongoing requirements to capture, store and exchange face biometric data. The best way to meet these requirements is for USG agencies to use the same biometric data interchange format standard for face images. While the standards support

data exchange, they also contain requirements for the capture of the image in such a manner as to optimize the performance of facial biometric matching systems.

Analysis of Issue

There are three data interchange standards for face images. They establish formats for the data, but they also include quality-related requirements for the photographic capture process.

- ISO/IEC 19794-5:2005 Biometric Data Interchange Format - Part 5: Face Image Data
- INCITS 385-2004 Face Recognition Format
- ANSI/NIST ITL 1-2007 Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information - Type-10 Facial and Scars, Marks and Tattoos image record

ISO/IEC 19794-5:2005 and INCITS 385-2004 both support three face image types: basic, full-frontal, and token image. The basic image can be any image of a face. The full-frontal image is a well-posed passport-style frontal image. The token image is a geometrically constrained frontal image that requires an eye-finding algorithm to drive correction of rotation, scale and position.

The INCITS 385-2004 and ISO/IEC 19794-5:2005 standards are primarily intended to support formal enrollment processes. The ANSI/NIST ITL 1-2007 standard supports a greater diversity of applications.

The 2D content of all three standards is stable. The 3D content of INCITS 385-2004 is recently final but is likely to differ from that of ISO/IEC 19794-5:2005, which remains under development. Revisions also include information concerning the acquisition of face images.

A detailed comparison of the differences between ANSI INCITS 385-2004 and ISO/IEC 19794-5:2005 has been published.[4] The differences between the base standards are minor. The ISO standard has been formally amended to include an informative annex on how best to acquire images from cooperative subjects.

There are many options within these standards and, each application must specifically determine which parts are to be used. The compilation of these specifications should be included in the Application Profile.

Potential Solutions

In all new USG biometric face applications in which cooperative subjects are photographed for enrollment or registration, the images collected should conform to the ISO/IEC 19794-5:2005 Face Image Data standard, for the capture, storage, and data exchange of face image data. This should include the Amendment 1 constraints on image

[4] http://www.incits.org/tc_home/m1htm/2006docs/m1060976.pdf

capture. The acquisition should be designed to be frontal and the result should be a conformant Full Frontal or Token instance. Applications should be designed to capture at least 90 pixels between the eyes from all subjects.

The images collected in all new USG biometric face applications in which subjects are imaged in a non-cooperative or covert manner should conform to the ANSI/NIST ITL 1-2007 Type-10 face record with subject acquisition profile (SAP) of level 1 or above. The acquisition should be frontal when possible.

For Machine Readable Travel Documents (MRTDs) (e.g., e-Passports and Visas), USG should follow the ISO/IEC 19794-5:2005, which is specified by ICAO 9303.

For all new USG biometric face applications, the standards should be formally profiled. These profiles should enumerate which of the options are permitted and instantiate minimum and maximum values for variables that the generic base standards do not prescribe. This should include specification of the maximum compression ratios and compression algorithms.

USG should develop default or example or candidate profiles for face image enrollment.

USG should develop technical means, including open-source tools, for transcoding images between instances of the standards, e.g. face images conforming to ISO/IEC 19794-5:2005 transcoded to the ANSI/NIST ITL 1-2007 Type-10 face record.

USG applications should adhere to the standards to the maximum extent possible but with the recognition that strict adherence may not be feasible, advisable, or cost efficient, therefore a specific application profile must be developed that deals with the issue of which parts of the standards are not to be adhered to in the particular application. The goal is to assure machine interoperability and accuracy.

As an example, at Ports of Entry (POE) the background is not controllable as required in the standards. This is a deviation, and while it may lead to some drop in face detection performance, it is unlikely to affect machine readability. For this reason a specific application profile may include limited, specified, deviations from the standard. Such deviations should be reported to NIST in each agency's annual reporting in accordance with the NTTAA.

USG agencies should reflect this policy in any agency specific adoption processes (e.g., DoD DISR, DHS TRM).

Agency standards registries should harmonize with this policy.

A.5 Iris Image Standard

Issue

USG agencies have ongoing requirements for the capture, storage, use, and exchange of iris biometric data. The best way to meet these requirements is for USG agencies to use the same biometric data interchange format standard for iris images.

The information provided in this Annex is a summation of the analyses performed by the SCA WG in the **first part of 2007**. Therefore some of the information below is now out-of-date. These analyses are being provided to give the background on the issues that shaped the subsequent first editions of *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards* and the *Registry of USG Recommended Biometric Standards* (Registry)."

Analysis of Issue

There are three voluntary consensus data interchange format standards for iris images presently available:

- ISO/IEC 19794-6:2005 Biometric Data Interchange Format - Part 6: Iris Image Data
- ANSI INCITS 379-2004 Iris Image Interchange Format
- ANSI/NIST-ITL 1-2007 Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information - Type-17 Iris image record

As of this writing, INCITS M1 issued 30-day letter ballots to approve the withdrawal of ANSI INCITS 379-2004 as an American National Standard and to approve the withdrawal of Project 1576-D – Revision of INCITS 379-2004.

Should these letter ballots not pass, it is important to note that these two standards have options that result in a potential implementation issue for the USG. ISO/IEC 19794-6:2005 and ANSI INCITS 379-2004 both specify two alternative image interchange formats for biometric authentication systems that utilize iris recognition. The first format is based on a rectilinear image storage format that may be a raw, uncompressed array of intensity values or a compressed format such as that specified by ISO/IEC 15444. The second format is based on a polar image specification. A detailed comparison of the differences between ANSI INCITS 379-2004 and ISO/IEC 19794-6:2005 has been published.[5] A major difference between these two standards is the polar coordinate conversion.

The ANSI/NIST-ITL 1-2007 Type-17 Iris image record only specifies a rectilinear image storage format, which is compatible with the rectilinear image storage format in ISO/IEC 19794-6:2005.

Potential Solutions

All new USG biometric iris applications should conform to the rectilinear image format requirements of ISO/IEC 19794-6:2005, *Biometric Data Interchange Format - Part 6: Iris Image Data*, for the capture, storage, and data exchange of iris image data. These requirements are compatible with the ANSI/NIST ITL 1-2007 Type-17 Iris image record. (Note: The ANSI/NIST ITL 1-2007 Type-99 CBEFF biometric data record is explicitly disallowed for use to exchange the rectilinear image storage format in ISO/IEC 19794-6:2005.)

Iris images conforming to the polar image format requirements of ISO/IEC 19794-6:2005 may be retained only if their rectilinear parents are also retained. If the USG receives a polar image only, the data may be retained but should be transcoded to a rectilinear

[5] http://www.incits.org/tc_home/m1htm/2006docs/m1060977.pdf

format. If USG receives an unformatted raw raster image, it should be encoded as a rectilinear image.

For all new USG biometric iris applications, the standards should be formally profiled. These profiles should enumerate which of the options are permitted and instantiate minimum and maximum values for variables that the generic base standards do not prescribe. Each profile should include specification of the maximum compression ratios and compression algorithms.

USG should develop default or example or candidate profiles for iris image enrollment in rectilinear format.

USG should develop technical means, including open-source tools, for transcoding images between instances of the standards, e.g. an iris image that conforms to the rectilinear image format requirements of ISO/IEC 19794-6:2005 transcoded to the ANSI/NIST ITL 1-2007 Type-17 Iris image record.

USG applications should adhere to the standards to the maximum extent possible but with the recognition that strict adherence may not be feasible, advisable, or cost efficient. In cases where a deviation from this policy is necessary, the specific application profile for that project must be developed that deals with the issue of which parts of the standards are not to be followed. This deviation must be listed in the agency's annual report to NIST on compliance with the terms of the National Technology Transfer and Acquisition Act (NTTAA).

USG agencies should reflect this policy in any agency specific adoption processes (e.g., DISR, DHS TRM).

Agency standards registries should harmonize with this policy.

A.6 Voice Standard

Issue

USG agencies have ongoing requirements to capture, storage, use, and exchange voice biometric data for personal recognition. The best way to meet these requirements is for USG agencies to use the same biometric data interchange format standard for voice data.

Analysis of Issue

There are two published standards related to the identification of speakers using voice information:

- VoiceXML2.0
- Speaker Verification API

Additionally, two data interchange formats are under development at the national and international levels that allow the exchange of speaker data.

The information provided in this Annex is a summation of the analyses performed by the SCA WG in the **first part of 2007**. Therefore some of the information below is now out-of-date. These analyses are being provided to give the background on the issues that shaped the subsequent first editions of *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards* and the *Registry of USG Recommended Biometric Standards* (Registry)."

- INCITS Project 1821-D: Speaker Biometrics Format for Data Interchange, which is the product of collaboration between the Speaker Biometrics Committee of the VoiceXML Forum (SBC), a liaison member of M1, and INCITS M1.
- ISO/IEC 19794 - Biometric data interchange format – Part 13: Speech data interchange format for speaker recognition, which is a recently approved project within JTC 1 SC 37.

The INCITS M1 project intends to define a method for characterizing the speech produced by an end user for enrollment, verification, or identification. It supports transmission of raw speech data with an optional extension for proprietary data. It defines the attributes that are needed to generate a voice model from the dialog and turns and includes the XML representation of those attributes. The USG has the option (recommended at this point) to require only the raw data and deprecate use of the optional extended data. Although as stated above, it currently specifies an optional extension for proprietary data (this could include vendor-dependent feature data or other types of data).

The JTC 1 SC 37 project intends to specify speech data interchange format(s) for speaker recognition. One data interchange format will support raw speech; other formats could include formats for interchange at the feature vector level.

At this time there are no known major implementations that include biometric standards for speaker identification or verification.

Potential Solutions

The standards need to become more stable before policy can be determined. A preliminary assertion is that all future USG biometric voice applications might require conformance to the national voice standard (once published). Although allowing extended optional data might be application dependent, the policy might require deprecating use of this extended optional data perhaps through profiling the base standard or affecting its content before the standard is completed.

USG should invest in the standards development and progress of R&D to support agency needs and implementations for voice applications.

USG should participate in the development of the national and international standards including the INCITS M1, ISO/JTC1/SC37.

Agencies should participate in interagency biometric standards working groups to communicate and define agency-specific requirements on operational use for voice applications.

The information provided in this Annex is a summation of the analyses performed by the SCA WG in the **first part of 2007**. Therefore some of the information below is now out-of-date. These analyses are being provided to give the background on the issues that shaped the subsequent first editions of *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards* and the *Registry of USG Recommended Biometric Standards* (Registry)."

A.7 DNA Data Standard

Issue

USG agencies have ongoing requirements to capture, storage, use and exchange DNA biometric data for personal recognition. The best way to meet these requirements is for USG agencies to use the same biometric data interchange format standard for DNA.[6]

Analysis of Issue

A data interchange format is under development at the international level to allow the exchange of DNA data.

- ISO/IEC 19794 - Biometric data interchange format – Part 14: DNA Data, which is a recently approved project within JTC 1 SC 37.

INCITS M1, the U.S. TAG for JTC 1/SC 37 on Biometrics is concerned that the scope of the working draft for 19794-14:

- Exceeds international DNA data exchange intent;
- Requires core loci that are primarily European-centric; and
- Contains searching, matching, and reporting requirements.

INCITS M1 further recommends that 19794-14 should concentrate on the following issues:

- Standardize DNA profile nomenclature;
- Standardize data exchange format;
- Remove core loci requirement and allow each country or each application domain to define which core loci they require through their respective application profiles;
- Eliminate searching, matching, and reporting requirements or move them to an informative annex; and
- Establish liaisons with multi-national advisory committees, such as European Network of Forensic Science Institutes (ENFSI), the Scientific Working Group on DNA Analysis Methods (SWGDAM), and the European DNA Profiling Group (EDNAP).

This project is intended to support the future emergence of DNA profiling systems that can produce electronic results (without manual intervention) within a few hours (automatic identification). Such automatic identification systems are not yet a reality; laboratory equipment, expert human supervision, and a lengthy identification period is

[6] Note: This issue does not address how to collect, store, transfer, or protect DNA samples. It is solely concerned with consistent data formatting of information used by DNA matching processes.

The information provided in this Annex is a summation of the analyses performed by the SCA WG in the **first part of 2007**. Therefore some of the information below is now out-of-date. These analyses are being provided to give the background on the issues that shaped the subsequent first editions of *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards* and the *Registry of USG Recommended Biometric Standards* (Registry)."

the current state of the art, but this is expected to improve on a time-scale similar to the production of an International Standard. This International Standard anticipates a reduction of human involvement and a reduction of the identification (enrollment and comparison) time, so that the identification becomes fully automatic.

Potential Solutions

The USG should develop a consolidated, consistent approach to DNA data reporting and participate in the standards development organization bodies proposing formats for DNA data storage and transmission.

USG should participate in the development of DNA standards through INCITS M1 and coordinate activities across disciplines, including biometric and medical standards bodies.

A.8 Multi-biometric Fusion

Issue

Multi-biometric fusion refers to any mechanism for combining information from:

- Multiple modalities, e.g. iris and fingerprint;
- Multiple samples, e.g. images of the right index and right middle fingers;
- Repeated samples, e.g. three passport images of a person over time;
- Samples gathered in sequential or otherwise staged process biometrics;
- Multiple algorithms, e.g. matching implementations from providers A, B and C.

Analysis of Issue

These offer substantial improvements in biometric accuracy, with the benefit decreasing in the order listed above, and they work because more information is available. Thus multimodal fusion is effective because two (or more) modes are more uniquely identifying. Multiple-sample fusion is a potent mechanism for utilizing more information in the recognition process. Repeated-sample fusion is particularly effective in cases where a first sample is weak. Multi-algorithmic fusion is effective in situations where different products fail on different samples.

The most readily implemented form of fusion is score-level fusion, in which matcher output scores are fused. It is easy to implement, and is highly effective. A further benefit is that it may be interoperable, i.e. the match scores from products X and Y feed a fusion module provided by supplier Z. Score level fusion is supported by standardized markup for statistical information from each matching implementation.

One draft standard exists. It is presently at stage of public review:

- INCITS 43X, Project Number 1790D, Fusion Information Format.

The standard supports multimodal or otherwise multi-algorithmic fusion processes. It is not needed for multi-sample and repeated sample fusion.

The information provided in this Annex is a summation of the analyses performed by the SCA WG in the **first part of 2007**. Therefore some of the information below is now out-of-date. These analyses are being provided to give the background on the issues that shaped the subsequent first editions of *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards* and the *Registry of USG Recommended Biometric Standards* (Registry)."

Potential Solutions

All future USG applications should produce a documented assessment of the costs and benefits of using single-supplier multimodal applications vs. interoperable different-supplier applications.

USG should institute mechanisms to identify operational needs and prioritize support of operationally relevant multi-biometric research. The USG should prioritize research into fusion for identification applications. The USG should de-prioritize research that addresses just the matching error rates in verification systems.

USG should support standards development for supporting accurate fusion processes, and for supporting the transmission and storage of fused biometric data, and for storage, interchange and use of multiple or repeated biometric samples.

USG should develop best practices for implementation of multi-biometric fusion.

Agencies should identify agency-specific requirements on use of multi-biometric standards.

USG should support near term development of mechanisms for accurate fusion processes, which should include the transmission and storage of fused biometric data, as well as storage, interchange and use of multiple or repeated biometric samples for large identification systems.

USG should support near term research use of multiple modalities for rectification of extant Type I and Type II consolidation errors in large biometric systems and databases.

USG should support research, development, testing and evaluation of the following items, in each case specifically targeting reduced matching error rates and improved efficiency.

Fusion of biometric modalities:

- Repeated-sample fusion paradigms
- Inclusion of quality values into fusion processes
- Use of un-segmented four-finger fingerprint images as a single biometric
- Use of un-segmented index and middle fingerprint images as a single biometric

A.9 Application Profiles

Issue

In any given application, it will often be insufficient to simply cite a biometric standard and require conformance to it. This arises because the standards have often been drafted to be application independent, and the standards developers had all along intended that the standard should be layered beneath an application profile or a requirements document, or both.

The information provided in this Annex is a summation of the analyses performed by the SCA WG in the **first part of 2007**. Therefore some of the information below is now out-of-date. These analyses are being provided to give the background on the issues that shaped the subsequent first editions of *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards* and the *Registry of USG Recommended Biometric Standards* (Registry)."

Analysis of Issue

The list below enumerates the kinds of options or open-ended issues that the standards leave to the user:

- In the ANSI/NIST-ITL 1-2007 standard, the Type 14 variable resolution fingerprint record has a set of fields that are optional, and the standard assumes that a consumer of the data (e.g. the FBI) would require the presence and legal population of those fields. For example, while the standard allows the original scanning resolution of a fingerprint to be recorded, it does not require it. Along the same lines a fingerprint quality field is provided but not required.
- Again, in reference to Type 14, the record allows variable resolution data. It does not, for example, mandate acquisition at 500 pixels per inch. Instead an application profile or requirements specification should call out 500 ppi, or perhaps 500 and 1000.
- In ISO/IEC 19794-6:2005, a standard for iris image data interchange, there is the possibility to save a captured iris image in one of two formats, rectilinear or polar. The latter requires use of image processing algorithms substantially more complicated than those needed to store the former conventional line scan image.
- In the ISO/IEC 19794-5:2005, a standard for face image data interchange, there is the possibility to allow acquisition of basic, full frontal, or token images. While the former may be non-frontal, the latter two require the subject's face to be frontal (to within specified limits) and this will drive design.

Potential Solutions

Any USG biometric application profile should select the proper parts of relevant standards for the different biometric modalities or for multi-modal biometric data capture and conform to appropriate selected standards. For unforeseen combination of factors, the biometric profile should provide a methodology to determine the proper combinations of parts from the relevant standards and document results. The resulting application profiles will be published as USG best practices.

USG applications should embed strong line-by-line profiling of the standards. As an example the following table shows an extract of the NIST Special Publication 800-76 profile of the INCITS 378-2004 minutiae record. It specifically calls out 500 ppi acquisition (line 22+23) of two index fingers (line 27) that must not be rolled fingerprints (line 29).

Extract of INCITS 378-2004 profile showing refined specification of requirements

Line	Clause of the base standard	Application-specific requirements	Application – Rationale for Requirement
22	X (horizontal) resolution (6.4.9)	500	Parent images must be 500 ppi. This ensures interoperability with legacy data.
23	Y (vertical) resolution (6.4.10)	500	
24	Number of Finger Views (6.4.11)	2	Application requires two finger templates

The information provided in this Annex is a summation of the analyses performed by the SCA WG in the **first part of 2007**. Therefore some of the information below is now out-of-date. These analyses are being provided to give the background on the issues that shaped the subsequent first editions of *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards* and the *Registry of USG Recommended Biometric Standards* (Registry)."

27	Finger Position (6.5.1.1)	1-10	These should be index fingers, but any allowed
29	Impression Type (6.5.1.3)	0 or 2	Flat impressions (not rolled) live or from paper
30	Finger Quality (6.5.1.4)	20,40,60,80,100	A quality values
31	Number of Minutiae (6.5.1.5)	$0 \leq M \leq 128$	Cap the maximum size of the record
36	Extended Data Block Length (6.6.1.1)	0	No proprietary extensions allowed

Each new USG biometric system (or grouping of systems) or application should develop an application profile. The profile should address on a line-by-line basis all the normative clauses of the target standard. Where appropriate:

- Values of parameters should be called-out,
- Normative practice should be called out,
- Informative material should be elevated to normative requirements,
- Normative requirements should be dropped if compliance would be problematic (such a step should be undertaken only with a well document rationale based on empirical evidence). This practice should be undertaken with utmost caution because conformance to the standard may no longer be claimable.

Configurable elements of standards should be specified as part of requirements documents based on operational needs of the implementations.

A.10 Large Scale Identification Applications

Issue

The Electronic Fingerprint Transmission Specification (EFTS) Version 8.0 is the current specification for interfacing with the FBI Integrated Automated Fingerprint Identification System (IAFIS). The EFTS contains a description of operational concepts, descriptors, and field edit specifications, image quality specifications, and other information related to IAFIS services. ANSI/NIST-ITL 1-2000 is specified in EFTS Version 8.0. This is a revision to EFTS Version 7.1. DoD has developed its own EBTS with the goal of being compatible with the FBI's EFTS and EBTS. ANSI/NIST-ITL 1-2000/EFTS Version 7.1 and ANSI/NIST-ITL 1-2007/ EBTS Version 8.0 will need to coexist for some time. A migration strategy for the USG is needed.

Analysis of Issue

The Department of Homeland Security's principal biometric system (IDENT) has moved to the Automated Biometric Identification System (IDENT) Exchange Messages (IXM) Specification.

There is a large movement to move more into the XML based transmission standards but these standards have not been completely flushed out as of yet.

The following standards exist:

- DoJ/FBI/CJIS, Electronic Fingerprint Transmission Specification (EFTS), Version 7.1, May 2005

The information provided in this Annex is a summation of the analyses performed by the SCA WG in the **first part of 2007**. Therefore some of the information below is now out-of-date. These analyses are being provided to give the background on the issues that shaped the subsequent first editions of *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards* and the *Registry of USG Recommended Biometric Standards* (Registry)."

- DoJ/FBI/CJIS, Electronic Biometric Transmission Specification (EBTS) Version 8.0, June 2007
- ANSI/NIST-ITL 1-2000 *Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information*
- ANSI/NIST-ITL 1-2007 Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information
- U.S. Army Biometrics Task Force, Department of Defense Electronic Biometric Transmission Specification, November 2006

The scope of the FBI EBTS has expanded over previous versions to include additional biometric modalities (e.g., palmprint, facial, and iris) in recognition of the rapidly developing biometric identification industry. The most recent update of the ANSI/NIST-ITL 1-2000 (ANSI/NIST-ITL 1-2007) standard includes new record types to facilitate data sharing for new biometric modalities. The FBI EBTS integrates biometric data in accordance with the ANSI/NIST-ITL 1-2007 standard. A logical record Type-99 was added to the ANSI/NIST-ITL 1-2007 standard to contain and exchange biometric data that is not supported by other ANSI/NIST-ITL logical record types (e.g., voice records), thus providing a basic level of interoperability and harmonization with the ANSI INCITS biometric image interchange formats. This is accomplished by using a basic record structure that is conformant with INCITS 398-2005, the Common Biometric Exchange Formats Framework (CBEFF) and a biometric data block specification registered with the International Biometrics Industry Association (IBIA). The Type-99 logical record type was created for "exotic" biometric data types and should not be used for existing ANSI/NIST data types. IAFIS will provide identification services for many of these evolving biometric modalities at some time in the future.

Potential Solutions

USG should support interoperability and harmonization between IDENT and IAFIS and affected systems utilizing XML based transmission standards. The Executive Steering Committee (DHS, DoJ, DoS) for the Interim Data Sharing Model (IDSM) should continue operation. This should addresse:

- Real-time connection of biometric systems operational
- DoJ/FBI/IAFIS 'wanted' data, known and suspected terrorist (KST) data to DHS/US-VISIT/IDENT
- DHS deportation, expedited removal data to FBI
- DoS Category 1 visa refusal information to FBI
- Funding to extend capabilities
- Expanding access to additional Governmental entities

The information provided in this Annex is a summation of the analyses performed by the SCA WG in the **first part of 2007**. Therefore some of the information below is now out-of-date. These analyses are being provided to give the background on the issues that shaped the subsequent first editions of *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards* and the *Registry of USG Recommended Biometric Standards* (Registry)."

DoD/DoJ data linkages should be maintained and promoted, utilizing the DoD data center at FBI/CJIS West Virginia site.

DHS/DoS data linkages should be maintained and promoted, including:

- DoS screening of visa applicants using IDENT
- DHS real-time inspection access to DoS database of visa applicants

Affected agencies should appoint representation to the NSTC Subcommittee on Biometrics and Identity Management as well as to the specific committees and working groups necessary to implement and maintain the capabilities referenced above.

A.11 Smart Cards Applications

Issue

Identity management applications based on user-carried credentials typically store biometric data on un-powered token devices. The archetype here is the ISO/IEC 7816 smart card credential (the US Government PIV card) which is a cryptographically enabled token embedding the cardholder's biometric data. These devices are additionally attractive because a number of FIPS 140-2 certified products exist today.

Analysis of Issue

Smart cards typically offer limited storage. In addition the computational resources needed to implement certain biometric operations and cryptographic encryption and digital signature computations is high and is often dependent on the size of the data in question. For these reasons, it is imperative that the stored biometric data is compact and standardized encodings need to support such constraints.

Potential Solutions

All biometric sample data stored on ISO/IEC 7816 smart cards, whether raw or processed, in standardized or proprietary format, should be stored in conformance with ISO/IEC 7816-11. In such data should be accompanied by digital signatures specified in NIST Special Publication 800-78 as revised.

USG should provide funds to extend MINEX series of evaluations. These should be directed at the identification of fingerprint templates that offer improved interoperability.

NIST should base these evaluations on the elemental minutia representations of the INCITS 378:2004 and ISO/IEC 19794-2:2005 standards.

NIST should identify performance-based improvements to these formats and propagate them through the formal standards development process.

NIST should initiate and support formal standardization of match-on-card evaluations SC 37 Working Group 5.

The information provided in this Annex is a summation of the analyses performed by the SCA WG in the **first part of 2007**. Therefore some of the information below is now out-of-date. These analyses are being provided to give the background on the issues that shaped the subsequent first editions of *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards* and the *Registry of USG Recommended Biometric Standards* (Registry)."

A.12 Mobile and Portable Biometric Devices

Issue

Lightweight, portable fingerprint collection devices are increasingly in operational US Government applications. The US Government maintains large repositories of operational ten-print fingerprint data that is almost universally collected on optical sensors, often EFTS/F certified. The US Government therefore has a compelling objective that data collected on low power devices in the field is interoperable with other systems.

Application of mobile and portable biometric devices for screening and counterterrorism applications and for the agencies within the counterterrorism community, biometrics of known or suspected terrorists (KSTs) can be used to enhance and expand existing watchlist and screening functions.

Standardization will reduce the likelihood of deployment of mobile biometric systems that do not perform in the manner desired or afford interoperability with other systems.

Analysis of Issue

The collection of biometric data is often performed in an uncontrolled environment, particularly when dealing with KSTs. The biometric data itself may be for enrollment and include associated biographic and situation descriptive material or it may be used to check against existing databases to determine if there has been previous contact with this individual (possibly under a different assumed identity). Thus, it is extremely important that the biometric data itself be of the highest possible quality and that the biometric sample be collected in a manner so as to minimize potential harm to the data collector or the subject. The time for collection must be reasonable for the given circumstances. In addition, the biometric sample(s) must be usable in the other systems which might rely upon KST watch lists. All of these issues are important and the adoption and application of relevant standards can significantly improve the likelihood of easier and more accurate/usable data collection efforts.

Potential Solutions

USG should continue to develop and support mobile, rugged, and portable biometric collection devices to work in austere environments. Mobile biometric solutions must demonstrate long operational life as well as rapid and high-quality data capture and collection at stand-off ranges sufficient to ensure operator safety.

USG should develop application profiles describing which parts of existing biometric/ergonomic/safety/security and other relevant standards are applicable for mobile biometric data collection activities. This should address both the 'store and forward' type of operation as well as those with direct/real-time links to databases. It will also need to address local checking against a limited database.

The development of an "application profile" that is required for all procurement of mobile biometric capture devices will ensure that data is collected consistently and in a

usable form. It will also ensure that when mobile devices are used in a verification/identification capability that the probe image is of sufficient quality to be likely to yield a correct match/non-match response from the matchers. This applies to all biometric modalities, including fingerprint, face, iris, voice and DNA.

US Government agencies should field certified devices. The certification procedure should embed the Federal Bureau of Investigation's single finger assessment of the imaging properties of the device and a performance interoperability test.

USG should develop multiple profiles to support various operational requirements for handheld biometric devices. This should be the responsibility for each Agency proposing a system using handheld biometric devices.

The proposed "application profiles" should select the proper parts of relevant standards for the different biometric modalities (and for multi-modal biometric data capture) and map them to generalized mobile scenarios. For unforeseen combinations of factors, the document will provide a methodology to determine the proper combinations of parts from the relevant standards. The resulting "application profile" will be published as a USG standard.

USG should establish a performance-based evaluation program. A submitted capture device should be used in a scenario-test collection conformant to the provisions of ISO/IEC 19795-2. The resulting samples should be assessed for interoperability with optical data conformant in a test conformant to ISO/IEC 19795-4.

NIST should test and publish reports that include empirical data about limited size, resolution, and other factors on performance in order to allow application profile developers to examine trade-offs in the designing of systems for their specific requirements.

A.13 Conformance Testing

Issue

To establish a high level of confidence that standards-based biometric equipment, software and data perform as expected in USG biometric applications, standards based conformity assessment is critical. Standards alone are insufficient to ensure interoperability and proper performance of USG systems, components, and applications.

Analysis of Issue

Conformity testing is the process of testing a technology implementation that claims to support a standard to determine if the implementation adheres to the referenced standard. *Conformance assessment* standards specify the manner in which a conformity assessment should be performed and recorded. Conformance testing captures the technical description of a standard and measures whether an implementation faithfully implements the standard. This is the most obvious type of testing. For instance, when a photograph is taken of an individual, does it meet the requirements for use in a face recognition system? Are there a sufficient number of pixels between the eyes? Is the pose full fontal? Do

biometric data records, data structures and applications conform to required open system standards? Standards-based conformance testing tools help both developers and users by validating conformance claims, leading to greatly increased levels of confidence in products. Conformance testing can also help ensure interoperability between standards-based products and systems.

Standards bodies are developing and have published several conformance testing standards for technical interfaces and data interchange formats applicable for many biometric modalities. However, the USG is unable to verify vendor claims of conformance without established second or third party conformity assessment programs. Although other industries have established conformity assessment programs, this area, while critical, remains undeveloped in the biometrics industry.

There are no ongoing or planned USG second or third party conformity assessment programs. As an initial step, the DoD developed in May 2004 a technical report titled "Biometrics Conformity Assessment Program for DoD". The report details the necessary steps, policies and activities necessary to establish a Biometric Conformity Assessment program within DoD. An article on DoD Biometric Conformity Assessment Initiative has been published in the Defense Standardization Program Journal in April/June 2005 issue.

Potential Solutions

USG should establish Biometric Conformance Assessment (BCA) programs for validating to standards and performance of biometric devices and systems for certain USG biometric applications.

USG should establish a Second- or third-party testing program(s) to achieve a high level of assurance of standards conformance by systems and components required for government standards implementations. USG should ensure that the BCA programs do not rely on vendor claims of conformance since first-party (vendor) testing is not sufficient.

USG should designate a USG entity (or entities) as a Certification Authority within the BCA responsible for evaluation (certification) of test results and for issuance and maintaining of the validated product lists/qualified product lists or certificates of conformance.

Agencies should establish agency requirements and needs for a USG Biometric Conformity Assessment Program.

Agencies should develop a unified Conformity Assessment guidelines document for circulation within the USG.

The information provided in this Annex is a summation of the analyses performed by the SCA WG in the **first part of 2007**. Therefore some of the information below is now out-of-date. These analyses are being provided to give the background on the issues that shaped the subsequent first editions of *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards* and the *Registry of USG Recommended Biometric Standards* (Registry)."

A.14 Performance Testing

Issue

In many large scale USG, cross-border or otherwise federated applications, biometric data captured and processed using one system may later be involved in verification or identification transactions with data collected and processed using another system. For example, fingerprints collected on a mobile sensor might be submitted to an identification system containing sets of fingerprint images captured during consular interviews. This presents interoperability issues:

- Are the sensors interoperable?
- Are the data interchange format standards compatible with one another?

Analysis of Issue

Biometric performance testing is concerned with measurement of the verification and identification error rates, and throughput performance, of biometric algorithms, components, devices and systems.

There are three published standards applicable to performance testing of biometric systems:

- ISO/IEC 19795-1:2006 Biometric Performance Testing and Reporting - Part 1: Principles and Framework
- ISO/IEC 19795-2:2007 Biometric Performance Testing and Reporting - Part 2: Testing Methodologies for Technology and Scenario evaluations
- ISO/IEC 19795-4:2007 Biometric Performance Testing and Reporting - Part 4: Interoperability Performance Testing

The standards are intended to do different things. ISO/IEC 19795-1 is a framework that should be required for all tests. ISO/IEC 19795-2 is appropriate to scenario or technology tests. There are options within ISO/IEC 19795-2 that should be profiled to govern the conduct of just a scenario test or just a technology test.

Potential Solutions

All new USG sponsored or mandated laboratory tests of commercial verification systems should conform to ISO/IEC 19795-1 and the scenario testing provision of 19795-2. When a test does not conform to specific sub-clauses, explanatory statements, excerpting the standard, should be included in the test reports.

All new USG sponsored laboratory tests of matching algorithms should conform to the technology testing provisions of ISO/IEC 19795-2. When a test does not conform to

specific sub-clauses, explanatory statements, excerpting the standard, should be included in the test reports.

All new USG sponsored tests of access control devices should conform to scenario testing provisions of ISO/IEC 19795-2

For all new USG applications, a policy and approach toward operational testing of the fielded system should be formulated. This should address, at least, the procurement of zero or more instances of the system that would be specifically instrumented to support capture of operational samples, and offline analysis thereof.

USG should revisit the above-stated policy on the conduct of the access control tests once the new ISO/IEC 19795-5 Scenario Evaluation of Biometric Access Control Systems has been completed.

USG should develop a strategy approach toward operational testing of potential fielded biometric systems and institute consistent testing procedures to support procurement actions.

Agencies should participate in standards development organizations and should advocate for, and support, tests of the effectiveness of biometric standards both during and after their development.

A.15 Interoperability Testing

Issue

In many large scale USG, cross-border or otherwise federated applications, biometric data captured and processed using one system may later be involved in verification or identification transactions with data collected and processed using another system. For example, fingerprints collected on a mobile sensor might be submitted to an identification system containing sets of fingerprint images captured during consular interviews. This presents interoperability issues:

- Are the sensors interoperable?
- Are the data interchange format standards compatible with one another?
- Are sensors and matching systems by different vendors interoperable?

Analysis of Issue

Biometric interoperability testing is concerned with the ultimate ability of cross-vendor, cross-implementation and cross-format biometric samples to be accurately verified or identified. This might involve assessing sensor performance, the viability of a data interchange format standard, the ability to upgrade a system from one provider to another. Interoperability testing is particularly important when different suppliers and manufacturers may provide software and/or hardware to various parts of the system that is viewed as a whole. The importance of testing is highlighted by this real-life example: At an ICAO NTWG meeting in October 2003, manufacturer representatives claimed to

The information provided in this Annex is a summation of the analyses performed by the SCA WG in the **first part of 2007**. Therefore some of the information below is now out-of-date. These analyses are being provided to give the background on the issues that shaped the subsequent first editions of *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards* and the *Registry of USG Recommended Biometric Standards* (Registry)."

ICAO that their products would be interoperable since they would conform to ICAO-established standards for the chip, data transmission, data format and content as well as for the chip readers. In February 2004 DHS co-sponsored a test session, where manufacturers of chips and readers were invited to demonstrate interoperability. The result was that no chip product was interoperable with the set of chip readers. Subsequent venues allowed manufacturers to develop and test products so that e-passports would be interoperable.

Some tests, such as Minutiae Exchange Interoperability Test (MINEX-conducted by NIST in an on-going basis for fingerprints) can assist in determining the relative levels of performance and interoperability based upon the capture device, minutia extraction and matcher. This concept of allowing vendors to self-test when ready should be expanded to the full range of biometric modalities.

Specific uniform procedures and standards must be established for interoperability testing for a wide variety of biometrics products.

Interoperability testing has been standardized in ISO/IEC 19795-4 FCD Biometric Performance Testing and Reporting - Part 4: Performance Interoperability Testing.

One mechanism to ensure sensor interoperability is to set acceptable minima for the relevant physical properties of the sensor. This has been done by the FBI for fingerprint sensors:

- For ten-print capture, see EFTS Appendix F IAFIS Image Quality Specifications
- For single finger capture see Personal Identity Verification (PIV): Image Quality Specifications for Single Finger Capture Devices.

As another example, NIST Special Publication 800-76-1 cites ISO/IEC 19795-4 to regulate fingerprint minutia interoperability testing.

Potential Solutions

USG should continue to support interoperability and performance testing for large scale biometric and identity management applications to ensure cross-vendor, cross implementation, and cross format biometric samples are accurately verified or identified.

All USG large scale applications, cross-border or otherwise federated applications, involving interoperable data formats, should reference, sponsor or conduct tests conforming to ISO/IEC 19795-4.

USG, and USG agencies participating in standards development organizations, should advocate for, and support, tests of the effectiveness of biometric standards both during and after their development.

Each Agency should institute consistent testing procedures as part of any new biometric application.

The information provided in this Annex is a summation of the analyses performed by the SCA WG in the **first part of 2007**. Therefore some of the information below is now out-of-date. These analyses are being provided to give the background on the issues that shaped the subsequent first editions of *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards* and the *Registry of USG Recommended Biometric Standards* (Registry)."

USG should develop a strategy approach toward operational testing of potential fielded biometric systems and institute consistent testing procedures to support procurement actions.

Agencies should participate in standards development organizations and should advocate for, and support, tests of the effectiveness of biometric standards both during and after their development.

A.16 Security Testing

Issue

Biometric systems may be actively attacked, in an attempt to illicitly gain access (in access control), or to insert/modify/delete identities or to evade detection in a one-to-many search. A number of kinds of attack are known, and these may be modeled in testing. Such testing is distinct from biometric performance testing which usually addresses system or component accuracy and capability.

Analysis of Issue

The principal question is: Does the standard include device attacks or attacks to circumvent portions of the system? This has been addressed by ISO/IEC 19792 Security Evaluation of Biometrics, which is under development in SC 27. It considers active attacks and differentiates between biometric components, systems, and applications. It quantifies security in terms of error rates, including the error rate encountered given specific active impostor attempts. It includes requirements on testing of vulnerability and on protection.

Secure biometric systems begin at conception. Red teaming and security involvement should occur throughout major system development to include system design. Similar efforts should be continually employed against the various underlying biometric algorithms, components, and devices. Red Teaming should also be focused on the underlying IT and telecommunications infrastructure upon which the biometric system rely. (Red teaming is the use of a person or group of people who attempt to defeat a system, reporting back their findings to the system owners/operators).

Certain security systems depend on a biometric comparison to serve as a supplemental authentication factor. The security module may need information from the biometric device concerning the context in which it was tested or certified status. For example, if the device has only been tested to a false acceptance rate of 0.02, this may be insufficient for the high security application.

Potential Solutions

USG should support development and adoption of biometric security testing standards.

USG should conduct security tests of biometric algorithms, components and devices.

USG should formulate a position on the use of such standards as they become available.

The information provided in this Annex is a summation of the analyses performed by the SCA WG in the **first part of 2007**. Therefore some of the information below is now out-of-date. These analyses are being provided to give the background on the issues that shaped the subsequent first editions of *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards* and the *Registry of USG Recommended Biometric Standards* (Registry)."

USG should formulate policy on classification of methods vs. results of such studies.

USG should sponsor specific research into security related properties of algorithms.

The USG should maintain an active role in ISO/IEC JTC 1/SC27.

The USG should review ISO/IEC 19792 Security Evaluation of Biometrics (when published) for applicability in Federal environments and develop a best practices document.

A.17 Establishment of USG QPL Based on Conformance, Performance, and Interoperability Testing

Issue

Presently, there is no commonality in approach across the various USG testing programs and across agencies in developing QPLs or QPL-like lists. This can cause multiple testing of the same product for conformance/performance to the same (or similar) requirements.

Analysis of Issue

In order to ensure that equipment and software is procured that will properly function and meet specifications, pre-qualification of items (based upon specified procedures) may be done. This could result in Qualified Product Lists, Validated Products Lists, Basic Ordering Agreements (IDIQ type of acquisition), or certificates of compliance. For instance, DHS has established a testing program for biometric devices that may be purchased by airport authorities for use in airport access control. The actual testing of devices has been contracted to specific testing laboratories. DHS defines the tests and the test procedures. Another case is GSA and NIST developing test specifications for PIV applications. Yet another example is the testing of slap-print readers according to specifications developed on an interagency basis by DoD, DHS, DoJ/FBI and DoS.

Potential Solutions

USG should examine the principal qualification criteria for product/unit/system qualification, starting with a particular agency. Based upon that agency's findings and any additional information available from other agencies, the Subcommittee should adopt a USG-wide approach to the testing and certification of biometrics-related products/units/systems.

USG should develop a model to establish a consistent testing approach in developing Qualified Product Lists (QPLs) or QPL-like lists that can be used by various programs for selecting biometric products for new applications. USG should examine the principal qualification criteria for product/unit/system qualification, starting with a particular agency. Based upon that agency's findings and any additional information available from other agencies, the Subcommittee should adopt a USG-wide approach to the testing and certification of biometrics-related products/units/systems.

The information provided in this Annex is a summation of the analyses performed by the SCA WG in the **first part of 2007**. Therefore some of the information below is now out-of-date. These analyses are being provided to give the background on the issues that shaped the subsequent first editions of *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards* and the *Registry of USG Recommended Biometric Standards* (Registry)."

Agencies should build upon existing applications such as the PIV (DHS/GSA) and Airport Access Control (DHS/TSA) to use these findings and any additional information available from other agencies, to develop a model and a commonality in approach across the various USG testing programs and across agencies in developing QPLs or QPL-like lists.

A.18 Reference Implementations and Data Sets

Issue

In order for the USG to have a robust testing infrastructure in support of deployment of standards-based biometric applications, there is a need for the availability of high quality reference implementations and standard reference data sets.

Analysis of Issue

An important aspect of developing and improving biometric systems and applications is that of reference implementations. This can take several forms, such as:

- NFIQ (for fingerprint image quality) that allows vendors and/or users to examine the quality of fingerprint samples in a common framework.
- Laboratory mock-ups of typical operational environments (such as a mock port-of-entry inspection station).
- Software and hardware 'duplication' of operating systems (used to test possible enhancements without disrupting the operational system).

By having a standard reference set of data and specified operating conditions, vendors can evaluate their products and product improvements. Reference data sets should be releasable to the biometrics community, but care must be taken to 'anonymize' the data as part of privacy protection guidelines.

Sequestered testing datasets are available, but large-scale test data suites are not (particularly for multi-modal work). This is due to several factors, including the cost of gathering the data; privacy rights of the individuals from whom the samples were taken; administrative requirements; and access rights on data sharing.

Potential Solutions

USG should support development and dissemination of reference data sets for reading, writing and validating conformant instances of the standards.

USG should support development and dissemination of reference data sets for reading, writing and validating conformant instances of the standards.

USG should promote that reference data sets be releasable to the biometrics community, but ensure data sets are utilized in a manner that meets the privacy protection guidelines.

USG should develop public domain software platforms for reference implementation and demonstration prototyping.

The information provided in this Annex is a summation of the analyses performed by the SCA WG in the **first part of 2007**. Therefore some of the information below is now out-of-date. These analyses are being provided to give the background on the issues that shaped the subsequent first editions of *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards* and the *Registry of USG Recommended Biometric Standards* (Registry)."

A.19 Technical Interface

Issue

USG agencies often have requirements for biometric systems that include plug and play capability. This permits agencies to easily/rapidly/seamlessly integrate system components into functioning systems and swap components as needed without losing functionality, such as the ability to achieve data interchange and to protect the biometric data during transmission and storage. Also, USG agencies often have requirements for deploying and invoking biometrics-based identity assurance capabilities that can be readily accessed using web services. The best way to meet these types of requirements is for USG agencies to use appropriate biometric technical interface standards.

Analysis of Issue

Product specific Application Programming Interfaces (APIs) provided with vendor software development kits (SDKs) require application developers and system integrators to develop custom interfaces for each biometric product they use. A biometric API standard known as the Speaker Verification API (SVAPI) was first developed in 1996.

The current BioAPI series of standards support plug and play compatibility by specifying how applications communicate with biometric vendor software in a common way independently of the biometric modality. This supports the swapping of products and incorporation of new products with no application modification. The Common Biometric Exchange Formats Framework (CBEFF) series of standards specify data structures that support multiple biometric technologies in a common way. CBEFF data structures allow exchanging of biometric data and metadata and support security of biometric data in an open systems environment. The Biometric Identity Assurance Services (BIAS) standards define a framework for deploying and invoking biometrics-based identity assurance capabilities that can be readily accessed using web services. The X9.84 and ISO 19092 standards define requirements for the use and management of biometric data and the processes that accompany that use.

Potential Solutions

USG should promote biometric industry product standardization and use of common interface standards such as BioAPI.[7] [8]

[7] Note: This policy does not apply to law enforcement applications and other large-scale identification applications that require conformance to standards such as FBI EBTS V8.0, DoD EBTS V1.2 or ANSI/NIST-ITL 1-2007.

[8] Note: There is no requirement for embedded devices to conform to the current versions of the BioAPI standards. This is deprecated because there would be no favorable cost-benefit.

The information provided in this Annex is a summation of the analyses performed by the SCA WG in the **first part of 2007**. Therefore some of the information below is now out-of-date. These analyses are being provided to give the background on the issues that shaped the subsequent first editions of *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards* and the *Registry of USG Recommended Biometric Standards* (Registry)."

All new USG biometric applications that require plug and play capability without losing functionality (such as may be the case for access control systems) should:

- Require Biometric Information Records (BIRs) conforming to a CBEFF Patron Format (PF) for the processing, exchange, protection, encapsulation, transmission and storage of biometric data. Use existing Patron Formats that permit incorporating in the data structure the required level of additional "processing" and "operational" metadata and data elements that support payload, security/integrity options and creation date/validity period. (Note: Patron Formats specified in INCITS 398, or instantiations of BioAPI BIRs are preferred.). Part 3 of the international version of CBEFF offers other alternatives.
- Encrypt biometric data within the BIRs and sign BIRs by relying on information in the CBEFF BIR Security Block, unless other system security mechanism are already provided by means external to these biometric data structures.
- Require conformance to INCITS 398-2005, Revision 1 Patron Formats for applications that require transmission or storage of BIRs that require clear text biometric headers or making metadata available without processing the record (e.g., for the purpose of indexing BIRs).
- Require conformance to BioAPI standards V1.1 or V2.0 for client-side verification (e.g., enrollment workstation, kiosk) or server-side verification for one-to-one and multi-biometric applications. (Note: The international standard is preferred.)
- Require conformance to SVAPI for applications based only on voice verification.
- Require conformance to the BIAS standard (including the BioAPI requirement) when the application requires the use of biometric technologies in a Service-Oriented Architecture (SOA).

USG agencies should reflect this policy in any agency specific standards adoption process (e.g., DoD DISR, DHS TRM).

Agency standards registries should harmonize with this policy.

A.20 Standardized Measurements for Biometric Sample Quality

Issue

Biometric systems can fail or yield questionable results when sample quality is poor. Biometric sample quality can in large part be ensured by adequate system design. However any inability to regulate the design or the environment, or any adverse behavioral or interactive effects, may cause samples to be ill suited for biometric use despite attempts to follow established procedures.

The information provided in this Annex is a summation of the analyses performed by the SCA WG in the **first part of 2007**. Therefore some of the information below is now out-of-date. These analyses are being provided to give the background on the issues that shaped the subsequent first editions of *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards* and the *Registry of USG Recommended Biometric Standards* (Registry)."

Analysis of Issue

Biometric quality can be quantified by values that are indicative of subsequent matching accuracy. Such quality values, if computed at the time of acquisition, can be used to initiate reacquisition of a sample should the quality be poor. The quality values may also be used to augment subsequent matching processes, or to trigger use of a second biometric modality.

No universally meaningful scale for biometric quality values exists, and a mechanism for tagging samples in the data record with a source designation is only now being standardized. Existing data format standards are under revision to include such attributes. This supports surveying of operational quality and promises increased effectiveness of USG capture, use, and exchange of biometric data.

Biometric sample quality assessment algorithms exist for a number of biometric modalities, both open-source and commercial. The issue of how to conduct a performance test of such algorithms has only recently been investigated and published (NIST, IEEE PAMI, April 2007). A comparative test of such algorithms has never been run, and a standard is warranted to regulate procedures and establish metrics.

Within industry, there are numerous biometric sample quality measurement algorithms. However, the effectiveness of these algorithms in predicting future matching performance has not been evaluated. With the exception of the NIST Fingerprint Image Quality (NFIQ), DoD Fingerprint Image Quality Measurement tool, and DoD prototype Face Image Quality measurement tool, almost all quality tools are proprietary 'black box' implementations with no publicly available performance statistics. As such, it is extremely difficult for the USG to make informed decisions with regard to the deployment of specific quality measurement measures and tools without extensive testing.

Potential Solutions

All new USG applications should compute quality scores of all collected biometric modality samples using a consistent methodology suited for the specific modality. When practical, USG entities must avoid the collection and use of insufficient quality biometric samples, as identified by deployed quality measurement algorithms. Quality measurement algorithm identifiers and quality summary statistic within the range [0-100] should accompany each biometric sample.

USG should continue progress towards Quality Score Normalization Dataset (QSND) standardization methods to ensure a consistent and interoperable interpretation of the quality scores.

USG should develop technical means for detecting defective biometric samples and assessing biometric sample quality. Such capabilities should support accuracy-based interoperable standardization of quality values.

The information provided in this Annex is a summation of the analyses performed by the SCA WG in the **first part of 2007**. Therefore some of the information below is now out-of-date. These analyses are being provided to give the background on the issues that shaped the subsequent first editions of *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards* and the *Registry of USG Recommended Biometric Standards* (Registry)."

USG should establish procedures for evaluating quality assessment implementations in terms of their relation to matching accuracy.

In all new USG biometric applications, the enrollment process should include a quality assessment for each biometric sample and a have a standardized criterion for initiating reacquisition if quality is poor.

All new USG applications should follow the Recommendations on Biometric Quality Summarization across the Application Domain published as NIST Interagency Report 7422.

USG should foster research, development, test and evaluation, and deployment of methods for the rapid detection of defective samples and the quantitative assessment of biometric quality during the acquisition process. This should be done for, at least, fingerprint, facial, iris and speech modalities.

USG should foster research, development, test and evaluation of methods for quantifying quality suitable for human examiner review of samples. USG should support development of methods for appropriate delivery of feedback to users and operators during biometric sample acquisition.

A.21 Human Factors (Usability and Accessibility)

Issue

A system and its components may meet all of the tests mentioned above but still cause system failure. If operators, users and subjects cannot effectively use the system, it is worthless. Usability can include factors such as human factors, accessibility, interpretability of results and instructions, ease of integration, size of unit, required facility modifications for installation, interfaces to existing parts of the system and other factors. The usability factors must be determined for each application; however, some standards can be developed for general types of applications. Human factors and accessibility are particularly good candidates for development of standards. DHS has begun work with NIST in this area.

Some areas of focus for all biometric systems include (but are not limited to):

- Operator interface
- Attended / Unattended / Covert
- Subject Interface
- Acclimated / Non-acclimated
- Cooperative / Non-cooperative / Uncooperative
- Assisted / Non-assisted

- Physical requirements [touching a unit / looking at a camera / …]
- Output
- Presentation of possible matches above a specified threshold
- Ability to interpret results [red/green condition or specified detailed results depending upon the circumstance]
- Etc.

USG agencies have ongoing requirements for biometric systems that are effective and efficient for users and user performance. To address these requirements USG agencies require guidelines for biometric user interfaces and standards for testing the usability of biometric systems in operational environments that measure user performance including timing, quality, and satisfaction.

Analysis of Issue

ISO 9241-11(1998): *Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs) - Part 11: Guidance on Usability* defines usability as "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use". The standard identifies three areas of measurement: effectiveness, efficiency, and user satisfaction, where

1 Efficiency is a measure of the resources expended in relation to the accuracy and completeness with which users achieve goals. Efficiency is related to productivity and is generally measured as task time

2 Effectiveness is a measure of the accuracy and completeness with which users achieve specified goals. Common metrics include completion rate and number of errors.

3 User satisfaction is the degree to which the product meets the users' expectations—a subjective response in terms of ease of use, satisfaction, and usefulness

This standard definition requires identification of the:

- Context of use: The users, tasks, equipment (hardware, software and materials), and the physical and social environments in which a product is used. Examples include: environmental factors such as temperature, humidity, indoors versus outdoors, stationary or mobile system, height of unit, assisted versus unassisted.
- User: The person who interacts with the product. Examples include: users with disabilities, non-English speaking users, cooperative verses un-cooperative users, acclimated versus non-acclimated users.
- Goal: An intended outcome of user interaction with a product. Specific goals relating to user interaction may be referred to as 'task goals'. Examples include: time constraints or the time required to collect biometric samples and the quality threshold for the samples.

- Task: The activities required to achieve a goal. Examples include: the specific process for acquiring the sample, the instructional set, or the order of slaps for fingerprints.

ISO 25062:2006: *Common Industry Format for Usability Testing* provides a standard format for reporting the results of a usability test.

Potential Solutions

USG should include human factors as a significant factor in the design and implementation of any biometric system. Specific design requirement to include at a minimum are:

- Accessibility
- Usability
- Environmental Factors
- Size
- Weight
- Health Effects
- User Interface
- Etc.

USG should have a coordinated interagency strategy for human factors and usability testing for biometric systems that require:

- Identification of the significant characteristics or requirements from the context of use, users, goals and tasks;
- Usability tests to understand the performance implications of these characteristics in terms of efficiency (timing), effectiveness (quality) and user satisfaction;
- Development of standards and/or guidelines that can be instituted in operational environments that compensate for or mitigate the influence of these factors in biometric systems;
- Acceptance test criteria for biometric systems to determine that systems have been tested and meet these standards and requirements before deployment.

USG should support analysis of human factors interfaces to biometric systems and development guidelines for future adoption.

Agencies should work with NIST to coordinate the USG interagency strategy for human factors and usability testing for biometric systems.

The information provided in this Annex is a summation of the analyses performed by the SCA WG in the **first part of 2007**. Therefore some of the information below is now out-of-date. These analyses are being provided to give the background on the issues that shaped the subsequent first editions of *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards* and the *Registry of USG Recommended Biometric Standards* (Registry)."

A.22 Privacy

Issue

Privacy as a term can signify many different concepts, the extraordinary advances and popularity of information technology bring one conceptualization of privacy – information privacy to the forefront of the privacy protection discussion. Biometric information is, by definition, personally identifiable information. Biometric systems use information generated from observing individuals to recognize a particular individual. Since personal information is any information that *could* be used in *any way* to identify an individual, biometric information is personal information even in those situations where the identity of the individual associated with the biometric information is unknown[9].

Analysis of Issue

A privacy assessment of a biometric system should be conducted when there is a direct use of personal information to analyze the impact that the use of this data may have on individual privacy interests and to ensure that personal information is used appropriately.

A privacy assessment should examine the stated purpose of the system and compare the purpose to the underlying authority of the organization and the specific authority for the program office that manages the system. The purpose for the system should align with the program office's specific authority, and the organization's general authority.

Potential Solutions

USG should request agencies to conduct privacy impact assessment to protect personal data for the implementation of any new biometric systems.

Agencies should recognize that biometric data is personally identifiable information and ensure that all applicable privacy compliance requirements are met prior to loading or using biometric data.

Agencies should conduct privacy impact assessment of biometric systems when there is a direct use of personal information to ensure that personally identifiable information is used appropriately.

[9] "Privacy & Biometrics: Building a Conceptual Foundation", September 2006. www.biometrics.gov

Annex B - Acronyms

Acronym / Abbreviation	Definition
AAMVA	American Association for Motor Vehicle Administrators
AHGBEA	Ad-Hoc Group on Biometrics and E-Authentication
ANSI	American National Standards Institute
APB	Advisory Policy Board
BFC	Biometrics Fusion Center (U.S. Army Biometrics Task Force)
BIAS	Biometric Identity Assurance Services
BIP	Biometric Inter-working Protocol
BSP	Biometric Service Provider
BSWG	Biometric Standards Working Group (DoD)
BTF	U.S. Army Biometrics Task Force
CBEFF	Common Biometric Exchange Format Framework
CIO	Chief Information Officer
CJIS	Criminal Justice Information Services Division (FBI)
COTS	Cost Off-the-Shelf
CTS	Conformance Test Suite
DHS	Department of Homeland Security
DISR	DoD Information Technology Standards Registry
DoD	Department of Defense
DoJ	Department of Justice
DoS	Department of State
DoT	Department of Transportation
EBTS	Electronic Biometric Transmission Specification
EFTS	Electronic Fingerprint Transmission Specification
FBI	Federal Bureau of Investigation
FDIS	Final Draft International Standard
FICC	Federal Identity Credentialing Committee
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GOTS	Government Off-the-Shelf
GSA	General Services Administration
HSPD	Homeland Security Presidential Directive
IAFIS	Integrated Automated Fingerprint Identification System
ICAO	International Civil Aviation Organization
ICT	Information and Communications Technologies

Acronym / Abbreviation	Definition
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
INCITS	International Committee for Information Technology Standards
IOE	INCITS Organizational Entity
IPMSCG	Identity Protection and Management Senior Coordinating Group
ISO	International Organization for Standardization
IT	Information Technology
ITL	Information Technology Laboratory
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
JTC	Joint Technical Committee
NBSP	National Biometric Security Project
NIJ	National Institute of Justice
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
NSTC	National Science and Technology Council
NTTAA	National Technology Transfer and Advancement Act
NTWG	New Technologies Working Group
OASIS	Organization for the Advancement of Structured Information Standards
PKI	Public Key Infrastructure
QUAHOG	Ad–Hoc Group on Data Quality
SC	Subcommittee
SDO	Standards-developing organization
TAG	Technical Advisory Group
TBD	To be determined
TBF	The Biometric Foundation
TC	Technical Committee
TF	Task Force
TSA	Transportation Security Administration
USG	U.S. government
US-VISIT	U.S. Visitor and Immigrant Status Indicator Technology
W3C	World Wide Web Consortium
WD	Working draft
WG	Working group
XCBF	XML Common Biometric Format
XML	eXtensible Markup Language

Annex C - Glossary

Acceptance Testing: The process of determining whether an implementation satisfies acceptance criteria and enables the user to determine whether or not to accept the implementation. This includes the planning and execution of several kinds of tests (e.g., functionality, quality, and speed performance testing) that demonstrate that the implementation satisfies the user requirements. *[ISO/IEC 15444-4]*

Accreditation: Procedure by which an authoritative body gives formal recognition that a body or person is competent to carry out specific tasks. *[ISO/IEC - Guide 2]*

Assertion:

a) The specification (description) for testing a conformance requirement. These are specific class of conditions that can be tested. *[NIST]*

b) The specification for testing a conformance requirement in an Implementation Under Test (IUT) in the form defined in [this] standard. *[ISO/IEC 9646-1]*

Certification: Procedure by which a third party gives written assurance that a product, process, or service conforms to specified requirements. *[ISO/IEC - Guide 2]*

Conformance Testing (or conformity testing):

a) Captures the technical description of a specification and measures whether an implementation faithfully implements the specification. *[NIST]*

b) Conformity evaluation by means of testing. *[ISO/IEC - Guide 2]*

Conformity: Fulfilment by a product, process or service of specified requirements. *[ISO/IEC - Guide 2]*

Conformity Evaluation: Systematic examination of the extent to which a product, process or service fulfills specified requirements. *[ISO/IEC - Guide 2]*

Interoperability Testing: The testing of one implementation (product, system) with another to establish that they can work together properly. *[NISTIR 6025]*

Means of Testing: Hardware and/or software, and the procedures for its use, including the executable test suite itself, used to carry out the testing required. *[ISO/IEC 9646-1]*

Performance Testing: Measures the performance characteristics of an Implementation Under Test (IUT) such as its throughput, responsiveness, etc., under various conditions. *[ISO/IEC 15444-4]*

Reference Data: In information technology, reference data is any data used as a standard of evaluation for various attributes of performance. *[NISTIR 6025]*

Reference Implementation: Implementation whose attributes and behavior are sufficiently defined by standard(s), tested by certifiable test method(s), and traceable to standard(s) that the implementation may be used for the assessment of a measurement method or the assignment of test method values. *[NISTIR 6025]*

Robustness Testing: The process of determining how well an implementation processes data which contains errors. *[ISO/IEC 15444-4]*

Test: Technical operation that consists of the determination of one or more characteristics of a given product, process or service according to a specified procedure. *[ISO/IEC - Guide 2]*

Test Assertion: A specification for testing a conformance requirement in an IUT in the form of a software or procedural methods that generate the test results (also named test outcomes or test verdicts) used for assessment of the conformance requirement. *[this M1 Ad Hoc Group]*

Test Case:

a) A description of the actions (e.g., condition of the test, expected results) required to achieve a specific test purpose or combination of test purposes. *[NIST]*

b) A specification of the actions required to achieve a specific test purpose or combination of test purposes. *[ISO/IEC 9646-1]*

Test Method: Specified technical procedure for performing a test. *[ISO/IEC Guide 2]*

Test Procedure: *[definition to be determined in the future]*

Test Purpose: A prose description of a narrowly defined objective of testing, focusing on a single conformance requirement. *[ISO/IEC 9646-1]*

Test Scenario: *[definition to be determined in the future]*

Testing: Action of carrying out one or more tests. *[ISO/IEC - Guide 2]*