Registry of USG Recommended Biometric Standards

Version 3.0

February 8, 2011

NSTC Subcommittee on
Biometrics and Identity Management

1. Introduction

This *Registry of USG Recommended Biometric Standards* (Registry) supplements the *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards*, which was developed through a collaborative, interagency process within the Subcommittee on Biometrics and Identity Management and approved by the NSTC Committee on Technology. This Registry is based upon interagency consensus on biometric standards required to enable the interoperability of various Federal biometric applications, and to guide Federal agencies as they develop and implement related biometric programs.

The Subcommittee's standards and conformity assessment working group is tasked to develop and update the Registry as necessary. The Subcommittee will continuously review the content of this document, and release updated versions as required to assist agencies in the implementation and reinforcement process of biometric standards to meet agency-specific mission needs. The latest version of this document is available on the Federal government's web site for biometric activities at www.biometrics.gov/standards[1].

The maintenance of this Registry is supported by agencies providing appropriate personnel and resources to the Subcommittee's standards and conformity assessment working group. Federal agencies identifying issues with this Registry should notify their representatives to the Subcommittee's standards and conformity assessment working group.

Two other documents support this Registry and the *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards*:

- Supplemental Information in Support of the NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards ;
- Catalog of USG Biometric Product Testing Programs.

In support of specific cross agency biometric data interoperability requirements, this Registry is cited by NATIONAL SECURITY PRESIDENTIAL DIRECTIVE/NSPD -- 59/ HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD -- 24, Biometrics for Identification and Screening to Enhance National Security.

For comments or to obtain additional information about this document, send e-mail to standards@biometrics.gov.

2. Scope

This Registry lists recommended biometric standards for USG-wide use. Only standards finalized and approved by a standards developing organization are eligible for analysis by the Subcommittee. Inclusion of a standard in this Registry requires consensus agreement of USG agencies through the Subcommittee's deliberative process. For dated references to standards, only the edition cited applies. For undated references to standards, the latest edition of the referenced standard (including any amendments) applies.

These recommendations take into account:

- the differences in how criminal identification and civil biometric authentication systems operate;
- the need to accommodate current implementations as well as new implementations;

[1] The latest version of this Registry is also available at www.standards.gov/biometrics.

— the movement to international versions of these national standards.

Therefore, along with recommended biometric standards, some high level guidance is often provided with respect to implementation, migration, and grandfathering of existing implementations. Further guidance may be found in the Supplemental document.

This Registry is divided into sub-registries of standards or profiles for:

— biometric data collection, storage, and exchange standards;

— biometric transmission profiles;

— biometric identity credentialing profiles;

— biometric technical interface standards;

— biometric conformance testing methodology standards;

— biometric performance testing methodology standards.

Additional biometric standards will be added to this Registry as other standards in the above categories (e.g., other modalities, such as DNA) or additional categories (e.g., biometric quality measurement standards) are approved by the standards developers and evaluated by the USG for USG-wide use.

This Registry may have supplements intended for use within specific communities of the USG. For information on the status of any such supplements, send email to standards@biometrics.gov.

3. Verbal forms for the expression of provisions

The following terms are used in this document to indicate mandatory, optional, or permissible requirements:

— the terms “shall” and “shall not” indicate requirements strictly to be followed in order to conform to this document and from which no deviation is permitted;

— the terms “should” and “should not” indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is deprecated but not prohibited;

— the terms “may” and “need not” indicate a course of action permissible within the limits of this document.

4. Terms and definitions

For the purposes of this document, the following terms and definitions apply. The terms are grouped according by conceptual area, not alphabetic order.

— **standard -** document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context. [ISO/IEC Guide 2:2004]

— **base standard** - a fundamental standard with elements that contain options

NOTE Base standards can be used in diverse applications, for each of which it may be useful to fix the optional elements in a standardized profile with the aim of achieving interoperability between instances of the specific application. [ISO/IEC 24713-1]

- **biometric profile** - conforming subsets or combinations of base standards used to effect specific biometric functions

  NOTE Biometric profiles define specific values or conditions from the range of options described in the relevant base standards, with the aim of supporting the interchange of data between applications and the interoperability of systems. [ISO/IEC 24713-1]

- **standards developing organization** - an organization that develops and approves consensus standards

  NOTE Such organizations may be: accredited, such as ANSI accredited INCITS and ANSI accredited NIST ITL; or international treaty based, such as ICAO; or international private sector based, such as ISO/IEC; or a consortium, such as RTIC; or a government agency, such as the DoD, DHS, FBI, and NIST.

- **certification -** third-party attestation related to products, processes, systems or persons [ISO/IEC 17000:2004, Conformity assessment — Vocabulary and general principles**]**

  NOTE 1 Certification of a management system is sometimes also called registration.

  NOTE 2 Certification is applicable to all objects of conformity assessment except for conformity assessment bodies themselves, to which accreditation is applicable.

- **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 2:2004]

- **testing** - action of carrying out one or more tests [ISO/IEC Guide 2:2004]

- **conformance testing** - process of checking, via test assertions, whether an implementation faithfully implements the standard or profile

- **performance testing** - measures the performance characteristics of an implementation such as system error rates, throughput, or responsiveness, under various conditions

- **sample -** raw data representing a biometric characteristic, which is captured and processed by the biometric system or the digital representation of a biometric characteristic used internally by a biometric system

- **template** - encoded representation of features extracted from a sample suitable for direct comparison

- **sample quality –** properties of a biometric sample associated with its fidelity to its source and its expected performance in a verification or identification system

- **sample quality –** one or more measureable properties of a biometric sample that are related to the utility of the sample to a receiving verification or identification system, or forensic examiner

- **signal –** non-image data, possibly multivariate, time series data or spatial data

  EXAMPLE 1 A speech recording

  EXAMPLE 2 The (x,y) coordinates and pressure of a pen in an online handwriting recognition system

- **image** - two or three dimensional spatial data

  EXAMPLE 1 A fingerprint image

  EXAMPLE 2 A three dimensional facial image (i.e. including shape information)

  EXAMPLE 3 Video of a moving face – not necessarily regularly spaced in time.

- **proprietary image** - image format defined in a privately controlled biometric data format specification

- **proprietary signal** - signal format defined in a privately controlled biometric data format specification

- **proprietary templ**ate – supplier-defined representation of a biometric sample, suitable for matching, usually in an unpublished format

- **basic interoperability** - ability of a generator to create samples that can be processed by other suppliers' comparison subsystems, and the ability of a supplier's comparison subsystem to process input samples from other suppliers' generators [INCITS/ISO/IEC 19795-4:2008 [2009] Interoperability Performance Testing]
- **interoperable performance** - performance associated with the use of generator and comparison subsystems from different suppliers
- **native performance** - performance associated with the use of generator and comparison subsystems from a single supplier
- **performance interoperability** - measure of the adequacy of interoperable performance
- **scenario test** - the online evaluation of end-to-end system performance in a prototype or simulated application in which samples collected from test subjects are processed in real time. [ISO/IEC 19795-2:2005 Testing Methodologies for Technology and Scenario Evaluation]

  NOTE Scenario tests are intended for measurement of performance in modeled environments, inclusive of test subject-system interactions. Scenario Testing assesses biometric technologies in a manner representative of the operational application while maintaining control of performance variables.
- **technology test** - the offline evaluation of one or more algorithms for the same biometric modality using a pre-existing or specially-collected corpus of samples
- **operational test** - process used to evaluate a biometric system in the targeted operational environment and population

5. Acronyms and Abbreviations

ABIS	Automated Biometric Identification System
ANSI	American National Standards Institute
APB	Advisory Policy Board
BDB	Biometric Data Block
BIAS	Biometric Identity Assurance Services
BioAPI	Biometric Application Programming Interface
BIR	Biometric Information Record
BSP	Biometric Service Provider
CBEFF	Common Biometric Exchange Formats Framework
CJIS	Criminal Justice Information Services
CTS	Conformance Test Suite
DHS	Department of Homeland Security
DoD	Department of Defense
EBTS	Electronic Biometric Transmission Specification
EFTS	Electronic Fingerprint Transmission Specification
FBI	Federal Bureau of Investigation
FDIS	Final Draft International Standard
FIPS	Federal Information Processing Standard
HSPD	Homeland Security Presidential Directive
IAFIS	Integrated Automatic Fingerprint Identification System
ICAO	International Civil Aviation Organization
IDENT	Automatic Biometric Identification System
IDMS	Identity management system
IEC	International Electrotechnical Commission

INCITS	InterNational Committee for Information Technology Standards
INT-I	Interpol Implementation of the ANSI/NIST ITL 1-2000 Standard
ISO	International Organization for Standardization
ITL	Information Technology Laboratory
IXM	IDENT Exchange Messages
JPEG	Joint Photographic Experts Group
LDS	Logical Data Structure
MINEX	Minutiae Interoperability Exchange Test
MRTD	Machine Readable Travel Document
NGI	Next Generation Identification
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
NSTC	National Science and Technology Council
PIV	Personal Identity Verification
PNG	Portable Network Graphics
RT	Registered Traveler
RTIC	Registered Traveler Interoperability Consortium
SAP	Subject Acquisition Profile
SOAP	Simple Object Access Protocol
TWIC	Transportation Workers Identification Credential
TWPDES	Terrorist Watchlist Person Data Exchange Standard
USG	United States Government
US-VISIT	United States Visitor and Immigrant Status Indicator Technology
WSQ	Wavelet Scalar Quantization
XML	Extensible Markup Language

6. Registry concepts and standards nomenclature

The meanings for the headings of the columns in the following tables are as follows:

Validity Period: This column shall be updated periodically as new or improved standards are developed. This may result in the retirement or deprecation of a standard. In such cases, a migration strategy to facilitate backward compatibility will be needed because standardized data will likely exist in databases or on identity credentials. Agencies engaged in the design of biometrically enabled applications shall adhere to the standards called out below, and shall heed the "validity period" value.

Biometric Data[2]: This column is organized around the kind of data that is being stored. This derives from the particular biometric modalities chosen for an operation. In some cases, feature based data is stored, and thus the column identifies the captured or processed representation of the sample.

Domain of Applicability: The functions of a generic biometric application include an enrollment phase, and a subsequent identification or verification phase. The enrollment phase embeds capture of an initial sample. The capture may be from a cooperative, non-cooperative or uncooperative subject. Enrollment itself is usually an attended operation. These factors influence the selection of an appropriate data interchange standard because conformance to a standard might be unattainable (e.g., non-cooperative imaging will not always yield a frontal face, for example).

Conceptually a general biometric system[3] might execute:

[2] This column appears only for the Biometric Data Collection, Storage, and Exchange Standards.

- data capture;
- transmission;
- image or signal processing;
- data storage;
- matching;
- decision;
- administration;
- interface.

Recommended standards: This column enumerates those standards. The intent is that all biometric samples captured, or otherwise instantiated during the validity period, in a domain of applicability shall be encoded in formal conformity with the identified standards. In cases where two or more standards are specified, either or both may be used. In cases where the standards contain high level options or branches, values are mandated as needed.

Notes: This column provides implementation guidance and caveats on use and non-use of this and other standards. When the column includes guidance and refinements on the use of the standard (e.g., on compression) the use of the word *shall* is normative. That is, when users adopt one of the recommended standards, the guidance is required.

Nomenclature for the ANSI/NIST Standard:

ANSI/NIST ITL X-YYYY Type ZZ					
ANSI	**NIST**	**ITL**	**X**	**YYYY**	**Type ZZ**
The standard is developed under ANSI procedures	The parent standards development body	The laboratory at NIST responsible for the standard development	Either 1 or 2. Part 1 defined the tagged data formats. Part 2 established XML-based formats.	This is the year that the standard was published. Development was generally completed a few months prior.	ZZ is an integer (1-22,99) indicating modality specific parts of the standard.

ISO Standards nomenclature: The ISO standards identified in the following sections carry specific nomenclature. The example in the Table below explains the fields. The base standard, as originally developed in the international body, is shown in bold. The details of any subsequent US adoption which enclose this are shown in normal type.

INCITS/**ISO/IEC 19794-6:2005**[2007][R2010]						
INCITS	**ISO/IEC**	**19794**	**-6**	**2005**	2007	R2010
This is the name of the body in the U.S. that adopts the international standard	**The parent standards development body**	**ISO/IEC 19794 is a multipart data interchange standard**	**The dash six denotes Part 6 which standardizes exchange of iris imagery**	**This is the year that the standard was published. Development was generally completed a few months prior.**	This identifies the year the standard was adopted by the adopter.	Indicates the standard was reaffirmed[4].

For standards that have published amendments, the amendment itself is identified with the following syntax: INCITS/ISO/IEC 19784-1:2006/Amdt. 1 -2007[2008]

[3] This description of biometric systems is expanded upon in ISO/IEC 24713-1:2008, Biometric Profiles for Interoperability and Data Interchange – Part 1: Overview of Biometric Systems and Biometric Profiles

[4] Re-affirmation of a standard reflects the decision of the responsible standards developer to maintain the availability of a standard without any change of its content. Re-affirmation usually indicates that the standard is technically sufficient for near term applications.

7. Biometric data collection, storage, and exchange standards

The biometric standards listed in Table 1 shall be used in all USG applications for which biometric data:

- are copied or moved between systems within an agency;
- are copied or moved to or by agencies;
- persist beyond the interaction of a subject with a sensor or system.

The biometric standards listed below cover:

- fingerprint images;
- latent fingerprint images;
- palm print images;
- fingerprint minutia records;
- facial images;
- iris images.

Standards for other modalities have been approved by the various standards developers. They are not listed here because the imperative for development of this Registry was ongoing or anticipated multi-agency or USG-wide applications. For parties seeking to collect, store and exchange data from modalities not covered by this Registry, they have the option of using standards approved by national or international standards developers[5].

It is assumed that parent applications can properly embed or wrap biometric data formatted according to the standards enumerated below (e.g., FBI's EBTS transactions embedding ANSI/NIST ITL 1-2007 Type 14 fingerprint records). Data records or sets of data records shall not be wrapped in a proprietary wrapper that requires a specific provider's software to decode or encode.

While Table 1 addresses collection, storage and exchange of biometric data, existing transmission profiles such as the FBI's EBTS (see Table 2) might further modify or restrict the recommended standards of Table 1.

Where the Table recommends more than one standard, users should review the standards for suitability to their application and select one or more. Users should predicate such decisions on application-specific constraints, and on current and anticipated exchange requirements.

[5] The DoD tracks biometric standards: See http://www.biometrics.dod.mil/CurrentInitiatives/Standards/dodcollaboration.aspx. For a copy of the DoD's "BIMA Standards Development Status Update" contact standards@biometrics.gov .

Table 1 - Registry of Biometric Data Collection, Storage, and Exchange Standards

#	Validity period	Biometric data	Domain of applicability	Recommended standards	Notes	Implementation Guidance
	Finger and Palm Recognition					
1.	October 2007 – current	Plain or rolled fingerprint images. For latent fingerprint images, see row 2.	Capture, storage and exchange of data (e.g., enrollment or registration)	ANSI/NIST-ITL 1-2007, Type 14	PIV (FIPS 201-1, 2006) requires the use of INCITS 381:2004 for the retention of images. Other standards, or standardized records, including those enumerated below shall not be used as a substitute for the required standard; they may be used only in addition: ANSI/NIST-ITL 1-2007, Type 3, 5 or 6; INCITS 381:2004; INCITS/ISO/IEC 19794-4:2005[2007].	Capture and storage with resolution ≥ 19.69 pixels/mm. When images are captured at 19.69 pixels/mm and compressed with WSQ [WSQ31], the compression ratio shall not exceed 15:1. When images are captured at 39.37 pixels/mm and compressed using JPEG 2000, the compression ratio shall not exceed 15:1. NOTE: While ANSI/NIST-ITL 1-2007 Type 4 remains the predominant format for transmission of rolled fingerprint information, the Type 14 record is recommended because it is: – used for plain impression transactions including segmentation coordinates; – supporting use of high resolution images; – a more flexible format for additional metadata. However, users should check with receiving agencies that they are capable of accepting Type 14 data. NOTE: ANSI/NIST-ITL 1a-2009 is an extension of the table*, Finger*
1XML	December 2008 – current	Plain or rolled fingerprint images	Capture, storage and exchange of data (e.g., enrollment or registration) in XML format.	ANSI/NIST-ITL 2-2008, Type 14	The following XML standards, or standardized records, shall not be used: ANSI/NIST-ITL 2-2008, Type 3, 5 or 6. This requirement deprecates the use of these legacy types in new applications even though ANSI/NIST-ITL 2-2008 included them by default. NOTE: Implementers migrating to ANSI/NIST-ITL 2-2008 should also migrate to Type 14 from Type 4.	

#	Validity period	Biometric data	Domain of applicability	Recommended standards	Notes	Implementation Guidance
						Position Code & Maximum Image Dimensions, in order to include additional finger combinations. The extension is to Table 12 in Part 1 and Table 212 in Part 2. This brings the ANSI/NIST standards into harmony with "*Mobile ID Device Best Practice Recommendation Version 1.0"* (NIST Special Publication 500-280).
2.	October 2007 - current	Latent fingerprints or latent palm print images	Storage and exchange of data (e.g., enrollment or registration)	ANSI/NIST-ITL 1-2007, Type 13	Other standards or standardized records, including those enumerated below shall not be used as a substitute for the required standard; they may be used only in addition: ANSI/NIST-ITL 1-2007, Type 7; INCITS 381:2004; INCITS/ISO/IEC 19794-4:2005[2007]. Other standards, including those enumerated below shall not be used: ANSI/NIST-ITL 2-2008, Types 3, 4, 5, 6, 14, 15, 16 and 99. When latent minutia are extracted from a latent image and encoded in, for example, an ANSI/NIST-ITL 1-2007, Type 9, the parent image shall be retained.	The latent image shall be acquired with a native resolution of 394 pixels/cm or greater. Latent images should be uncompressed. If losslessly compressed, images shall be stored in conformance to the ISO/IEC 15948 format (PNG). Images shall not be compressed using a lossy compression algorithm If reduced resolution versions are prepared (e.g., for transmission) the parent high resolution image shall be retained.
2XML	December 2008 - current	Latent fingerprints or latent palm print images	Storage and exchange of data (e.g., enrollment or registration) in XML format	ANSI/NIST-ITL 2-2008, Type 13	Other standards, including those enumerated below shall not be used: ANSI/NIST-ITL 2-2008, Types 3, 4, 5, 6, 14, 15, 16 and 99. When latent minutia are extracted from a latent image and encoded in, for example, an ANSI/NIST-ITL 2-2008, Type 9, the parent image shall be retained.	
3.	October 2007 –	Palm prints (excluding	Storage and exchange	ANSI/NIST-ITL 1-2007, Type 15	Other standards or standardized records,	Capture and storage with resolution ≥ 197 pixels/cm.

#	Validity period	Biometric data	Domain of applicability	Recommended standards	Notes	Implementation Guidance
	current	latent palm prints)	of data (e.g., enrollment or registration)		including those enumerated below shall not be used as a substitute for the required standard; they may be used only in addition: INCITS 381:2004; INCITS/ISO/IEC 19794-4:2005[2007]. Other standards or standardized records, including those enumerated below shall not be used: ANSI/NIST-ITL 1-2007, Types 3, 4, 5, 6, 13, 14, 16 and 99.	When images are captured at 197 pixels / cm and compressed with WSQ, the compression ratio shall not exceed 15:1. This may be achieved by invoking the WSQ compressor with a target bit rate parameter greater than or equal to 8/15 bits per pixel. When images are captured at 394 pixels/cm and compressed using JPEG 2000 the compression ratio shall not exceed15:1. This may be achieved by invoking the JPEG 2000 compressor with a target bit rate greater than or equal to 8/10 bits per pixel. If images scanned at 1000 ppi and compressed using JPEG 2000 are to be converted to images at 500 ppi and compressed using WSQ, then the MITRE procedures [MITRE1000] shall be followed.
3XML	December 2008 – current	Palm prints (excluding latent palm prints)	Storage and exchange of data (e.g., enrollment or registration) in XML format	ANSI/NIST-ITL 2-2008, Type 15	Other standards or standardized records, including those enumerated below shall not be used: ANSI/NIST-ITL 2-2008, Types 3, 4, 5, 6, 13, 14, 16 and, 99.	
4.	October 2007 – current	Fingerprint minutiae, not latent minutiae For minutiae encoded in latent images, see row 7.	Storage and exchange outside and unrelated to personal identity credentials	INCITS 378:2004 or ANSI/NIST-ITL 1-2007 Type 9, Fields 1-4 and 13-23 or	Other standards or standardized records, including those enumerated below shall not be used as a substitute for the required standard; they may be used only in addition: INCITS/ISO/IEC 19794-2:2005[2008]. If ANSI/NIST-ITL 1-2007 Type 9 is used, vendor blocks (i.e. fields 31 - 125 and 151-175) shall not be used.	Verification applications (e.g., access control or benefits claim verification) shall not use the "vendor-defined extended data" fields of INCITS 378:2004 clause 6.6. Better accuracy will be obtained if, within the target application, it is possible to additionally exchange standardized image

#	Validity period	Biometric data	Domain of applicability	Recommended standards	Notes	Implementation Guidance
				ANSI/NIST-ITL 1-2007 Type 9, Fields 1-4 and 126-150		records, per row 1 of this Table. Identification applications shall use the INCITS 378:2004 standard. This may include proprietary template data in the "vendor-defined extended data" fields of INCITS 378:2004 clause 6.6. Proprietary template data is non-interoperable but some implementations have been shown to have improved accuracy over standardized data alone [MINEX04]. It is usually usable only if the data is prepared and matched by the products of a single supplier. Reliance on such proprietary data will promote vendor lock-in. In order to mitigate this risk, the parent images shall be retained. To eliminate this risk, standardized image records should be exchanged, per row 1 of this Table. To avoid abuse of this allowance of proprietary data, the standardized minutiae data required by clauses 6.1 through 6.5 of INCITS 378:2004 should be produced by MINEX compliant template generators.
4 XML	December 2008 – current	Fingerprint minutiae encoded in XML. For minutiae encoded in latent images, see row 7.	Storage and exchange outside and unrelated to personal identity credentials	ANSI/NIST-ITL 2-2008 Annex G XML encoding of INCITS 378:2004 or ANSI/NIST-ITL 2-2008 Type 9, per Tables 216a and 216b	If ANSI/NIST-ITL 2-2008 Type 9 is used, vendor blocks (i.e. fields 31 - 125 and 151-175) shall not be used.	
5.	October 2007 – current	Fingerprint minutiae	Storage in, and transmission to, personal identity credentials for match-on-	INCITS/ISO/IEC 19794-2:2005[2008], clause 8 compact card format with clause 9 format	INCITS/ISO/IEC 19794-2:2005[2008] (compact card format) shall be stored on the card for match-on-card. INCITS/ISO/IEC 19794-2:2005[2008] (compact card format) shall be sent to the card for verification against the reference template on the card.	

#	Validity period	Biometric data	Domain of applicability	Recommended standards	Notes	Implementation Guidance
			card	types 0001, 0003, 0005	In both cases the minutiae may be prepared from parent INCITS 378:2004 records. For match-on-card, neither INCITS 378:2004 nor INCITS/ISO/IEC 19794-2:2005[2008] clause 7 (record format) shall be stored on the card. For match-on-card, neither INCITS 378:2004 nor INCITS/ISO/IEC 19794-2:2005[2008] clause 7 (record format) shall be sent to the card. Regarding INCITS/ISO/IEC 19794-2:2005[2008] card formats, the absence of a header and ambiguities inherent in the sort-ordering of minutiae mean that such records shall not be used for persistent storage off-card. ANSI/NIST-ITL 1-2007 and ANSI/NIST-ITL 2-2008 shall not be used.	
6.	October 2007 – current	Fingerprint minutiae	Storage in, and transmission from, personal identity credentials for match-off-card	INCITS 378:2004	In match-off-card applications, none of the INCITS/ISO/IEC 19794-2:2005[2008] formats shall be used. This applies to both the reference and verification templates. ANSI/NIST-ITL 1-2007 and ANSI/NIST-ITL 2-2008 shall not be used.	
7.	October 2007 – current	Latent fingerprint minutiae	Storage and exchange of data (e.g., enrollment or registration)	ANSI/NIST-ITL 1-2007, Type 9, Fields 1-4 and 13-23 or ANSI/NIST-ITL 1-2007 Type 9, Fields 1-4 and 126-140	Other standards, including those enumerated below shall not be used as a substitute for the required standard; they may be used only in addition: INCITS 378:2004.	Standardized minutiae records afford only limited automated matching accuracy, and therefore parent latent images shall be retained with any extracted minutiae. Fields 13-23 are defined in Appendix J of the FBI's EBTS.

#	Validity period	Biometric data	Domain of applicability	Recommended standards	Notes	Implementation Guidance
7 XML	October 2007 – current	Latent fingerprint minutiae encoded using XML	Storage and exchange of data (e.g., enrollment or registration)	ANSI/NIST-ITL 2-2008, Type 9, Tables 216a and 216b		
	Face Recognition					
8.	October 2007 – current	2D Face images	Storage of digital images in personal identity credentials	INCITS/ISO/IEC 19794-5:2005[2007], Full Frontal or Token	The INCITS/ISO/IEC 19794-5:2005[2007] "basic" mode shall not be used. INCITS 385:2004 shall not be used. ANSI/NIST-ITL 1-2007 and ANSI/NIST-ITL 2-2008 shall not be used. The following informative material should be consulted. For general case: INCITS/ISO/IEC 19794-5: 2005/Amd 1:2007 [2009] adds an Annex to the base standard as guidance for producing or requiring either conventional printed photographs or digital images of faces that may be used in applications for passports, visas, or other identification documents and when those images are required to conform to the frontal image types of this standard (INCITS/ISO/IEC 19794-5:2005[2007]).	
9.	October 2007 - current	2D Face images	For capture and storage in MRTDs (e.g., e-Passport chip reading)	ICAO 9303 and Supplement	ICAO 9303 covers capture, storage and transmission. INCITS 385:2004 shall not be used. ANSI/NIST-ITL 1-2007 and ANSI/NIST-ITL 2-2008 shall not be used.	
10.	October 2007 - current	2D Face images	Capture and storage (i.e., enrollment or	ANSI/NIST-ITL 1-2007, Type 10 with subject	Other standards or standardized records, including those enumerated below shall not be used:	Failure to conform to the quality-related requirements of these standards will undermine

#	Validity period	Biometric data	Domain of applicability	Recommended standards	Notes	Implementation Guidance
			registration processes) for which end-to-end subject capture times above 120 seconds are tolerable	acquisition profile (SAP) of level 10 or above or INCITS/ISO/IEC 19794-5:2005[2007], Full Frontal or Token, with at least 90 pixels between the eyes from all subjects	INCITS 385:2004 ANSI/NIST-ITL 1-2007, Types 7, 16 and 99.	facial recognition performance. INCITS/ISO/IEC 19794-5: 2005/Amd 1:2007 [2009] should be consulted. It adds an Annex to the base standard as guidance for producing either conventional printed photographs or digital images of faces that may be used in applications for passports, visas, or other identification documents.
10 XML	December 2008 - current	2D Face images encoded in XML	Capture and storage (i.e., enrollment or registration processes) for which end-to-end subject capture times above 120 seconds are tolerable	ANSI/NIST-ITL 2-2008, Type 10 with subject acquisition profile (SAP) of level 10 or above	Other standards or standardized records, including those enumerated below shall not be used: ANSI/NIST-ITL 2-2008, Types 7, 16 and 99.	
11.	October 2007 – current	2D Face images	Non-cooperative or uncooperative capture and storage of images	ANSI/NIST-ITL 1-2007, Type 10 with subject acquisition profile (SAP) of level 1 or above or INCITS/ISO/IEC 19794-	For images collected in applications in which subjects are imaged in a non-cooperative or uncooperative manner. The acquisition should be frontal when possible. Other standards or standardized records, including those enumerated below shall not be used: INCITS 385:2004 ANSI/NIST-ITL 1-2007, Types 7, 16 and 99.	

#	Validity period	Biometric data	Domain of applicability	Recommended standards	Notes	Implementation Guidance
				5:2005[2007] Basic type only		
11 XML	December 2008 – current	2D Face images	Non-cooperative or uncooperative capture and storage of images	ANSI/NIST-ITL 2-2008, Type 10 with subject acquisition profile (SAP) of level 1 or above	For images collected in applications in which subjects are imaged in a non-cooperative or uncooperative manner. The acquisition should be frontal when possible. Other standards or standardized records, including those enumerated below shall not be used: ANSI/NIST-ITL 2-2008, Types 7, 16 and 99.	
12.	October 2007 – current	2D Face images	All other capture, storage or exchange applications	ANSI/NIST-ITL 1-2007, Type 10 with subject acquisition profile (SAP) of level 1 or above or INCITS/ISO/IEC 19794-5:2005[2007], Basic, Full Frontal or Token	Conformance to the ANSI/NIST-ITL 1-2007 SAP level 1 and the INCITS/ISO/IEC 19794-5:2005[2007] "Basic" type allows storage of an arbitrarily poor photograph whose digital, scene, photometric and geometric properties are unlikely to yield acceptable face recognition accuracy. Other standards or standardized records, including those enumerated below shall not be used: INCITS 385:2004 ANSI/NIST-ITL 1-2007, Types 7, 16 and 99.	
12 XML	December 2008 - current	2D Face images	All other capture, storage or exchange applications	ANSI/NIST-ITL 2-2008, Type 10 with subject acquisition profile (SAP) of level 1 or above	Conformance to the ANSI/NIST-ITL 2-2008 SAP level 1 allows storage of an arbitrarily poor photograph whose digital, scene, photometric and geometric properties are unlikely to yield acceptable face recognition accuracy. Other standards or standardized records, including those enumerated below shall not be used: ANSI/NIST-ITL 2-2008, Types 7, 16 and 99.	
	Iris Recognition					
13.	October	Iris images	Capture,	The rectilinear	Other standards or standardized records,	If lossy compression is applied to

#	Validity period	Biometric data	Domain of applicability	Recommended standards	Notes	Implementation Guidance
	2007 – current		storage and exchange of data (e.g., enrollment or registration)	image format of INCITS/ISO/IEC 19794-6:2005[2007] or ANSI/NIST-ITL 1-2007, Type 17	including those enumerated below shall not be used: INCITS 379:2004 (standard withdrawn 2008) ANSI/NIST-ITL 1-2007, Types 7 and 16. The ANSI/NIST-ITL 1-2007, Type 17 format is a strict derivative of INCITS/ISO/IEC 19794-6:2005[2007], and may be used as an alternative. Other standards, including those enumerated below shall not be used as a substitute for the required standard; they may be used only in addition: All ISO/IEC 19794-6:2005 polar image formats. Irises stored in any of the polar image formats of INCITS/ISO/IEC 19794-6:2005[2007] may be retained only if their rectilinear image parents are also retained.	iris images the compression ratio shall not exceed 6:1. For compression algorithms without a bit-rate parameter (e.g., JPEG), this may require iteration over the compression "quality" parameter.
13 XML	December 2008 – current	Iris images encoded in XML	Capture, storage and exchange of data (e.g., enrollment or registration)	ANSI/NIST-ITL 2-2008, Type 17	The ANSI/NIST-ITL 2-2008, Type 17 format is a strict derivative of INCITS/ISO/IEC 19794-6:2005[2007], and may be used as an alternative. Other standards or standardized records, including those enumerated below shall not be used: ANSI/NIST-ITL 2-2008, Types 7 and 16.	

8. Biometric transmission profiles

To facilitate interoperability, biometric base standards, such as the Biometric Data Collection, Storage, and Exchange Standards in Table 1, should normally be used in conjunction with a biometric profile. Such profiles specify application-specific criteria onto the base standard. This profiling could consist of establishing definitive values for performance related parameters in the base standard (e.g., resolution, maximum compression) or enumerating values for optional or conditional requirements (e.g., full-frontal face vs. token face in INCITS/ISO/IEC 19794-5:2005[2007]).

Biometric profiles developed for USG applications should address, on a clause-by-clause basis, all the normative requirements of the base standards, and where appropriate:

- call out values of parameters (e.g., number of finger);
- call out normative practice (e.g., encoding of core and delta positions in minutia records);
- promote informative material to become normative requirements (e.g., maximum face image compression ratios);
- demote normative requirements if compliance would be problematic. Such a step shall be undertaken only after an evidence-based justification can be established and documented. This practice should be undertaken with utmost caution because it breaks conformance to the standard, and may undermine interoperability.

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

Proprietary data

Some of the base standards enumerated in this document include fields for additional proprietary data. A biometric profile should disallow population of these fields because proprietary data is non-interoperable and is likely to be used in preference to standardized data thereby subverting interoperability via vendor lock-in.

USG applications shall not use proprietary image or signal formats when a national or international standard exists for images or signals related to that biometric.

Proprietary extensions

USG applications should generally prohibit inclusion of proprietary data in standardized records that contain standardized data. Applications may embed proprietary templates, and achieve interoperability at the image-level.

Biometric Profiles and Data Models for Large Scale Identification Applications

The biometric transmission profiles of Table 2 are specifications developed by federal and international organizations that permit electronic communication with the specified system. These documents are not base standards but are critical because they define current ("as is") technical requirements that facilitate interoperability.

Federal Bureau of Investigation

Prior to 2007, the Electronic Fingerprint Transmission Specification (EFTS 7.1) in conjunction with the ANSI/NIST-ITL 1-2000 standard was used to support the FBI's IAFIS system. Since then, the IAFIS has been enhanced with additional functionalities including new biometric modalities specified by the Next Generation Identification (NGI). To acknowledge additional processing capabilities and these new biometric modalities, the Electronic Biometric Transmission Specification (EBTS 8.0) was introduced in September 2007. As NGI evolves over time, incremental enhancements are developed and installed. The EBTS is being continually updated to keep pace with these newly installed NGI enhancements. In order to properly interface with the NGI, each revision is fully backward compatible with earlier revisions and with the EFTS. The EBTS's scope continues to be expanded over previous versions to include additional biometric modalities (e.g., palmprint,

facial, and iris) in recognition of the rapidly developing biometric identification industry. This allows the FBI to move toward a capability that will facilitate multimodal biometric searching of its databases. EBTS 9.1 is the current version being used to interface with NGI. It inherits the basic requirements for logical records set forth in the ANSI/NIST-ITL 1-2007 standard.

Department of Defense

The DoD EBTS was originally developed as an interface to the DoD Automated Biometric Identification System (ABIS). The DoD ABIS is an electronic database and an associated set of software applications that support the storage, retrieval, and searching of fingerprint and latent data collected from persons of national security interest. The DoD ABIS was designed to be similar to the FBI Criminal Justice Information Services (CJIS) Integrated Automated Fingerprint Identification System (IAFIS) and therefore its interface was based on the FBI's Electronic Fingerprint Transmission Specification (EFTS). Because of the different nature of DoD encounters and detainment circumstances, the DoD has additional operational requirements beyond those defined in the FBI EFTS. The DoD-unique capabilities are defined in the DoD EBTS.

Following extensive expert review and multiple revisions, the first widely distributed version (version 1.2) of the DoD EBTS was released in November 2006. That document described a set of capabilities that had been implemented in the DoD Biometric Enterprise as well as defining future capabilities.

DoD EBTS version (v) 1.2 was based on the FBI Electronic Fingerprint Transmission Specification (EFTS) v7.0 and ANSI/NIST-ITL 1-2000. Since the release of DoD EBTS v1.2, a number of events have shaped the release of a new version of the DoD EBTS—version 2.0:

- As biometric support for various DoD mission activities has evolved, so have the requirements for a more flexible standard. As result, the scope of DoD biometric data collection and sharing has expanded to a wider range of operational scenarios. This broader set of scenarios necessitated the use of a mechanism to tailor the DoD EBTS to individual applications. This mechanism is called an "application profile," which is an addition to the base DoD EBTS document. It is used to describe customizations for individual operational scenarios that make use of the DoD EBTS. The concept of an application profile is described in Section 2.1.
- Data elements pertaining to biometric data collection and sharing have been defined in a Glossary, a Data Dictionary, and a Data Model. All of the data elements used in the DoD EBTS v2.0 are defined in the Integrated Data Dictionary v2.2.1.
- ANSI/NIST-ITL 1-2000 was updated to ANSI/NIST-ITL 1-2007 Part 1. FBI EFTS v7 was updated to FBI EBTS v8 to reflect ANSI/NIST ITL-1 2007 Part 1.
- The DoD ABIS has evolved into the Next Generation ABIS (NG-ABIS), which provides additional functionality such as searching of iris images and face images. Additionally, the DoD EBTS needs to be usable for communications with DoD biometric repositories in addition to DoD ABIS (or NG-ABIS).

Department of Homeland Security

The Automated Biometric Identification System (IDENT) Exchange Messages (IXM) Specification is the transmission profile required for communicating with US-VISIT systems. It establishes common interface specifications and mechanisms for new US-VISIT systems users; leverages existing data models and standards such as ANSI/NIST-ITL 1-2007, FBI EFTS v7.1, FBI EBTS v8.1; and leverages existing Web services specifications and technology for binary data transmission. Since the release of version 3.1 of IXM, IDENT services have been expanded; the most recent version of IXM (v5.5) reflects changes to v3.1 to add new services and options that address the expanding needs of US-VISIT stakeholders.

US-VISIT originally developed and implemented the IXM specification according to the Global Justice XML Data Model (GJXDM). In addition to IXM, US-VISIT supports other, legacy transmission profiles and standards for several of its stakeholders. IXM offers two methods for transferring data: (1) embedding an ANSI/NIST-ITL record in a lightweight XML wrapper and (2) encoding data directly in XML. The lightweight XML wrapper maintains the structure of the embedded ANSI/NIST-ITL record and its tagged field format data are parsed and processed by US-VISIT systems. The second XML method – encoding data directly in XML – allows a more direct interpretation of the data and accommodates greater flexibility for data definitions.

US-VISIT is collaborating with the FBI and DOD to develop full interoperability between US VISIT systems, the FBI's Integrated Automated Fingerprint Identification System (IAFIS) and the DOD ABIS. IXM is currently being revised to accommodate additional modalities and to be interoperable with several additional international partners. It will continue to support legacy transmission profiles and will be updated to be compatible with the changes being developed by NIST, the FBI, DOD, and other stakeholders.

Intelligence Community

The Terrorist Watchlist Person Data Exchange Standard (TWPDES) provides a comprehensive XML based standard for exchanging and sharing terrorist-related information across the entire intelligence and law enforcement communities, both in the United States and abroad with biometric and biographic support in a single package. It incorporates the ANSI/NIST-ITL 2-2008 standard for biometric identifiers and is NIEM compliant. This standard was originally developed by the Intelligence community to exchange information about terrorists in XML.

TWPDES 3.0 (TWPDES) is a minor upgrade of 1.2b both are NIEM 2.0 compliant and support all terrorist, screening and watchlisting requirements and encounter scenarios in the communities. TWPDES 3.0 makes minor technical corrections and contains updated references to external standards including biometric descriptors. Users may constrain the standard to support only the specific requirements in the users' domain. The specification also has built-in extension mechanisms that can be used for inter-agency terrorist-data exchange models. TWPDES 1.2b has been accepted by DHS, DoD, and DOJ as a recognized standard for exchanging data. TWPDES 3.0 was approved December 29, 2010 and has been accepted by ODNI, DHS and FBI. TWDES 3.0 is specified by the State and Local Fusion Center standard for transmission of positive encounters created by the Bureau of Justice Assistance.

Table 2 - Registry of Biometric Transmission Profiles

#	Validity period	Domain of applicability	Recommended Transmission Profiles	Notes
1.	May 2008 – December 2009	Applications sharing data with the U.S. Government's intelligence community and law enforcement.	TWPDES 1.2b	This version supersedes versions 1.0, 1.1, 1.2a and 2.0.
2.	December 2009 -- current	Applications sharing data with the U.S. Government's intelligence community and law enforcement.	TWPDES 3.0	This version supersedes version 1.2b and Is a minor update to TWPDES 1.2b. There are no updates currently planned.
3.	Through October 2008	Applications exchanging data with the FBI IAFIS/NGI identification	FBI EFTS Version 7.1	Superseded by FBI EBTS Version 8.1. FBI EFTS v7.1 exists within this registry for backwards compatibility with legacy systems.

#	Validity period	Domain of applicability	Recommended Transmission Profiles	Notes
		system		
4.	October 2007 – November 2009	Applications exchanging data with the FBI IAFIS/NGI identification system	FBI EBTS Version 8.1	The Criminal Justice Information Services (CJIS) Advisory Policy Board (APB) has recently approved the FBI EBTS Version 8.1 for interfacing with the FBI Integrated Automated Fingerprint Identification System (IAFIS) and its successor Next Generation Identification (NGI). Version 8.1 offers a superset of the functionality provided by prior versions. Version 8.1 is backward compatible with prior versions. In any case version 8.1 should be adopted for new applications.
5.	December 2009 – April 2010	Applications exchanging data with the FBI IAFIS/NGI identification system	FBI EBTS Version 9.0	Reorganization of document into NGI Core User Services. Removal of all TOTs listed for "Future Capability". Additional new section for card scanning. Additions and modifications to the appendices.
6.	May 2010 - current	Applications exchanging data with the FBI IAFIS/NGI identification system	FBI EBTS Version 9.1 Or FBI EBTS Version 9.1 XML	Ensure references, wording, definitions, and descriptions are compatible with ANSI/NIST 2007. Changes to RISC notifications. Clarifications for certain TOTs. Changes to appendices.
6.	October 2007 – June 2010	Applications exchanging data with the DoD ABIS identification system	DoD EBTS v1.2	DoD EBTS v1.2 is a superset of the FBI EFTS v7.1 for DoD-specific needs. DoD EBTS v1.2 preceded the development of FBI EBTS v8.001.
7.	June 2010 – current	Applications exchanging data with the DoD ABIS identification system	DoD EBTS v2.0	DoD EBTS v2.0 implements ANSI/NIST ITL1-2007.
8.	September 2007 – current	Applications exchanging data with the DHS IDENT identification system	IDENT eXchange Messaging (IXM) version 5.5	The IXM specification provides detailed information on messaging operation, and steps required to create an interface for external users to interact with US-VISIT/IDENT applications.
9.	October 2005 – November 2010	Applications exchanging data with the Interpol identification system	Interpol Implementation of ANSI/NIST-ITL 1-2000 (INT-I)	This standard is used to transmit information between nations for international law enforcement.
10	June 2010 - current	Applications exchanging data with the Interpol identification system	Interpol Implementation of ANSI/NIST-ITL 1-2007 (INT-Ib)	This revision are valid - 5.0 Oct 23, 2008 are current – The new version supports transmission of iris data.

9. Biometric identity credentialing profiles

The FIPS 201 standard specifies the architecture and technical requirements for a common identification standard for all US Government employees and contractors. It contains two major sections. Part one describes the requirements for a

personal identity verification system that meets the control and security objectives of Homeland Security Presidential Directive 12, including personal identity proofing, registration, and issuance. Part two provides detailed specifications that will support technical interoperability among PIV systems. It describes the card elements, system interfaces, and security controls required to securely store, process, and retrieve identity credentials from the card. The interfaces and data formats of biometric information are specified in NIST Special Publication 800-76-1, Biometric Data Specification for Personal Identity Verification.

The TWIC Reader Hardware and Card Application Specification leverages FIPS 201. For all transportation workers requiring unescorted physical and/or logical access to national facilities, the TWIC design defines the behavior at the card interface of the TWIC card application as well as the requirements for TWIC smart card readers to be used with the TWIC.

Similarly the Registered Traveler Technical Interoperability Specification leveraged the FIPS 201 standard to specify the identify management infrastructure requirements for a fully-interoperable, vendor-neutral RT program within the United States.

The biometric credentialing profiles of Table 3 should be considered for all USG applications.

Table 3 - Registry of Biometric Identity Credentialing Profiles

#	Validity period	Domain of applicability	Recommended standards	Notes
1.	October 2007 – current	Personal identity verification	FIPS 201-1, 2006 NIST SP 800-76-1, 2007	HSPD-12 is applicable to Federal employees and contractors. Applicability to other agency specific categories of individuals (e.g., short-term (i.e., less than 6 months) guest researchers; volunteers; or intermittent, temporary or seasonal employees) is an agency risk-based decision. The TWIC and RT specifications are based upon the PIV standards (FIPS 201, and supporting NIST Special Publications) with certain extensions and modifications for their unique application environment.
2.	October 2007 – current	Registered travelers	Registered Traveler Interoperability Consortium *Technical Interoperability Specification Version 1.7* April 15, 2008	Version 1.0 of this Registry recommended Registered Traveler Interoperability Consortium *Technical Interoperability Specification Version 1.5* December 21, 2007

10. Biometric technical interface standards

The biometric technical interface standards listed in Table 4 shall be used in all USG applications for biometric systems that include “plug and play” capability. This permits agencies to easily, rapidly and 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.

The BioAPI 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 CBEFF standards specify data structures that support multiple biometric technologies in a common way. CBEFF's data structures, termed BIRs, conform to a CBEFF Patron Format which allows exchange of biometric data and related metadata (e.g., time stamp, validity period, and creator) and support security of biometric data in an open systems environment.

The BIAS standard defines biometric services used for identity assurance that are invoked over a services-based framework. It is intended to provide a generic set of biometric and identity-related functions and associated data definitions to allow remote access to biometric services.

Table 4 - Registry of Biometric Technical Interface Standards

#	Validity period	Domain of applicability	Recommended standards	Notes
1.	October 2007 - current	For plug and play functionality in client-side capture and verification (e.g., enrollment workstation, kiosk) or server-side verification for one-to-one and multi-biometric applications. This is not applicable for embedded systems.	INCITS/ISO/IEC 19784-1:2006[2007] INCITS/ISO/IEC 19784-2:2007[2008]	A framework component for INCITS/ISO/IEC 19784-1:2006[2007] is commercially available (i.e., license fee), which can serve the same purpose as a publicly available reference implementation. A graphical user interface specification, BioGUI, is available as INCITS/ISO/IEC 19784-1:2006/Amdt 1 - 2007[2008]. This allows the application to control the user interface to tailor the 'look and feel' of the biometric capture windows to the business application (e.g., for operational efficiency and training purposes). ISO/IEC 19784-1:2006, Amd. 2:2009 [2009] defines a Framework Free BioAPI that support use of a minimal number and type of biometric devices or algorithms or when resource constraints exist which contraindicate use of the ISO/IEC 19784-1 framework. ISO/IEC 19784-3 Amd. 3 is available for applications that use BioAPI and ISO/IEC 24761, Information technology -- Security techniques -- Authentication context for biometrics (ACBio) – developed by JTC 1/SC 27. This allows passing of encryption/signing of data across the API boundary. NIST and DoD have publicly available Conformance Test Suites (CTSs)[6] to test Biometric Service Providers that claim conformance to INCITS 358:2002 [R2007]. No publicly available CTSs are known to be available for ISO/IEC 19784-1.
2.	October 2007 – November 2010	For plug and play functionality in client-side capture and verification (e.g., enrollment workstation, kiosk) or server-side verification for one-to-one and	INCITS 358:2002	INCITS 358:2002 [R2007] shall only be used instead of ISO/IEC 19784 in the case where the existence of a publicly available reference implementation for INCITS 358:2002 [R2007] is required. There are no such reference

[6] http://www.itl.nist.gov/div893/biometrics/BioAPI_CTS/index.htm and http://www.biometrics.dod.mil/CurrentInitiatives/Standards/BioAPI/Default.aspx

<table>
<tr><th>#</th><th>Validity period</th><th>Domain of applicability</th><th>Recommended standards</th><th>Notes</th></tr>
<tr><td></td><td></td><td>multi-biometric applications. This is not applicable for embedded systems.</td><td></td><td>implementations of ISO/IEC 19784.</td></tr>
<tr><td>3.</td><td>October 2007 – current</td><td>Biometric Information Records conforming to a CBEFF Patron Format for the exchange, protection, encapsulation, transmission and storage of biometric data

Encrypt and sign biometric data contained in Biometric Data Blocks in CBEFF BIRs by relying on the BIR Security Block, unless other system security mechanisms are already provided by means external to the BIR

Patron Formats for applications that require transmission or storage of BIRs that require cleartext biometric headers or making metadata available without processing the record (e.g., for the purpose of indexing BIRs)

This does not apply to law enforcement applications and other large-scale identification applications that require conformance to biometric profiles such as FBI EBTS.</td><td>INCITS 398:2008</td><td>Although the user can specify a new Patron Format, those specified in INCITS 398:2008 are preferred:

In addition to citing the INCITS 398:2008 standard, parties to a biometric interchange shall agree on a Patron Format. The ones specified in the standard are tabulated below.

<table><tr><th>#</th><th>Name</th><th>Domain</th></tr><tr><td>1</td><td>Patron Format A</td><td>General purpose - See NOTE 1.</td></tr><tr><td>2</td><td>BioAPI BIR</td><td>BioAPI Interfaces</td></tr><tr><td>3</td><td>ICAO LDS</td><td>e-Passports / MRTDs</td></tr><tr><td>4</td><td>PIV</td><td>PIV</td></tr><tr><td>5</td><td>ANSI/NIST Type 99</td><td>Other modalities</td></tr><tr><td>6</td><td>Patron Format B</td><td>Complex structures</td></tr></table>
NOTE 1 NIST has a publicly available conformance testing architecture and Conformance Test Suite (CTS)[7] to test implementations of Patron Format A.</td></tr>
<tr><td>4.</td><td>October 2007 – current</td><td>Biometric services for identity assurance that are invoked over a services-based framework</td><td>INCITS 442:2008</td><td></td></tr>
</table>

11. Biometric conformance testing methodology standards

Conformance testing methodology standards may specify physical test requirements, logical test requirements (e.g., test assertions, test cases), use of reference data, test reporting formats, and means of testing requirements. Such standards can serve as the basis for the development of test tools (e.g., executable test code, reference data) and reference implementations, which can be used by organizations operating conformance testing programs.

The biometric conformance testing methodology standards listed in Table 5 should be considered for all tests run, commissioned or otherwise sponsored by USG agencies.

[7] http://www.itl.nist.gov/div893/biometrics/CBEFF_PFA_CTS/

Table 5 - Registry of Biometric Conformance Testing Methodology Standards

#	Validity period	Domain of applicability	Recommended standards	Notes
1.	September 2007 - current	FBI certification of fingerprint systems that scan and capture fingerprints in digital, softcopy form, including hardcopy scanners such as ten-print card scanners, and live scan devices, altogether called "fingerprint scanners"; and systems utilizing a printer to print digital fingerprint images to hardcopy called "fingerprint printers"	FBI EBTS Version 8.1, Appendix F	The procedures for conduct of an Appendix F test can be found at http://www.mitre.org/tech/mtf/
2.	October 2007 – current	Conformance testing of Biometric Service Provider (BSP) implementations claiming conformance to critical requirements specified in INCITS/ISO/IEC 19784-1:2006[2007] (BioAPI 2.0)	INCITS/ISO/IEC 24709-1:2007[2009] and INCITS/ISO/IEC 24709-2:2007[2009]	BSP implementations that are tested according to the methodology specified in INCITS/ISO/IEC 24709-1:2007[2009] and with the test assertions specified in this part of ISO/IEC 24709 can only claim conformance to those aspects of ISO/IEC 19784-1 that are covered by these test assertions.
3.	October 2007 - current	Conformance testing of application(s) or service(s) implementations claiming conformance to the ANSI INCITS 378:2004 standard	INCITS 423.1:2008 and INCITS 423.2:2008	

12. Biometric performance testing methodology standards

The biometric performance testing methodology standards listed in Table 6 should be considered for all tests run, commissioned or otherwise sponsored by USG agencies.

Use of the standards does not restrict testing laboratories from conducting additional activities or using different practices. The standards are therefore suitable for agencies sponsoring tests in experimental or developmental applications.

Table 6 - Registry of Biometric Performance Testing Methodology Standards

#	Validity period	Domain of applicability	Recommended standards	Notes
1.	October 2007 – current	Physical and logical access control tests	INCITS/ISO/IEC 19795-1:2005[2007] and INCITS/ISO/IEC 19795-2:2007[2009]	INCITS/ISO/IEC 19795-2:2007[2009] defines "technology" and "scenario" tests. For access control tests, only the latter is required. The following technical report should be consulted for modality specific guidance: ISO/IEC 19795-3:2007 - Biometric Performance Testing and Reporting – Part 3: Modality-Specific Testing.
2.	October	Testing of performance and	INCITS/ISO/IEC 19795-	The following technical report should be

#	Validity period	Domain of applicability	Recommended standards	Notes
	2007 - current	interoperability of cross-supplier implementations generating and matching instances of standardized biometric data interchange data	1:2005[2007] and INCITS/ISO/IEC 19795-4:2008 [2009]	consulted for modality specific guidance: ISO/IEC TR 19795-3:2007 - Biometric Performance Testing and Reporting – Part 3: Modality-Specific Testing.

13. References

Identification of Standards

The ISO standards identified in this section carry specific nomenclature. The example in the Table below explains the fields. The base standard, as originally developed in the international body, is shown in bold. The details of any subsequent US adoption which enclose this are shown in normal type.

INCITS/**ISO/IEC 19794-6:2005**[2007]					
INCITS	**ISO/IEC**	**19794**	**-6**	**2005**	2007
This is the name of the body in the U.S. that adopts the international standard	**The parent standards development body**	**ISO/IEC 19794 is a multipart data interchange standard**	**The dash six denotes Part 6 which standardizes exchange of iris imagery**	**This is the year that the standard was published. Development was generally completed a few months prior.**	This identifies the year the standard was adopted by the adopter.

For standards that have published amendments, the amendment itself is identified with the following syntax: INCITS/ISO/IEC 19784-1:2006/Amdt. 1 -2007[2008]

1.	ANSI/NIST-ITL 1-2007	Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information – Part 1. Published as NIST Special Publication 500-271, May 2007. http://biometrics.nist.gov/standard/
2.	ANSI/NIST-ITL 1a 2009	Amendment to ANSI/NIST-ITL 1-2007 establishing code for multi-finger impressions. http://fingerprint.nist.gov/standard/ANSI_NIST-ITL_1a-2009.pdf
3.	ANSI/NIST-ITL 2-2008	Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information – Part 2: XML Version, Published as a NIST Special Publication 500-275, August 2008 http://biometrics.nist.gov/standard/
4.	EBTS Version 1.2	DoD Electronic Biometric Transmission Specification (EBTS) Version 1.2 http://www.biometrics.dod.mil/CurrentInitiatives/Standards/dodebts.aspx http://www.biometrics.dod.mil/Files/Documents/Standards/DOD_BTF_TS_EBTS_Nov06_01 02 00.pdf 02 00.pdf
5.	EBTS Version 2.0	DoD Electronic Biometric Transmission Specification (EBTS) Version 2.0 http://www.biometrics.dod.mil/CurrentInitiatives/Standards/dodebts.aspx http://www.biometrics.dod.mil/Files/Documents/Standards/DoD_ABIS_EBTS_v2.0.pdf
6.	EBTS Version 9.1	FBI Electronic Biometric Transmission Specification (EBTS) Version 9.1 http://www.fbibiospecs.org/fbibiometric/biospecs.html
7.	EBTS Version 8.1	FBI Electronic Biometric Transmission Specification (EBTS) Version 8.1 http://www.fbibiospecs.org/fbibiometric/biospecs.html
8.	EFTS Version 7.1	FBI Electronic Fingerprint Transmission Specification (EFTS) Version 7.1 http://www.fbi.gov/hq/cjisd/iafis/efts71/efts71.pdf

9.	FIPS 201-1, 2006	Personal Identity Verification for Federal Employees and Contractors http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf
10.	HSPD-12	Policy for a Common Identification Standard for Federal Employees and Contractors http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm
11.	ICAO 9303	Part 1 - Machine Readable Passport - Volume 2 Specifications for Electronically Enabled Passports with Biometric Identification Capabilities http://mrtd.icao.int/content/view/33/202/ SUPPLEMENT to Doc 9303, Version: Release 8, March 19, 2010 http://www2.icao.int/en/MRTD/Downloads/Supplements to Doc 9303/Supplement to ICAO Doc 9303 - Release 8.pdf
12..	INCITS 358	INCITS 358:2002 [R2007] - American National Standard for Information Technology – The BioAPI Specification http://webstore.ansi.org/
13.	INCITS 378	INCITS 378:2004 - American National Standard for Information Technology — Finger Minutiae Format for Data Interchange http://webstore.ansi.org/
14.	INCITS 381	INCITS 381:2004 - American National Standard for Information Technology — Finger Image-Based Data Interchange Format. http://webstore.ansi.org/
15.	INCITS 398	INCITS 398:2008 - Common Biometric Exchange Formats Framework (CBEFF) http://webstore.ansi.org/
16.	INCITS 423.1	INCITS 423.1:2008 - Conformance testing Methodology Standard for Biometric Data Interchange Format Standards – Part 1: Generalized Conformance Testing Methodology http://webstore.ansi.org/
17.	INCITS 423.2	INCITS 423.2:2008 - Conformance testing Methodology Standard for Biometric Data Interchange Format Standards - Part 2: Conformance Testing, Finger Minutia http://webstore.ansi.org/
18.	INCITS 442	INCITS 442:2008 - Biometric Identity Assurance Services (BIAS) http://webstore.ansi.org/
19.	INT-I	ANSI/NIST-ITL 1-2000 Date Format for the Interchange of Fingerprint, Facial & SMT Information INTERPOL Implementation, Version No. 4.22b - October 28, 2005 http://www.interpol.int/Public/Forensic/fingerprints/RefDoc/implementation6.pdf
20.	INT-Ib	INTERPOL Implementation Version 5 (ANSI/NIST-ITL 1-2000) , The INTERPOL AFIS Expert Group Version 5.0 – Oct 23, 2008 http://www.interpol.int/Public/Forensic/fingerprints/RefDoc/implementation7.pdf
21.	ISO/IEC 15948	ISO/IEC 15948:2004 Computer graphics and image processing – Portable Network Graphics (PNG): Functional specification. http://webstore.ansi.org/
22.	ISO/IEC 19784-1	INCITS/ISO/IEC 19784-1:2006[2007] BioAPI – Biometric Application Programming Interface – Part 1: BioAPI Specification http://webstore.ansi.org/
23.	ISO/IEC 19784-5/Amdt 1	INCITS/ISO/IEC 19784- 1:2006/AM1 -2007 [2008], Information technology - BioAPI - Biometric Application Programming Interface - Part 1: BioAPI Specification - Amendment 1: BioGUI specification
24.	ISO/IEC 19784-2	INCITS/ISO/IEC 19784-2:2007[2008] Biometric Application Programming Interface (BioAPI) – Part 2: Biometric Archive Function Provider Interface http://webstore.ansi.org/
25.	19784-1, Amd. 1	19784-1:2006, Amd. 1:2007 [2008] - Information technology - Biometric application programming interface – Part 1: BioAPI specification – Amendment 1:2007 – BioAPI GUI specification http://webstore.ansi.org/

26.	19784-1, Amd. 2	19784-1:2006, Amd. 2:2009 [2009] - - Information technology - Biometric application programming interface – Part 1: BioAPI specification – Amendment 2: Framework-free BioAPI http://webstore.ansi.org/
27.	19784-1, Amd. 3	19784-1:2006, Amd. 3:2010 - Information technology -Biometric application programming interface – Part 1: BioAPI specification – Amendment 3: Support for interchange of certificates and security assertions, and other security aspects http://webstore.ansi.org/
28.	ISO/IEC 19794-2	INCITS/ISO/IEC 19794-2:2005[2008] — Information technology — Biometric data interchange formats — Part 2: Finger minutiae data. http://webstore.ansi.org/ ISO/IEC 19794-2:2005/Cor.1:2007 — Information technology — Biometric data interchange formats — Part 2: Finger minutiae data – Technical Corrigendum 1
29.	ISO/IEC 19794-4	INCITS/ISO/IEC 19794-4:2005[2007] — Information technology — Biometric data interchange formats — Part 4: Finger image data. http://webstore.ansi.org/
30.	ISO/IEC 19794-5	INCITS/ISO/IEC 19794-5:2005[2007] — Information technology — Biometric data interchange formats — Part 5: Face image data. http://webstore.ansi.org/
31.	ISO/IEC 19794-5/Amdt 1	INCITS/ISO/IEC 19794-5: 2005/Amd 1:2007 [2009] — Information Technology — Biometric Data Interchange Formats — Part 5: Face Image Data - Amendment 1 - Conditions for Taking Photographs for Face Image Data. http://webstore.ansi.org/
32.	ISO/IEC 19794-6	INCITS/ISO/IEC 19794-6:2005[2007] - Information technology — Biometric data interchange formats — Part 6: Iris image data. http://webstore.ansi.org/
33.	ISO/IEC 19795-1	INCITS/ISO/IEC 19795:2005[2007] - Biometric Performance Testing and Reporting – Part 1: Principles and Framework http://webstore.ansi.org/
34.	ISO/IEC 19795-2	INCITS/ISO/IEC 19795-2:2007[2009] - Biometric Performance Testing and Reporting – Part 2: Testing Methodologies for Technology and Scenario evaluations http://webstore.ansi.org/
35.	ISO/IEC 19795-3	ISO/IEC TR 19795:2007 - Biometric Performance Testing and Reporting – Part 3: Modality-Specific Testing http://webstore.ansi.org/
36.	ISO/IEC 19795-4	INCITS/ISO/IEC 19795-4:2008 [2009] - Biometric Performance Testing and Reporting – Part 4: Interoperability Performance Testing http://webstore.ansi.org/
37.	ISO/IEC 24709-1	INCITS/ISO/IEC 24709-1:2007[2009] - Information technology -- Conformance testing for the biometric application programming interface (BioAPI) -- Part 1: Methods and procedures http://webstore.ansi.org/
38.	ISO/IEC 24709-2	INCITS/ISO/IEC 24709-2:2007[2009] - Information technology -- Conformance testing for the biometric application programming interface (BioAPI) -- Part 2: Test assertions for biometric service providers http://webstore.ansi.org/
39.	ISO/IEC 24713-1	ISO/IEC 24713-1:2008 - Biometric Profiles for Interoperability and Data Interchange – Part 1: Overview of Biometric Systems and Biometric Profiles http://webstore.ansi.org/
40.	IXM v2.0	Automated Biometric Identification System (IDENT) Exchange Messages (IXM) Specification – v2.0, September 7, 2007, IDENT-TO007-MAN-IXMTSP-004-D.

		http://www.biometrics.gov/Standards/Default.aspx
41.	IXM v3.1	Automated Biometric Identification System (IDENT) Exchange Messages (IXM) Specification – v3.1, November 26, 2008, IDENT-TO007-MAN-IXMTSP-004-D http://www.biometrics.gov/standards/IXM_Spec_3_1.pdf
42.	IXM 5.5	Automated Biometric Identification System (IDENT) Exchange Messages (IXM) Specification – v5.5 http://www.biometrics.gov/standards
43.	JPEG 2000	ISO/IEC 15444-1:2004 - Information technology - JPEG 2000 image coding system - Part 1: Core coding system http://webstore.ansi.org/
44.	MINEX04	P. Grother et al., *Performance and Interoperability of the INCITS 378 Template,* NISTIR 7296 http://fingerprint.nist.gov/minex04/minex_report.pdf
45.	MITRE1000	Margaret Lepley, *Profile for 1000ppi Fingerprint compression*, Version 1.1 April 2004. Mitre Technical Report 04B0000022. http://www.fbibiospecs.org/fbibiometric/docs/J2K1000.pdf
46.	NIEM	National Information Exchange Model, Production Release 2.1 http://www.niem.gov/niem/index.html
47.	NIST SP 800-76-1	NIST Special Publication 800-76-1, Biometric Data Specification for Personal Identity Verification, Revision 1, January 24, 2007 http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf
48.	RTIC	Registered Traveler Interoperability Consortium (RTIC), Technical Interoperability Specification, Version 1.7, April 15, 2008. http://www.rtconsortium.org/_docpost/RTICTIGSpec_v1.7.pdf
49.	TWIC	TWIC Reader Hardware and Card Application Specification, September 11, 2007. http://www.tsa.gov/assets/pdf/twic_reader_card_app_spec_091107.pdf
50.	TWPDES	Terrorist Watchlist Person Data Exchange Standard, Version 3.0. http://www.niem.gov/TWPDES.php
51.	WSQv31	WSQ Gray-Scale Fingerprint Image Compression Specification, IAFIS-IC-0110(V3), October 4, 2010. https://www.fbibiospecs.org/docs/WSQ_Gray-scale_Specification_Version_3_1.pdf