Registry of USG Recommended Biometric Standards

Version 5.0

September, 2014

White House National Science and Technology Council

Contents

1. Introduction

On behalf of the White House Office of Science and Technology Policy this *Registry of USG*[1] *Recommended Biometric Standards* was developed through a collaborative, interagency process and approved by the NSTC. 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 Biometric Standards and Conformity Assessment Working Group (BSCA WG) is tasked to develop and update the Registry as necessary. The BSCA WG reviews the content of this document, and releases updated versions as required to assist agencies in implementing and enforcing the use of biometric standards to promote interoperability and meet agency-specific mission needs. The approved version of this document is available on the NSTC web site www.biometrics.gov

The maintenance of this Registry is supported by USG agencies providing appropriate personnel and resources to participate in the BSCA WG activities. Federal agencies identifying issues with this Registry should notify their USG representatives to the BSCA WG Group.

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.

2. Scope

This Registry lists recommended biometric standards for USG-wide use. Only standards published and approved by a standards setting or developing organization are eligible for recognition and registration in this document by the BSCA WG. Inclusion of a standard in this Registry represents consensus agreement of USG agencies through the deliberative process. For dated references to standards, only the edition cited applies. For undated references to standards, the latest edition of the referenced standard applies.

These recommendations take into account:

- the differences in how criminal identification and civil biometric authentication systems operate;
- the need to accommodate legacy and current implementations as well as new implementations;
- the movement to international versions from national standards; and,
- the use of biometric characteristics for forensic applications.

All amendments, supplements and corrigenda are included as part of the recommended biometric standard.

[1] USG stands for **U**nited **S**tates **G**overnment.

Along with the 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 agency-specific reference documentation.

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 or additional categories are approved by the standards developing organizations and adopted for USG-wide use.

These biometric standards in this Registry govern the use of biometric characteristics for both automated (biometric) applications, as well as partially or non-automated (forensic) applications.

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.

- **application profile** is conforming subsets or combinations of one or more base standards and/ or profiles necessary to accomplish particular functions specific to the application and its domain of use.

- **transmission profile -** a profile developed to define sender and receiver requirements for electronic communications between systems.
- **credentialing profile -** a profile developed to support the requirements of a specific USG personal identity verification system and the sender and receiver specification for electronic communication between systems.
- *(alternative)* **credentialing profile -** a profile developed to define specific requirements for vetting an entity using biometrically enabled personal identity verification systems.

- **base standard -** a generic standard containing options that may be profiled for application-specific purposes [Source: ISO/IEC 24713-1:2008]. Base standards can be used in diverse applications. For a specific application, it may be useful to construct a profile that specifies or restricts values and practices from the options in a base standard. The aim of such a profile is to achieve interoperability for a specific application.
- **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 [Source: INCITS/ISO/IEC 19795-4:2008 [2009]]
- **best practice recommendations –** documents that describe processes and procedures that, if followed, will assist in ensuring the integrity and usefulness of biometric data
- **biometric data interchange record (BDIR) -** data package containing biometric data that claims to be in the form prescribed by a base standard

  If the BDIR is encapsulated in a Common Biometric Exchange Formats Framework (CBEFF) record, then the BDIR is also a biometric data block (BDB) as defined in ISO/IEC 19785, but this will not always be the case for BDIRs defined in ISO/IEC 19794.

- **certification -** third-party attestation related to products, processes, systems or persons [Source: ISO/IEC 17000:2004]

  * Certification of a management system is sometimes also called registration.

  * Certification is applicable to all objects of conformity assessment except for conformity assessment bodies themselves, to which accreditation is applicable.
- **conformance testing -** testing determination of one or more characteristics of an object of conformity assessment, according to a procedure
- **class resolution -** The value of resolution (scanning or nominal) used to name (or identify) an acquisition process or image, where the resolution is within a specified tolerance around that value. [Source: ANSI/NIST-ITL 1-2011]
- **exemplar –** In earlier versions of this Registry, this term meant the friction ridge prints of an individual, associated with a known or claimed identity, and deliberately recorded directly from an individual -- whether electronically, by ink, or by another medium (also called 'known prints'). This term has now been expanded in this document to include other images taken directly from an individual (such as lip prints).

- **friction ridge image -** An image of an impression from the palmar surfaces of the hands or fingers, or from the plantar (sole) surfaces of the feet or toes.
- **image -** two or three dimensional spatial data

  EXAMPLE 1 A two dimensional fingerprint image

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

  EXAMPLE 3 Video of a moving face – not necessarily regularly spaced in time.
- **latent print -** In earlier versions of this Registry, this term meant an impression or image of friction ridge skin left on a surface. It has now been expanded to include other impressions or images left by other body parts, such as lips prints on a surface or entire footprints in mud or impressions of teeth in a substance such as chewing gum. In other words, the biometric print is retrieved from an object or other person and not directly from the subject.
- **operational evaluation -** process used to evaluate a biometric system in the targeted operational environment and population

  NOTE By its nature, it is not a repeatable process. Population, actual environmental conditions, and other factors will vary during operational evaluations.
- **performance testing -** measures the performance characteristics of an implementation such as system error rates, throughput, or responsiveness, sometimes under various conditions
- **profile -** conforming subsets or combinations of base standards used to effect specific functions [Source: ISO/IEC 24713-1:2008] Profiles define specific values or conditions from the range of options described in the relevant base standard(s), with the aim of supporting the interchange of data between applications and the interoperability of systems. [Source: ISO/IEC 24713-1:2008]
- **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 template -** supplier-defined representation of a biometric sample, suitable for matching, usually in an unpublished format
- **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
- **sample quality -** measurable properties of a biometric sample associated with its fidelity to its source, and related to the utility, and its expected performance in a verification or identification system or by a forensic examiner
- **scenario evaluation -** 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. [Source: ISO/IEC 19795-2:2005]

NOTE 1 Scenario evaluations are intended for measurement of performance in modeled environments, inclusive of test subject-system interactions. Scenario evaluation assesses biometric technologies in a manner representative of the operational application while maintaining control of performance variables.

NOTE 2 The word "online" in the definition refers to human subject involvement.

NOTE 3 The term "real time" indicates that the human-system interaction is on the timescale of the operational scenario

- **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

  EXAMPLE 3 An electropherogram used in many kinds of DNA typing

- **simple object access protocol -** A formal set of conventions governing the format and processing of XML for implementation of web services.

- **standard –** a 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. [Source: ISO/IEC Guide 2:2004]

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

  Such organizations may be:

  - accredited, such as American National Standards Institute (ANSI) accredited InterNational Committee for Information Technology Standards (INCITS) and ANSI accredited National Institute of Standards and Technology – Information Technology Laboratory (NIST-ITL);
  - international treaty based, such as the International Civil Aviation Organization (ICAO), which is a specialized agency of the United Nations;
  - international private sector based, such as International Organization for Standardization / International Electrotechnical Commission (ISO/IEC);
  - a consortium, such as Organization for the Advancement of Structured Information Standards (OASIS); or,
  - a government agency, such as the Department of Defense, the Department of Homeland Security, the Federal Bureau of Investigation and the National Institute of Standards and Technology.

- **standards setting organization -** any entity whose primary activities are developing, coordinating, promulgating, revising, amending, reissuing, interpreting, or otherwise maintaining standards that address the interests of a wide base of users outside the standards development organization.

- **technology evaluation -** the offline evaluation of one or more algorithms for the same biometric modality using a pre-existing or specially-collected corpus of samples

  NOTE The concept can be generalized to other biometric components, the key being that the evaluation is deterministic and repeatable. For example, the Appendix F imaging certification tests applied to fingerprint sensors.

- **template -** encoded representation of features extracted from a sample suitable for direct comparison
- **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 [Source: ISO/IEC Guide 2:2004]
- **testing -** action of carrying out one or more tests [Source: ISO/IEC Guide 2:2004]

5. Acronyms and abbreviations

ABIS	Automated Biometric Identification System
ADA	American Dental Association
ANSI	American National Standards Institute
BIAS	Biometric Identity Assurance Services
BioAPI	Biometric Application Programming Interface
BIR	Biometric Information Record
BSP	Biometric Service Provider
CBEFF	Common Biometric Exchange Formats Framework
DFBA	Defense Forensics and Biometrics Agency
DHS	Department of Homeland Security
DICOM	Digital Imaging and Communications in Medicine
DoD	Department of Defense
EBTS	Electronic Biometric Transmission Specification
EFTS	Electronic Fingerprint Transmission Specification
FBI	Federal Bureau of Investigation
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
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
MINEX	Minutiae Interoperability Exchange Test
MRTD	Machine Readable Travel Document

NEMA	National Electrical Manufacturers Association
NG-ABIS	Next Generation - Automated Biometric Identification System
NGI	Next Generation Identification
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
NSTC	National Science and Technology Council
OASIS	Organization for the Advancement of Structured Information Standards
OBIM	Office of Biometrics and Identity Management
PIV	Personal Identity Verification
RT	Registered Traveler
RTIC	Registered Traveler Interoperability Consortium
SAP	Subject Acquisition Profile
SMT	Scars, Marks, and Tattoos
SOAP	Simple Object Access Protocol
TWIC	Transportation Worker Identification Credential
TWPDES	Terrorist Watchlist Person Data Exchange Standard
USG	United States Government
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 may be needed because standardized legacy data may 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.

Intended Applicability: The functions of generic biometric applications include: an enrollment phase, and a subsequent identification or verification phase. The enrollment phase embeds capture of an initial sample and is usually an attended operation. The capture may be from a cooperative, non-cooperative or uncooperative subject. 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).

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. For data interchange, the intent is that all biometric samples captured, or otherwise instantiated during the validity period, shall be encoded in conformance with the identified standards. For non-data applications, such as performance testing, the intent is that the normative[4] requirements of the standards are followed. 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.

Nomenclature for the ANSI/NIST-ITL Standard: The ANSI/NIST-ITL standard identified in the following sections carries specific nomenclature. Table 1 below explains the fields.

ANSI/NIST-ITL X-YYYY Type ZZ					
ANSI	NIST	ITL	X	YYYY	ZZ
The standard is developed under ANSI approved procedures	The parent standards developing organization	The laboratory at NIST responsible for the standard development	The sequence number for the standard within the calendar year	The year that the standard was published. Development was generally completed a few months prior.	An integer (1-21, 98, 99) indicating specific Type Records of the standard.

Table 1 - ANSI/NIST-ITL Standard Nomenclature

When references in this Registry are to ANSI/NIST-ITL 1-2011, they are also valid for later updates to that version, such as ANSI/NIST_ITL 1-2011 Update: 2013. When a specific Update is mentioned, that is because the specific capability referred to did not exist prior to that Update (such as forensic dental data)

Nomenclature for the INCITS/ISO/IEC Standards: The ISO/IEC standards adopted by INCITS are INCITS/ISO/IEC standards. Such standards identified in the following sections use the nomenclature illustrated in Table 2. 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

[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] Standards often contain required content, expressed as *normative* requirements, and recommended content, expressed in *informative* text.

The name of the body in the U.S. that adopts the international standard	The parent standards developing organization	The ISO/IEC 19794 is a multipart data interchange standard	The dash six denotes Part 6 which in this case standardizes exchange of iris images	The year that the standard was originally published. Development was generally completed a few months prior.	The year the standard was adopted by the US National Body (INCITS).	The year the standard was reaffirmed[5].

Table 2 - INCITS/ISO/IEC Standard Nomenclature

For standards that have published amendments they are identified with the following type of syntax: INCITS/ISO/IEC 19784-1:2006/Amd. 1 -2007

7. Biometric data collection, storage, and exchange standards

The biometric standards recommended in Tables 3-8 should be used in all USG applications for which biometric data:

- are exchanged between systems within an agency,
- are exchanged between agencies,
- persist beyond the interaction of a subject with a sensor or system.

The biometric standards listed below primarily cover:

- friction ridge imagery (latent and exemplar images of: fingerprints, palms, and/or plantars);
- friction ridge features;
- face[6] images;
- iris images;
- DNA;
- scars, marks, tattoos;
- body part images;
- forensic mark-ups of samples;
- voice recognition;
- cheiloscopy (lip prints);
- patterned injury imagery;
- forensic dental and other identifying medical and physical characteristics; and
- associated metadata for all of the above.

Standards for other biometric modalities have been approved by the various standards setting or developing organizations; however they are not listed here because the imperative for development of this Registry is ongoing or anticipated multi-agency or USG-wide applications. For parties seeking to collect, store and exchange data from biometric modalities not covered by this Registry, they have the option of using standards approved by national or international standards setting or developing

[5] Re-affirmation of a standard reflects the decision of the responsible standards developing organization 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.

[6] This document refers to "face recognition" and "face images". Other documents have used the modifier "facial" without any difference in meaning.

organizations. It should be noted that the ANSI/NIST-ITL standard explicitly allows the transmission of data conforming to those standards within a Type-99 record.

It is assumed that parent applications can properly embed or wrap biometric data formatted according to the standards enumerated below, such as the DoD or FBI's Electronic Biometric Transmission Specification (EBTS) transactions embedding ANSI/NIST-ITL 1-2011 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 Tables 3-15 address collection, storage and exchange of biometric data, existing transmission profiles such as the DoD or FBI's EBTS (see Table 17) might further modify or restrict the recommended standards of Tables 3-15. The shaded cells in all tables indicate the standard is no longer recommended for use, but may still be implemented in current or legacy systems.

It is important to note that several transmission standards rely upon other standards, such as for image compression. Any such cross-reference within standards that are listed in this registry is therefore incorporated by this Registry without being explicitly listed.

A rather unique standard affecting biometrics is the National Information Exchange Model (NIEM) Biometrics Domain. NIEM specifies principles and enforceable rules for XML data components, including naming and design rules. XML schemas and components that obey the rules are considered to be NIEM-conformant. ANSI/NIST-ITL XML schemas are developed in accordance with NIEM principles. In 2012, the Biometrics Domain of NIEM was formally established. The NIEM Biometrics domain defines the XML representation for biometrics for the USG.

Intended applicability	Biometric data	Validity period	Recommend standard(s)
The XML encoding of transmissions based upon standards in this registry.	All modalities	December, 2013 - Present	NIEM Version 2.1 (Valid for ANSI/NIST-ITL 1-2011 Update: 2013)
		November 2011 – December 2013	NIEM Version 2.1 (Valid for ANSI/NIST-ITL 1-2011)
		2007 - 2009	NIEM Version 2.0 (Used for ANSI/NIST-ITL 2-2008)

Table 3 – XML biometric encoding standards

7.1 Friction ridge imagery

Intended applicability	Biometric data	Validity period	Recommend standard(s)
The electronic exchange of images to be used in the identification or verification process of a subject among criminal justice administrations or organizations that rely on automated identification systems or use other biometric and image data for identification purposes.	Fingerprint, Palm, Plantar Image Data	December 2013 – Present	ANSI/NIST_ITL 1-2011 Update: 2013. Type 13, Type 14, Type 15, Type 19
		November 2011 – December 2013	ANSI/NIST-ITL 1-2011, Type 13, Type 14, Type 15, Type 19
		October 2007 – November 2011	ANSI/NIST-ITL 1-2007 (Traditional Encoding), Type 4, Type 13, Type 14, Type 15
		December 2008 –November 2011	ANSI/NIST-ITL 2-2008 (XML Encoding), Type 4, Type 13, Type 14, Type 15
The interchange among organizations that rely on automated devices and systems for identification or verification purposes based on the information from finger and palm image areas	Finger and Palm Image Data	December 2011 – Present	ISO/IEC 19794-4:2011
The interchange among organizations that rely on automated devices and systems for identification or verification purposes based on the information from finger image areas	Finger Image Data	October 2007 – December 2011	INCITS/ISO/IEC 19794-4:2005[2007]
		October 2007 – July 2012	INCITS 381-2004
		October 2009 – July 2012	INCITS 381-2009

Table 4 - Registry of Friction Ridge Imagery Standards

ANSI/NIST-ITL 1-2011: Update 2013 includes both the Traditional and NIEM-conformant XML encodings. There are no longer separate versions of the standard for each encoding as in ANSI/NIST-ITL 1-2007 and ANSI/NIST-ITL 2-2008.

ANSI/NIST-ITL 1-2011 deprecates the Type-3, -5, and -6 records, but retains the Type-4 record to ensure backward compatibility; *however, new users are encouraged to utilize the Type-14 record to convey fingerprint images*. While the Type-4 record remains the predominant format for transmission of rolled fingerprint information, the Type 14 record is highly 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.

Users should coordinate with receiving agencies to ensure they have the capability to accept Type-14 variable-resolution fingerprint image data.

The variable-resolution image data contained in the Type-13, Type-14, Type-15, and Type 19 records may be in a compressed form. 19.69 ppmm (500 ppi) images may be exchanged (however, images with lower ppi are not acceptable). It is strongly recommended that the resolution for fingerprint, palm and plantar images be 39.37 ppmm (1000 ppi). If images scanned at 1000 ppi are to be transmitted at 500 ppi, then the guidance in NIST Special Publication 500-289 shall be followed for downsampling prior to compression using WSQ at 500 ppi. There are currently no published standards for compression of 2000 ppi (or greater) images.

When friction ridge images are captured at 19.69 ppmm (500 ppi) and compressed with WSQ, the compression ratio shall not exceed 15:1. An optimal compression rate of is 10:1 for card scan imagery, 15:1 for live scan imagery, and 12:1 for exemplars meant to be compared to latent imagery. Based on the automated matcher behavior data however, the compression rate of 10:1 shall be applied to all exemplar impressions to mitigate any potential performance degradation resulting from mixed compression cases (i.e., 10:1 to 15:1) . Exemplar images stored at 1000 ppi shal use lossy 10:1 compression with JPEG2000 using parameters specified in NIST Special Publication 500-289.

Latent friction ridge images should be acquired with a native resolution of 39.37 ppmm (1000 ppi). Latent images shall be stored according to NIST Special Publication 500-289 (lossless compression imagery using the JPEG2000 reversible filter). If reduced resolution images are prepared (e.g., for transmission), then the parent high resolution image shall be retained.

PIV was designed to require the use of INCITS 381-2004 for the retention of fingerprint images. However, the INCITS standard for finger image (INCITS 381-2004) has been withdrawn and is no longer being maintained by the INCITS. When PIV was updated in 2013 (FIPS 201-2, 2013), the reference to INCITS 381-2004 was maintained to ensure backward compatibility with the millions of PIV cards that have already been issued, which is why it does not use ISO/IEC 19794-5 as a basis for the finger image specifications.

7.2Friction ridge features

Intended applicability	Biometric data	Validity period	Recommend standard(s)
The electronic exchange of friction ridge feature sets to be used in the identification or verification process of a subject among criminal justice administrations or organizations that rely on automated identification systems.	Friction ridge minutiae data and other features (Until 2008, fingerprint and palm print features only. Plantar print features were added in 2011)	December 2013 – Present	ANSI/NIST-ITL 1-2011 Update: 2013 It adds a new optional field to Type-9 for temporary markup lines and corrects some data values from the 2011 version.
		December	ANSI/NIST-ITL 1-2011 Type

Intended applicability	Biometric data	Validity period	Recommend standard(s)
		2011– December 2013	9
		October 2007 – November 2011	INCITS 378-2004 – or – 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 126-150
		December 2008 – November 2011	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
Used in a wide range of application areas to include cards where automated fingerprint recognition is involved	Fingerprint minutiae (only)	November 2011 – Present	ISO/IEC 19794-2:2011
		October 2007 – November 2011	INCITS/ISO/IEC 19794-2:2005[2008], clause 8 compact card format with clause 9 format types 0001, 0003, 0005

Table 5 - Registry of Friction Ridge Feature Standards

The primary use of the ANSI/NIST-ITL 1-2011 Update: 2013, Type 9 (Minutiae data) record is for remote searching of latent prints in criminal justice organizations.

The 2004 version of INCITS 378 had one item for the product identifier. This was clarified and broken into two items in the 2009 version of INCITS 378; the product identifier and the format type. See ANSI/NIST-ITL 1-2011 Update: 2013 for additional guidance. If ANSI/NIST-ITL 1-2011 Update: 2013 Type 9 is used, vendor blocks (i.e. fields 31 - 125 and 151-175) should not be used.

Identification / verification applications may use either the ISO/IEC 19794-2:2011 standard or the ANSI/NIST-ITL standard. This may include proprietary template data in "vendor-defined extended data" fields. Proprietary template data is non-interoperable but some implementations have shown 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

promotes vendor lock-in. To mitigate this risk, the parent images shall be retained. To eliminate this risk, standardized image records should be exchanged. In order to avoid abuse of this allowance of proprietary data, the standardized minutiae data should be required.

In on-card comparison applications it is recommended to use the core three-byte-per-minutia format defined in ISO/IEC 19794-2:2011; moreover, instances of this format shall be produced from parent instances of the ISO/IEC 19794-2:2011 template. See Biometric Specifications for Personal Identity Verification [NIST SP-800-76-2] for additional guidance.

Although PIV (FIPS 201-1, 2006 and FIPS 201-2, 2013) requires the use of INCITS 378-2004 for the retention of fingerprint minutia; the INCITS national standard for finger minutia has been withdrawn and is no longer being maintained by INCITS. As an existing application, this use of an older standard is allowed, but new applications shall not be based upon obsolete standards. Guidance on minutia detection and estimation appears in ISO/IEC 19794-2:2011.

7.3 Face images

There are several types of face images used in biometric and forensic applications, as described below.

7.3.1 2D imagery in visible light

Intended applicability	Biometric data	Validity period	Recommend standard(s)
The electronic exchange of face image data to be used in the identification or verification process of a subject among criminal justice administrations or organizations that rely on automated identification systems. Another important application is forensic investigation of unknown deceased.	2D face images	December 2013 – Present	ANSI/NIST-ITL 1-2011 Update: 2013 This adds new optional fields for Image subject condition, Capture organization name and Image capture date range estimate.
		November 2011 – December 2013	ANSI/NIST-ITL 1-2011, Type 10
Capture and storage (i.e., enrollment or registration processes) for which end-to-end subject capture times above 120 seconds are tolerable	2D Face images	October 2007 – November 2011	ANSI/NIST-ITL 1-2007, Type 10 with subject acquisition profile (SAP) of level 10 or above – or – INCITS/ISO/IEC 19794-5:2005[2007], Full Frontal or Token, with at least 90

Intended applicability	Biometric data	Validity period	Recommend standard(s)
			pixels between the eyes from all subjects
		December 2008 – November 2011	ANSI/NIST-ITL 2-2008, Type 10 with subject acquisition profile (SAP) of level 10 or above
Non-cooperative or uncooperative capture and storage of images	2D face images	October 2007 – November 2011	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 type only
		December 2008 – November 2011	ANSI/NIST-ITL 2-2008, Type 10 with subject acquisition profile (SAP) of level 1 or above
All other capture, storage or exchange applications	2D face images	October 2007 – November 2011	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
		December 2008 – November 2011	ANSI/NIST-ITL 2-2008, Type 10 with subject acquisition profile (SAP) of level 1 or above
Used in a wide range of application areas to include cards where automated face recognition is involved	2D face images	December 2005 - Present	INCITS/ISO/IEC 19794-5:2005[2007]
	2D face images	October 2007 – July 2012	INCITS 385-2004
		October 2009 – July 2012	INCITS 385-2009
Capture and storage in Machine Readable Travel Documents	2D face images	October 2007 – Present	ICAO 9303 and Supplement

Table 6a - Registry of 2D Face Imagery Standards

2D face images are the most widely used facial biometric. Facial imagery may be used for both automated and manual comparisons. Automated systems work best with several factors controlled, such as: lighting, pose of the subject, background, angle of the face, and without coverage of portions of the face by hair, glasses or scarves. It is also very important that there be sufficient resolution and that there be no photographic enhancement of the original image. Best Practice guidelines for the acquisition of facial images are available in:

- "ANNEX E: Facial Capture - SAPs 30 and above" of ANSI/NIST-ITL 1-2011 Update: 2013
- "ICAO MRTD Photo Guidelines"
- "Annex A: Best Practices for Face Images" of INCITS/ISO/IEC 19794-5:2005[2007]

ISO/IEC 19794-5:2005[2007] standard is currently adopted by the International Civil Aviation Organization for e-Passports. Best practices are strongly recommended for the application in the e-passport framework. This ensures that, issuing authorities and/or photographers do not have to change their already-published photo requirements that are based on the existing best practice requirements. The 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; when those images are required to conform to the frontal image types of this standard (INCITS/ISO/IEC 19794-5:2005[2007]).

The addition of new fields in ANSI/NIST-ITL Update: 2013 was intended to assist in the forensic identification of unknown deceased using photographic imagery. It is important to annotate whether the images are ante-mortem or post-mortem (**Image subject condition**). For ante-mortem photographs provided by families and other persons, the exact date of the photo may not be known, thus the introduction of the new field **Image capture date range estimate**.

As an existing application, PIV (FIPS 201-1, 2006 and FIPS 201-2, 2013) continues to use facial images formatted such that they conform to INCITS 385-2004. That standard has been withdrawn and is no longer supported by INCITS. As an existing application, this use of an older standard is allowed, but new applications shall not be based upon obsolete standards.

7.3.2 Forensic markups

Intended applicability	Biometric data	Validity period	Recommend standard(s)
Manual or automated markup of photographic imagery.	2D face images	December 2013 – Present	ANSI/NIST-ITL 1-2011: Update 2013, Type 10 INCITS/ISO/IEC 19794-5:2005[2007]

Intended applicability	Biometric data	Validity period	Recommend standard(s)
		November 2011 – December 2013 October, 2007 - Present	ANSI/NIST-ITL 1-2011, Type 10 INCITS/ISO/IEC 19794-5:2005[2007]

Table 6b - Registry of Forensic Markup Face Imagery Standards

Similar to the forensic markup of friction ridge images using the Extended Feature Set in Type-9 of ANSI/NIST-ITL 1-2011 Update: 2013, forensic analysts may desire to record detailed analytical information about the face image. Both ANSI/NIST-ITL and INCITS/ISO/IEC 19794-5 use feature points based upon the MPEG4 standard for 2D markups. Additional feature points are available for 3D markups of 2D images (such as to indicate the depth of the nose, etc.). The feature points are the same in both standards.

7.3.3 2D imagery using light outside the visible range

Intended applicability	Biometric data	Validity period	Recommend standard(s)
The electronic exchange of face image data to be used in the identification or verification process of a subject	2D face images	December 2013 – Present	ANSI/NIST-ITL 1-2011 Update: 2013, Type 22

Table 6c - Registry of 2D Face Imagery light outside visible range Standards

ANSI/NIST-ITL 1-2011 Update: 2013 added the capability to transmit imagery that is not traditional 2D visible light photography. Included in this capability are capture systems compatible with infrared, ultraviolet and other wavelengths (such as X-ray).

7.3.4 3D imagery

Intended applicability	Biometric data	Validity period	Recommend standard(s)
The electronic exchange of face image data to be used in the identification or verification process of a subject	Specialized 3D imagery and 3D printing or cast models	December 2013 - Present	ANSI/NIST-ITL 1-2011 Update: 2013, Type 22
	3D face images	October 2007 – Present	INCITS/ISO/IEC 19794-5:2005[2007] ANSI/NIST-ITL 1-2011, Type-

Intended applicability	Biometric data	Validity period	Recommend standard(s)
			99

Table 6d - Registry of 3D Face Imagery Standards

3D imagery is captured and stored in a manner very different from conventional 2D photography. 3D cast models and specialized medical imagery may be conveyed in the ANSI/NIST-ITL Type-22 record.

7.4 Scars, Marks and Tattoo

Intended applicability	Biometric data	Validity period	Recommend standard(s)
The electronic exchange of image data from the scars, (needle) marks, and tattoos (SMT) to be used in the identification or verification process of a subject among criminal justice administrations or organizations that rely on automated identification systems.	Scar, (needle) mark, and tattoo information	December 2013 - Present	ANSI/NIST-ITL 1-2011 Update: 2013, Type 10
		November 2011 – December, 2013	ANSI/NIST-ITL 1-2011, Type 10

Table 7 - Registry of SMT Standards

Marks, as used in this standard, means needle marks typical of drug use. In some nations the term 'marks' denotes what is called 'latent prints' within the terminology of this standard.

An SMT image consisting of several parts or sub-images shall use subfields to fully describe the various parts or features found in the total image. The first subfield shall describe the most predominant feature or sub-image contained in the SMT image. Subsequent repeating subfields shall describe additional portions of the image that are not part of the main or central focal point of the image. For example, a tattoo consisting of a man with a snake on the arm being followed by a dog may contain three subfields: one describes the man, a second describing the snake, and a third describing the dog.

7.5 Iris images

Intended applicability	Biometric data	Validity period	Recommend standard(s)
The electronic exchange of iris image data to be used in the identification or verification process of a subject among criminal justice administrations or	Iris images	December 2013 - Present	ANSI/NIST-ITL 1-2011 Update: 2013, Type 17
		November 2011 - December 2013	ANSI/NIST-ITL 1-2011, Type 17

Intended applicability	Biometric data	Validity period	Recommend standard(s)
organizations that rely on automated identification systems.		October 2007 – November 2011	The rectilinear image format of INCITS/ISO/IEC 19794-6:2005[2007] – or – ANSI/NIST-ITL 1-2007, Type 17
		December 2008 – November 2011	ANSI/NIST-ITL 2-2008, Type 17
Used in a wide range of application areas to include cards where automated iris recognition is involved.		November 2011 - Present	ISO/IEC 19794-6:2011
Used in a wide range of application areas to include cards where automated iris recognition is involved.		October 2007 – July 2012	INCITS 379-2004

Table 8 - Registry of Iris Image Standards

The ANSI/NIST-ITL 1-2011 Update: 2013, Type-17 record was developed to provide a basic level of interoperability and harmonization with the INCITS 379-2004 Iris image interchange format and the ISO/IEC 19794-6:2011 Iris image data interchange format. It also contains optional descriptive data fields and image markup fields. Generic iris images may be exchanged using the mandatory fields of this record type. Images may be monochrome or color with 256 or more intensity levels (gray or per-color component), and vary in size depending on field of view and compression. The recommended formats all store sampled pixel data from rectilinear images. The data shall be encoded as a raw array of intensity values, a raw array of red green blue color values, or as losslessly compressed or lossy-compressed versions thereof. Like face image data, this record type has descriptive characteristics for various subject acquisition profiles which are defined in detail in the ANSI/NIST-ITL 1-2011.

For storage of iris data on-card, off-card, iris capture devices, and the components involved in automated recognition of iris imagery shall conform to the data format specified in 19794-6:2011. In iris recognition, templates are proprietary non-standardized mathematical encodings of information extracted from the formally standardized images that are defined in ISO/IEC 19795-6:2011. The templates are not interoperable therefore organizations retaining only templates are subject to a supplier lock-in hazard.

7.6 DNA

Intended applicability	Biometric data	Validity period	Recommend standard(s)
The electronic exchange of DNA	DNA	December 2013 -	ANSI/NIST-ITL 1-2011

Intended applicability	Biometric data	Validity period	Recommend standard(s)
data to be used in the identification or DNA verification process of a subject among criminal justice administrations or organizations that rely on automated identification systems.		Present	Update: 2013, Type 18
		November 2011 – December, 2013	ANSI/NIST-ITL 1-2011, Type 18
The exchange of DNA data for person for only biometric identification or verification technologies that utilize human DNA.		December 2012 - Present	ISO/IEC 19794-14:2012

Table 9 - Registry of DNA Standards

To provide full consideration to privacy, the ANSI/NIST-ITL 1-2011 Update: 2013, Type 18 record only uses the non-coding regions of DNA; the regions of the DNA that encode phenotypic information are deliberately avoided. This record type provides a basic level of interoperability with the ISO/IEC 19794-14:2012. The recommended DNA standards should not be used for the exchange of medical and other health related information

7.7 Patterned injuries

Intended applicability	Biometric data	Validity period	Recommend standard(s)
The electronic exchange of imagery of patterned injuries on human bodies.	Patterned Injuries	December 2013 - Present	ANSI/NIST-ITL 1-2011 Update: 2013, Type-10 and ANSI/ADA 1077

Table 10 - Registry of Patterned Injury Standards

Patterned injuries are those injuries on a body that exhibit characteristics typical of being caused by an external object, such as teeth or a whip. The analysis of such injuries can be an integral part of criminal investigations and determination of the cause of death. ANSI/NIST-ITL 1-2011 Update: 2013 includes the capability to include images of the patterned injury and to include descriptors based upon the common taxonomy established in ANSI/ADA 1077 *Dental Biometric Descriptors.* In all imagery of patterned injuries, it is extremely important to follow the guidance of the *Diplomates Reference Manual* published by the American Board of Forensic Odontology.

7.8 Forensic dental (odontology)

Intended applicability	Biometric data	Validity period	Recommend standard(s)

Intended applicability	Biometric data	Validity period	Recommend standard(s)
The electronic exchange of descriptive data, imagery, 3D cast mold data, and other information that may assist in the forensic identification of deceased individuals and living persons unable to identify themselves (such as accident victims in comas) based upon dental and oral characteristics.	Patterned Injuries	December 2013 - Present	ANSI/NIST-ITL 1-2011 Update: 2013, Type-10 (for photographic intraoral and extraoral images) ANSI/NIST-ITL 1-2011 Update: 2013, Type-12 for forensic dental data and mouth condition descriptors, in conjunction with ANSI/ADA 1058 ANSI/NIST-ITL 1-2011 Update: 2013, Type-22 for non-photographic imagery NEMA/DICOM for electronic dental records from dentist offices

Table 11 - Registry of Forensic Dental Standards

The 2013 Update to ANSI/NIST-ITL includes new capabilities to transmit data associated with the identification of individuals based upon forensic dentistry (odontology). Visual images of the mouth (extraoral and intraoral) may be included in the Type-10 record. Non-photographic imagery (including images outside of the normal visible light range) such as radiographs and cone beam imagery and 3D cast models are conveyed in a Type-22 record. The Type-22 record also allows the encapsulation of DICOM imagery and data (which is a format commonly used in dental offices). Note that data stored according to the specification of NEMA/DICOM *Digital Imaging and Communications in Medicine* can also be transmitted directly, without the use of ANSI/NIST-ITL standard.

An important part of the transmission of forensic dental data is the Type-12 record of ANSI/NIST-ITL Update: 2013. It encodes the descriptors based upon the taxonomy of ANSI/ADA 1058 *Forensic Dental Data Set* and ANSI/ADA 1067 *Standard Functional Requirements for an Electronic Dental Record System.*

7.9Cheiloscopy (lip prints)

Intended applicability	Biometric data	Validity period	Recommend standard(s)

Intended applicability	Biometric data	Validity period	Recommend standard(s)
The electronic exchange of imagery of lip prints and forensic markups of those prints.	Patterned Injuries	December 2013 - Present	ANSI/NIST-ITL 1-2011 Update: 2013, Type-10

Table 12 - Registry of Cheiloscopy Standards

The analysis of cheiloscopic imagery (lip prints) may assist in criminal investigations. Lip prints may be left upon inanimate surfaces (such as a glass) or on a person (lipstick and lip balm). A new field was added to the Type-10 record in the 2013 Update to accommodate the characterization of lip prints.

7.10 Other body part imagery

Intended applicability	Biometric data	Validity period	Recommend standard(s)
The electronic exchange of imagery of non-facial body parts.	2D imagery	December 2013 - Present	ANSI/NIST-ITL 1-2011, Type-10 ANSI/NIST-ITL 1-2011 Update: 2013, Type-22

Table 13 - Registry of Other Body Part Imagery Standards

Visible light imagery of body parts is transmitted in Type-10 ANSI/NIST-ITL records. Other imagery (such as x-rays) is transmitted using a Type-22 record. This is particularly useful in forensic applications when body parts may be separated (such as after a disaster) or when a body part has a particular characteristic that may be useful in identification of unknown deceased (such as a club foot).

7.11 Forensic and investigatory voice

Intended applicability	Biometric data	Validity period	Recommend standard(s)
The electronic exchange of voice recordings and associated analytical information.	Voice recordings	December 2013 - Present	ANSI/NIST-ITL 1-2011 Update: 2013, Type-11

Table 14 - Registry of Forensic and Investigatory Voice Standards

A recording may be transmitted using the ANSI/NIST-ITL Update: 2013 Type-11 record along with descriptors (such as the timings of individual speakers' voices being audible) and other metadata such as transcripts, translations, and results of automated matching against pre-stored voice data.

7.12 Video

Intended applicability	Biometric data	Validity period	Recommend standard(s)
The electronic exchange of video recordings and associated analytical information.	Video clips	December 2013 - Present	ANSI/NIST-ITL 1-2011 Update: 2013, Type-20, Type-21 and Type-22
Video Surveillance data exchange	Video clips	December 2012 - Present	ISO 22311

Table 15 - Registry of Video Standards

A video recording in visible wavelengths may be transmitted using the ANSI/NIST-ITL Update: 2013 Type-20 and / or Type-21 records. This may include sources as different as television recordings, videos captured by computer cameras, and infrared videos presented in visible wavelengths. Other videos types, such as used in medical technology are transmitted using a Type-22 record.

ISO 22311 *Societal security – Video Surveillance – Export interoperability* is designed to provide for the exchange of data collected by CCTV systems from different locations.

8. Biometric transmission profiles

Biometric transmission profiles identified in Table 16 are intended to provide interoperability. Such profiles specify application-specific criteria onto the base standard. 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 ISO/IEC 19794-5:2011).

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

- call out values of parameters (e.g., finger number);
- 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 approved standards should be specified as part of requirements documents; furthermore, configurable elements should be based on operational needs of the implementations.

8.1 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.

8.2 Proprietary extensions

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

8.3 Biometric Profiles and Data Models for Large Scale Identification Applications

The biometric transmission profiles of Table 16 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.

The scope of biometric data sharing has expanded to encompass a wider range of operational scenarios that may call for customizable requirements not established in base standards. The biometric transmission profiles recommended above provide an adaptation, constraint, and/or augmentation of the ANSI/NIST-ITL standard to suit the needs of a particular community or an application domain. Since it should be noted that requirements can often change based on real-world events, the use of transmission profiles allows for organizations to more efficiently standardize data without changing the base standard. This flexibility in some instances may cause data to not be fully backwards compatible with legacy devices and vice versa. For example, files provided by systems which originate transactions may not be in a format supported by systems that receive transactions in different versions of the transmission profile are implemented. To ensure the latest requirements and capabilities have been implemented, system integrators are strongly encouraged to coordinate with host organizations prior to implementing recommended biometric transmission profiles. A detailed change log should be included in each biometric transmission profile.

Intended applicability	Validity period	Recommended Transmission Profiles
For sharing biometric and biographical data with the U.S. Government's intelligence community and law enforcement.	December 2009 – Present	TWPDES 3.0
	September 2008 – December 2009	TWPDES 1.2b
For electronically communicating with the Criminal Justice Information Services (CJIS) Division.	July 2013 - Present	FBI EBTS Version 10.0 for both Traditional and XML formats
	December 2011 – July 2013	FBI EBTS Version 9.3
	January 2012 –July 2013	FBI EBTS XML Version 3
	May 2011 – December 2011	FBI EBTS Version 9.2
	March 2010 – January 2012	FBI EBTS XML Version 2
	May 2010 – May 2011	FBI EBTS Version 9.1
	November 2009 – May 2010	FBI EBTS Version 9.0
	November 2008 – November 2009	FBI EBTS Version 8.1
	Through November 2008	FBI EFTS Version 7.1
For communicating electronically between DoD systems that capture biometric data and repositories of biometric data.	April 2013 – Present	DoD EBTS v3.0; and DoD EBTS IDD v5.0; and DoD EBTS Baseline; Application Profile v1.0; and DoD EBTS IEPD v1.0;
	June 2010 – April 2013	DoD EBTS v2.0
	October 2007 – June 2010	DoD EBTS v1.2
For interfacing with one or more OBIM/IDENT messaging services. It describes the IDENT eXchange Messaging (IXM) specification and rules for its use.	October 2013 – Present	IDENT IXM version 6.0.7
	June 2010 – October 2012	IDENT IXM version 5.0
For exchanging biometric data in a NATO.	October 2013 - Present	STANAG 4715 – NATO Biometrics Data, Interchange, Watch listing and reporting Standard
For supplementing the ANSI/NIST-ITL standard for the guidance of members of the International Criminal Police Organization.	June 2010 – Present	Interpol Implementation of ANSI/NIST-ITL 1-2007 (INT-Ib)
	October 2005 – November 2010	Interpol Implementation of ANSI/NIST-ITL 1-2000

Intended applicability	Validity period	Recommended Transmission Profiles
		(INT-I)
Exchange of latent prints and data among law enforcement agencies.	February 2013 - Present	Latent Interoperability Transmission Specification (LITS)

Table 16 - Registry of Biometric Transmission Profiles

Table 16 does not include other profiles that are used internationally (such as that of the Royal Canadian Mounted Police or of the European Visa Information System), or state and local profiles such as those of New York, Florida and Texas. The reason is that this document is focused upon the transmission profiles that are used by the USG. It may be necessary, upon occasion to interface with non-USG systems that use different profiles, which is acceptable practice.

8.4 Terrorist Screening Center

The Terrorist Screening Center's Business Model is to reduce effort on our partners by sharing Terrorist Screening Database information in their preferred format. The TSC's primary exchange of Known or Suspected Terrorist (KST) data is the Terrorist Watchlist Person Data Exchange Standard (TWPDES). TWPDES was developed by the intelligence community to exchange information about KST's. TWPDES provides a comprehensive XML based standard for exchanging and sharing terrorist-related information with biometric and biographic support in a single package across the entire intelligence and law enforcement communities in the United States and internationally. It incorporates the ANSI/NIST-ITL 2-2008 standard's format for the interchange of biometric information and is NIEM compliant.

TWPDES 3.0, a minor upgrade to TWPDES 1.2b, is NIEM 2.0 compliant and supports 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. One of the goals of TWPDES is to provide not only biographic, but also biometric data for the communication of known and suspected terrorist (KST) information across the intelligence community, law enforcement and international communities, as appropriate. TWPDES 3.0 includes support for biometric identifiers at the person level, support for encounter reporting, including biometrics gathered in an encounter and a more robust watchlisting support. In addition, it is backwards compatible with TWPDES 1.2a and TWPDES 1.2b. The biometric sections of TWPDES 3.0 are compliant with the ANSI/NIST ITL 2-2008 biometric standard as approved on August 12, 2008. 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 3.0 was approved December 2009 and has been accepted by Office of the Director of National Intelligence (ODNI), DHS, DoD and FBI.

8.5 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 replaced by Next Generation Identification (NGI) to incorporate additional functionalities including new biometric modalities and higher accuracy rates. As NGI has been phased into service, the FBI EBTS was continually updated to keep pace with newly installed NGI enhancements, culminating in EBTS 10.0.x, which represents NGI's Full Operational Capacity (FOC). It inherits the basic requirements for logical records set forth in the ANSI/NIST-ITL 1-2011 standard. The FBI EBTS's scope has been expanded over previous versions to include additional biometric modalities (e.g., palm print, face, 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.

8.6 Department of Defense

The DoD Electronic Biometric Transmission Specification (EBTS) was developed by the DoD Biometrics Standards Working Group and lead by the Defense Forensics and Biometrics Agency as a biometric and contextual data transmission format standard for the exchange of biometric and contextual information within the DoD. The DoD ABIS is an electronic database and an associated set of software applications that support the storage, retrieval, searching and matching of biometric related data collected from persons of national security interest. Due to the mission of the DoD, additional operational requirements beyond those defined in the ANSI/NIST ITL are defined in the DoD specification and its supplemental documentation. The DoD-unique capabilities are defined in the current version of the DoD EBTS Integrated Data Dictionary.

The first widely distributed version of the DoD EBTS v1.2 was released by DFBA in November 2006. That document described a set of capabilities that were 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 version DoD EBTS v2.0:

- As biometric support for various DoD mission activities 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 through the use of DoD EBTS Application Profiles. This broader set of scenarios necessitated the use of a mechanism to tailor the DoD EBTS to individual applications. This mechanism called “Application Profiles” 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.
- Data elements pertaining to biometric data collection and sharing have been defined in a Glossary, an Integrated 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.

- The DoD ABIS 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).

The Defense Forensics and Biometrics Agency and the DoD Forensic and Biometric Standards Working Group released an updated version of DoD EBTS to allow for additional capabilities and modalities. The DoD EBTS v3.0 and IEPD v1.0 is based on ANSI/NIST ITL 1-2011; new functionality to DoD EBTS v3.0 adopted from ANSI/NIST-ITL 1-2011 is as follows:

- Type-18 shall be used to exchange DNA and related data
- Type-20 shall contain the source representation(s) from which other Record Types were derived
- Type-21 shall contain an associated context, audio/visual recording or other related data (i.e., pocket litter)
- Type-98 shall contain security information that allows for the assurance of the authenticity and/or integrity of the transaction including such information as binary data hashes, attributes for audit or identification purposes and digital signatures

Additionally, DoD EBTS v3.0 relies on companion documents to be consistently implemented: such as the DoD EBTS Integrated Data Dictionary v5.0 which defines individual data elements, the DoD EBTS Baseline Application Profile which describes mandatory and optional fields for commonly used Types of Transactions (TOTs), and Information Exchange Package Documentation for XML implementation.

Currently the DoD is developing revisions to the DoD Biometrics IEPD which aims to incorporate the ANSI/NIST ITL 1-2011 Update: 2013 and align with NIEM v3.0.

8.7 Department of Homeland Security

The Automated Biometric Identification System (IDENT) Exchange Messages (IXM) Specification is the transmission profile required for communicating with the Office of Biometric Identity Management (OBIM), formerly known as the US Visitor and Immigrant Status Indicator Technology (US-VISIT), IDENT system. The IDENT database was developed in 1994 to support rapid identification of subjects for immigration purposes.

The IXM is an XML based message exchange format provides an easy-to-manage, standards based interface to the services offered by OBIM. The specification was designed for high volume rapid transaction processing of biometric and biographic data, and leverages existing data standards and data exchange models. IXM v5.0 and earlier versions also supports binary data transmission using existing Web services specifications and technology. IXM v5.0 and earlier versions of the specification are based on the Global Justice XML Data Model (GJXDM) and the ANSI/NIST-ITL 1-2000 standard.

IXM v6.0 was developed to support additional modalities and services, and is conformant with ANSI/NIST-ITL 1-2011 and NIEM v2.1 design rules. As a NIEM-based version, IXM v6.0 is not backward compatible with prior versions, which are based on the GJXDM data model. However conversion from IXM v5.0 to IXM v6.0.7 can be accomplished via straightforward syntactic translations using common XML tools. Unlike previous versions, IXM v6.0.7 does not support the binary coded form of the FBI EBTS or DOD EBTS as an embedded attachment to IXM messages. OBIM is collaborating with the FBI and DOD to achieve and maintain full interoperability between DHS' IDENT, the FBI's IAFIS and the DOD ABIS system.

IXM 7.0 has been developed and is NIEM conformant; however, 7.0 is not currently in production but when it is will be made available on www.biometrics.gov

9. Biometric identity credentialing profiles

Homeland Security Presidential Directive 12 (HSPD - 12), dated August 27, 2004, entitled "Policy for a Common Identification Standard for Federal Employees and Contractors," directed the promulgation of a Federal standard for secure and reliable forms of identification for Federal employees and contractors. It further specified secure and reliable identification that—

- Is issued based on sound criteria for verifying an individual employee's identity
- Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation
- Can be rapidly authenticated electronically
- Is issued only by providers whose reliability has been established by an official accreditation process.

The directive stipulates that standards include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application.

Intended applicability	Validity period	Recommended Credentialing Profiles
Specifies the architecture and technical requirements for a common identification standard for Federal employees and contractors.	September 2013 - Present	FIPS 201-2, 2013: Personal Identity Verification (PIV) of Federal Employees and Contractors.
	October 2007 – September 2013	FIPS 201-1, 2006: Personal Identity Verification (PIV) of Federal Employees and Contractors.
Describes technical acquisition and formatting specifications for the biometric credentials of the PIV system, including the PIV Card itself.	July 2013 - Present	NIST SP-800-76-2, 2013
	October 2007 -- Present	NIST SP-800-76-1, 2007 ADD Row for 800-76-2 July 2013

Intended applicability	Validity period	Recommended Credentialing Profiles
Fosters a fully interoperable, vendor-neutral Registered Traveler (RT) program within the United States.	April 2008 -- Present	Registered Traveler Interoperability Consortium Technical Interoperability Specification Version 1.7 April 15, 2008
	March 2008—April 2008	Registered Traveler Interoperability Consortium Technical Interoperability Specification Version 1.6 March 10, 2008
	December 2007 – March 2008	Registered Traveler Interoperability Consortium Technical Interoperability Specification Version 1.5 December 21, 2007
Specifies the behavior at the card interface of the TWIC card application as well as the requirements for TWIC readers, both fixed and portable, to be used with the Transportation Worker Identification Credential (TWIC)	May 2008 - Present	TWIC Reader Hardware and Card Application Specification, Version 1.1.1 May 2008
	October 2007 – May 2008	TWIC Reader Hardware and Card Application Specification, Version 1 September 2007
Specifies the usage of inter-industry commands and data objects related to personal verification through biometric methods	October 2007 - Present	ISO/IEC 7816-11:2004

Table 17 - Registry of 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 for FIPS 201-2 are specified in NIST Special Publication 800-76-2, Biometric Data Specification for Personal Identity Verification. This now includes a section for iris data specifications, extending the format requirements of ISO/IEC 19794-6:2011 with image quality related properties.

The TWIC Reader Hardware and Card Application Specification leverages FIPS 201. For all transportation workers requiring unescorted physical 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 card readers to be used with the TWIC. TWICs are tamper-resistant biometric credentials issued

to workers who require unescorted access to secure areas of ports, vessels, outer continental shelf facilities and all credentialed merchant mariners.

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. After TSA's pilot ended in July 2008, all RT service providers were obligated to follow data security standards to continue offering service. Each service provider's use of data, however, is regulated under its own privacy policy and by its relationship with its customers and sponsoring airport or airline. Editors Note: Update from TSA or remove paragraph and associated tables

10.Biometric technical interface standards

The biometric technical interface standards listed in Table 18 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 (ISO/IEC 19784 series and INCITS 358) support "plug and play" compatibility by specifying how applications communicate with biometric vendor software in a common way independent of the biometric modality. This supports the swapping of products and the incorporation of new products with no application modification.

Intended applicability	Validity period	Recommended Standard(s)
Establishes the framework 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.	October 2007 – Present	INCITS/ISO/IEC 19784-1:2006 [2007]
	October 2007 – November 2010	INCITS 358-2002
Defines the interface between a biometric service provider (BSP) and a biometric archive function provider (BAFP) for BioAPI.	October 2007 – Present	INCITS/ISO/IEC 19784-2:2007 [2008]
Specifies a biometric sensor interface for a Biometric Service Provider	December 2011 – Present	INCITS/ISO/IEC 19784-4:2011 [2011]
Defines a basic structure for standardized biometric information records (BIRs) that consists of three parts, the standard biometric header (SBH), the biometric data block (BDB), and the security block (SB)	October 2007 – Present	INCITS/ISO/IEC 19785-1:2006 [2008]
Support for additional data elements in 19785-1	October 2010 – Present	INCITS/ISO/IEC 19785-1:2006/Amd 1:2010 [2010]

<table>
<tr><th>Intended applicability</th><th>Validity period</th><th>Recommended Standard(s)</th></tr>
<tr><td>Specifies several patron formats that conform to the requirements of ISO/IEC 19785-1</td><td>October 2007 – Present</td><td>INCITS/ISO/IEC 19785-3:2007 [2008]</td></tr>
<tr><td>Support for additional data elements in 19785-3</td><td>October 2010 – Present</td><td>INCITS/ISO/IEC 19785-3:2007/Amd 1:2010 [2010]</td></tr>
<tr><td rowspan="2">Specifies a common set of data elements necessary to support multiple biometric technologies and to promote interoperability of biometric-based application programs and systems by allowing for biometric data exchange.</td><td>October 2008 – Present</td><td>INCITS 398-2008<table><tr><th>#</th><th>Name</th><th>Domain</th></tr><tr><td>1</td><td>Patron Format A</td><td>General purpose</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></td></tr>
<tr><td>October 2007 – October 2008</td><td>INCITS 398-2005</td></tr>
<tr><td rowspan="2">Specifies biometric services for identity assurance that are invoked over a services-based framework</td><td>December 2011 – Present</td><td>INCITS 442-2010</td></tr>
<tr><td>December 2008 – December 2011</td><td>INCITS 442-2008</td></tr>
<tr><td>Provides a common, yet flexible, Web services interface that can be used within both closed and open SOA systems.</td><td>May 2012 – Present</td><td>OASIS Biometric Identity Assurance Services (BIAS) SOAP Profile version 1, May 2012</td></tr>
<tr><td>Provides a command and control protocol for biometric devices.</td><td>March 2012 - Present</td><td>NIST Special Publication 500-288 Specification for WS-Biometric Devices (WS-BD)</td></tr>
</table>

Table 18 - Registry of Biometric Technical Interfaces

The CBEFF standard (INCITS 398) specifies data structures that support multiple biometric technologies in a common way. CBEFF's data structures, termed Biometric Information Records (BIRs), conform to a CBEFF Patron Format that allows for exchange of biometric data and related metadata (e.g., time stamp, validity period, and creator); moreover, it supports security of biometric data in an open systems environment. While the current recommended CBEFF standard is INCITS 398-2005 for FIPS 201-1, 2006 and ANSI/NIST-ITL 1-2011(Type-99), this standard has been withdrawn and is no longer being maintained by INCITS. Additionally, the FIPS 201 standard states that PIV cards shall adopt certain defined constants from ISO/IEC 19785-3:2007 for on-card matching. NIST has developed the Conformance Test Suite (CTS) for "Patron Format A" data structures specified in INCITS 398-2008 to help users determine whether binary file implementations of BIRs based on this Patron Format

conform to the standard. The International Biometrics and Identification Association (IBIA) recognizes both ISO/IEC 19785-1 and INCITS 398-2005 CBEFF versions. It should be noted that INCITS 398-2005 is not backwards compatible with enhanced revisions.

The Biometric Identity Assurance Services (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. The BIAS SOAP Profile is a specific implementation (or binding) of INCITS 442-2010, which defines the requirements for BIAS operations and data elements that can be implemented using any encoding scheme or messaging protocol. The BIAS SOAP Profile defines a conformant implementation. These SOAP-based services enable a software application (requester) to invoke biometric identity assurance operations provided by a local or remote BIAS service provider (responder).

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.

For data interchange standards, the

- **LEVEL 1 TESTING –** in a data interchange standard, a conformance testing methodology that checks field by field and byte by byte conformance with the specification of the BDIR as specified in the standard, both in terms of fields included and the ranges of the values in those fields [ISO/IEC 19794-1:2011]

  NOTE This type of testing tests morphological requirements of the base standard.

- **LEVEL 2 TESTING -** conformance testing methodology that tests the internal consistency of the BDIR under test, relating values from one part or field of the BDIR to values from other parts or fields of the BDIR [ISO/IEC 19794-1:2011]

  NOTE This type of testing tests syntactic requirements of the base standard.

- **LEVEL 3 TESTING -** conformance testing methodology that tests that a BDIR is a faithful representation of the BDIR subject to the constraints of the parameters in the metadata records [ISO/IEC 19794-1:2011]

  This type of testing tests semantic requirements of the base standard.

The biometric conformance testing methodology standards listed in Table 19 should be considered for all test runs, commissioned or otherwise sponsored by USG agencies.

Intended applicability	Validity period	Recommended Standard(s)
Specifies criteria for ensuring the image quality of	July 2013 -	FBI EBTS Version 10.0,

Intended applicability	Validity period	Recommended Standard(s)
fingerprint scanners and printers that input fingerprint images to, or generate fingerprint images from within, the Integrated Automated Fingerprint Identification System (IAFIS).	Present	Appendix F
	December 2011 – July 2013	FBI EBTS Version 9.3, Appendix F
	September 2007 – December 2011	FBI EBTS Version 8.1, Appendix F
Specifies 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)	October 2007 – Present	INCITS/ISO/IEC 24709-1:2007[2009]
Specifies test assertions for testing conformance of BSPs of all conformance subclasses.	October 2007 – Present	INCITS/ISO/IEC 24709-2:2007[2009]
Defines a number of test assertions written in the assertion language specified in ISO/IEC 24709-1:2007. These assertions enable a user of ISO/IEC 24709-3:2011 (such as a testing laboratory) to test the conformance to ISO/IEC 19784-1 (BioAPI 2.0) of any BioAPI Framework that claims to be a conforming implementation of ISO/IEC 19784-1. Each test assertion specified in ISO/IEC 24709-3:2011 exercises one or more features of an implementation under test.	December 2011 – Present	ISO/IEC 24709-3:2011
Specifies generalized conformance testing methodologies for 1st Generation 19794 Data interchange records.	December 2009 – Present	INCITS/ISO/IEC 29109-1:2009[2010]
Conformance testing methodology for INCITS/ISO/IEC 19794-5:2005[2007] when using 2D.	December 2010 – Present	ISO/IEC 29109-5:2012
Specifies generalized conformance testing methodologies for 2nd Generation 19794 Data interchange records.	December 2011 – Present	ISO/IEC 19794-1 AMD 1:2011
Methodology Standard for Biometric Data Interchange Format Standards – Part 1: Generalized Conformance Testing Methodology for INCITS data interchange records	October 2007 – July 2012	INCITS 423.1-2008
Specifies conformance testing of application(s) or service(s) implementations claiming conformance to the INCITS 378-2004 standard.	October 2007 – July 2012	INCITS 423.2-2008
Specifies conformance testing of application(s) or service(s) implementations claiming conformance to the INCITS standard INCITS 398:2008.	December 2011 – Present	INCITS 473-2011
NIST Special Publication 500-295 Conformance Testing	December 2011	NIST SP 500-295

Intended applicability	Validity period	Recommended Standard(s)
Methodology for ANSI/NIST-ITL 1-2011, Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information (ANSI/NIST_ITL 1-2011 Record Types 1,4,10,13,14,15 and 17)	- Present	

Table 19 - Registry of Conformance Testing Methodologies

While conformance of individual elements of data interchange records to relevant requirements can be determined, no test can be absolutely comprehensive and prove that a given system generating or using biometric data interchange records is conformant under all possible circumstances, especially when there are optional components of the standard. A well designed conformance test can, however, test all of the most likely sources of problems and ensure that the implementation under test conforms under a reasonable set of circumstances, giving assurance, but not a guarantee, of conformance.

NOTE Conformance testing methodologies for 19794 Data interchange Formats 19794-x of second (2G) generation standards are currently under development. The trend is to merge conformance criteria and methodologies into the base standards.

12.Biometric performance testing methodology standards

The biometric performance testing methodology standards listed in Table 20 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.

Intended applicability	Validity period	Recommended Standard(s)
Present the requirements and best scientific practices for conducting technical performance testing	October 2007 – Present	INCITS/ISO/IEC 19795-1:2005[2007]
Defines "technology" and "scenario" evaluations	October 2007 – Present	INCITS/ISO/IEC 19795-2:2007[2009]
Describes the methodologies relating to these modality-dependent variations. It presents and defines methods for determining, given a specific biometric modality, how to develop a technical performance test	October 2007 – Present	ISO/IEC TR 19795-3:2007
Prescribes methods for technology and scenario evaluations of multi-supplier biometric systems that use biometric data conforming to biometric data interchange format standards	December 2008 – Present	INCITS/ISO/IEC 19795-4:2008
Specifies a framework for testing and a grading scheme for reporting the performance of a	January 2011 – Present	INCITS/ISO/IEC 19795-5:2011

Intended applicability	Validity period	Recommended Standard(s)
biometric system suitable for use in access control applications		
Specifies metrics and provides guidance on the operational testing for biometric systems	July 2012 – Present	INCITS/ISO/IEC 19795-6:2012
Testing of On-Card biometric comparison algorithms	November 2011 – Present	INCITS/ISO/IEC 19795-7:2011

Table 20 - Registry of Performance Testing Methodologies

Testing a biometric system will involve the collection of input images or signals, which are used for template generation at enrollment and for calculation of matching scores for verification or identification attempts. The images/signals collected can either be used immediately for an online enrollment, verification or identification attempt, or may be stored and used later for offline enrollment, verification or identification.

In a technology evaluation, testing of all algorithms is carried out on a standardized corpus, ideally collected by a "universal" sensor (i.e. a sensor that collects samples equally suitable for all algorithms tested). Performance against this corpus will depend on both the environment and the population in which it is collected. Prior to technology tests example data may be distributed for developmental or tuning purposes. Actual testing needs to be done on data that has not previously been seen by algorithm developers, and is carried out using offline processing of the data. Because the corpus is fixed, the results of technology tests are repeatable.

In a scenario evaluation, testing is carried out on a complete system in an environment that models a real-world target application of interest. Each tested system will have its own acquisition sensor and so will receive slightly different data. Consequently, if multiple systems are being compared, care will be required that data collection across all tested systems is in the same environment with the same population. Depending on the data storage capabilities of each device, testing might be a combination of offline and online comparisons. Test results will be repeatable only to the extent that the modeled scenario can be carefully controlled.

In an operational evaluation, depending on the data storage capabilities of the operational system, offline testing might not be possible. In general, operational test results will not be repeatable because of unknown and undocumented differences between operational environments. Furthermore, "ground truth" (i.e. who was actually presenting a "good faith" biometric measure) can be difficult to ascertain, particularly if an operational evaluation is performed under unsupervised conditions without an administrator, operator or observer present.

13. References

1.	ANSI/NIST-ITL 1-2011	Data Format for the Interchange of Fingerprint, Face, & Other Biometric Information Published as NIST Special Publication 500-290, Rev.1 December 2013.

	Update: 2013	(adds new record types and fields to the base 2011 standard) http://www.nist.gov/itl/iad/ig/ansi_standard.cfm
	ANSI/NIST-ITL 1-2011	Data Format for the Interchange of Fingerprint, Face, & Other Biometric Information Published as NIST Special Publication 500-290, November 2011. http://www.nist.gov/itl/iad/ig/ansi_standard.cfm
2.	ANSI/NIST-ITL 1-2007	Data Format for the Interchange of Fingerprint, Face, & Other Biometric Information – Part 1. Published as NIST Special Publication 500-271, May 2007. http://www.nist.gov/itl/iad/ig/ansi_standard.cfm
3.	ANSI/NIST-ITL 1a 2009	Amendment to ANSI/NIST-ITL 1-2007 establishing code for multi-finger impressions. http://www.nist.gov/itl/iad/ig/ansi_standard.cfm
4.	ANSI/NIST-ITL 2-2008	Data Format for the Interchange of Fingerprint, Face, & Other Biometric Information – Part 2: XML Version, Published as a NIST Special Publication 500-275, August 2008 http://www.nist.gov/itl/iad/ig/ansi_standard.cfm
5.	BioCTS	Conformance test tool for ANSI/NIST_ITL 1-2011 www.nist.gov/itl/csd/biometrics/biocta_download.cfm
6.	DoD EBTS	DoD Electronic Biometric Transmission Specification (EBTS) http://www.dfba.mil/References/Standards.aspx
7.	DoD EBTS IDD	DoD Electronic Biometric Transmission Specification (EBTS) Integrated Data Dictionary http://www.dfba.mil/References/Standards.aspx
8.	DoD EBTS XML IEPD	DoD Electronic Biometric Transmission Specification (EBTS) Information Exchange Package Documentation http://www.dfba.mil/References/Standards.aspx
9.	FBI EBTS	FBI Electronic Biometric Transmission Specification (EBTS) https://www.fbibiospecs.org/ebts.html
10.	FBI EBTS XML IEPD	FBI Electronic Biometric Transmission Specification (EBTS) Information Exchange Package Documentation https://www.fbibiospecs.org/ebts.html
11.	FIPS 201-2, 2013	Personal Identity Verification for Federal Employees and Contractors http://csrc.nist.gov/publications/PubsFIPS.html
12.	HSPD -12	Policy for a Common Identification Standard for Federal Employees and Contractors http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm
13..	ICAO 9303	Part 1 - Machine Readable Passport - Volume 2 Specifications for Electronically Enabled Passports with Biometric Identification Capabilities http://www.icao.int/Security/mrtd/Pages/Document9303.aspx SUPPLEMENT to Doc 9303
14.	INCITS 358	INCITS 358:2002 [R2007] - American National Standard for Information Technology – The BioAPI Specification http://webstore.ansi.org/
15.	INCITS 378	INCITS 378-2004 - American National Standard for Information Technology — Finger Minutiae Format for Data Interchange http://webstore.ansi.org/
16.	INCITS 381	INCITS 381-2004 - American National Standard for Information Technology — Finger Image-Based Data Interchange Format. http://webstore.ansi.org/

17.	INCITS 398	INCITS 398-2008 - Common Biometric Exchange Formats Framework (CBEFF) http://webstore.ansi.org/
18.	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/
19.	INCITS 423.2	INCITS 423.2-2008 - Conformance testing Methodology Standard for Biometric Data Interchange Format Standards - Part 2: Conformance Testing, Finger Minutiae http://webstore.ansi.org/
20.	INCITS 442	INCITS 442-2010 - Biometric Identity Assurance Services (BIAS) http://webstore.ansi.org/
21.	INT-I	ANSI/NIST-ITL 1-2000 Date Format for the Interchange of Fingerprint, Face & SMT Information INTERPOL Implementation, Version No. 4.22b - October 28, 2005 https://www.interpol.int/Public/Forensic/Fingerprints/RefDoc/default.asp
22.	INT-Ib	INTERPOL Implementation Version 5 (ANSI/NIST-ITL 1-2000), The INTERPOL AFIS Expert Group Version 5.0 – Oct 23, 2008 https://www.interpol.int/Public/Forensic/Fingerprints/RefDoc/default.asp
23.	ISO 22311	ISO 22311 First edition 2012-11-15 Societal security – Video-surveillance – Export interoperability
24.	ISO/IEC 15948	ISO/IEC 15948:2004 Computer graphics and image processing – Portable Network Graphics (PNG): Functional specification. http://webstore.ansi.org/
25.	ISO/IEC 19784-1	INCITS/ISO/IEC 19784-1:2006[2007] BioAPI – Biometric Application Programming Interface – Part 1: BioAPI Specification http://webstore.ansi.org/
26.	ISO/IEC 19784-5/Amd 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
27.	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/
28.	ISO/IEC 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/
29.	ISO/IEC 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/
30.	ISO/IEC 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/
31.	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
32.	ISO/IEC 19794-4	INCITS/ISO/IEC 19794-4:2011 — Information technology — Biometric data interchange formats — Part 4: Finger image data. http://webstore.ansi.org/
33.	ISO/IEC 19794-5	INCITS/ISO/IEC 19794-5:2011 — Information technology — Biometric data interchange formats — Part 5: Face image data. http://webstore.ansi.org/
34.	ISO/IEC 19794-5/AMD 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/
35	ISO/IEC 19794-6	INCITS/ISO/IEC 19794-6:2011 - Information technology — Biometric data interchange formats — Part 6: Iris image data. http://webstore.ansi.org/
36.	ISO/IEC 19794-14	ISO/IEC 19794-14:2012 Information technology — Biometric data interchange formats — Part 14: DNA data. http://webstore.ansi.org/
37.	ISO/IEC 19795-1	INCITS/ISO/IEC 19795:2005[2007] - Biometric Performance Testing and Reporting – Part 1: Principles and Framework http://webstore.ansi.org/
38.	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/
39.	ISO/IEC 19795-3	ISO/IEC TR 19795:2007 - Biometric Performance Testing and Reporting – Part 3: Modality-Specific Testing http://webstore.ansi.org/
40.	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/
41.	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/
42.	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/
43.	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/
44.	IXM 5.0	Automated Biometric Identification System (IDENT) Exchange Messages (IXM) Specification – v5.0

		http://www.biometrics.gov/standards
45.	MINEX04	P. Grother et al., *Performance and Interoperability of the INCITS 378 Template,* NISTIR 7296 http://fingerprint.nist.gov/minex04/minex_report.pdf
46.	NIEM	National Information Exchange Model https://www.niem.gov/Pages/default.aspx
47.	NIST SP 500-288	NIST Special Publication 500-288, Specification for WS-Biometric Devices (WS-BD), Version 1, March 2012 http://www.nist.gov/itl/iad/ig/bws.cfm
48.	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
49.	NSPD – 59/HSPD - 24	National Security Presidential Directive and Homeland Security Presidential Directive http://www.biometrics.gov/Documents/NSPD59%20HSPD24.pdf
50.	OASIS BIAS SOAP Profile	Biometric Identity Assurance Services (BIAS) SOAP Profile v.1 www.oasis-open.org/standards, May 2012
51.	RTIC	Registered Traveler Interoperability Consortium (RTIC), Technical Interoperability Specification, Version 1.7, April 15, 2008. http://www.rtconsortium.org/_docpost/RTICTIGSpec_v1.7.pdf
52.	TWIC	TWIC Reader Hardware and Card Application Specification, May 30, 2008. http://www.tsa.gov/sites/default/files/publications/pdf/twic/twicreaderhardwareandcardapplicationspecification.pdf
53.	TWPDES	Terrorist Watchlist Person Data Exchange Standard, Version 3.0. https://www.niem.gov/documentsdb/Documents/Technical/TWPDES_3_final.zip
54.	WSQv3.1	WSQ Gray-Scale Fingerprint Image Compression Specification, IAFIS-IC-0110(V3.1), October 04, 2010. https://www.fbibiospecs.org/docs/WSQ_Gray-scale_Specification_Version_3_1_Final.pdf

Table 21 - Reference of Standards