Catalog of USG Biometric Product Testing Programs

Version 1.0
November 15, 2010

**NSTC Subcommittee on
Biometrics and Identity Management**

1. Introduction

This *Catalog of USG Biometric Product Testing Programs* (Catalog) supplements the *Registry of USG Recommended Biometric Standards*, which was developed through a collaborative, interagency process within the Subcommittee on Biometrics and Identity Management and approved by the NSTC Committee on Technology. This document provides a listing of Federal biometric testing and certification programs, and is a supplementary guide to Federal agencies as they develop and implement biometric programs. The Subcommittee's standards and conformity assessment working group is tasked to develop and update the Catalog.

The content of this document will be reviewed, revised and updated regularly to assist agencies in the implementation and reinforcement process of using USG recommended biometric standards to meet agency-specific mission needs. The latest version of this document is available on the Federal government's web site for biometric activities at www.biometrics.gov/standards.

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

Another document supporting the *Registry of USG Recommended Biometric Standards* is the *Supplemental Information in Support of the NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards.*

2. Scope

This document lists active programs that test biometric products against USG recommended standards as listed in the *Registry of USG Recommended Biometric Standards*. The Catalog addresses only the biometric aspects of the testing program. It does not include non-biometric aspects of the products related to the use of these products such as security or environmental testing.

The Catalog takes into account the need to support current implementations as well as new implementations as referenced in the *Registry of USG Recommended Biometric Standards*. The Registry includes conformance, performance, and interoperability testing standards.

The Catalog does not describe differences in how various implementing entities have designed their Biometric Testing and Certifications Programs. Details of various testing programs should be assessed by the user to determine applicability to their needs. Additional testing programs will be added to this Catalog as they are implemented.

3. Purpose of Document

This document is intended as an informative guide for program managers seeking to find biometric products that have been tested against standards recommended by the Registry of USG Recommended Biometric Standards. It also provides a description of a framework that can be used by the agencies to develop additional product tests to meet specific Agency requirements. This description is also intended to stimulate the development of a common framework for testing and listing biometric products to support greater interoperability between the various USG users of biometric products.

4. Terms and definitions

For the purposes of this document, the following terms and definitions apply.

- **acceptance (of biometrics products) -** The administrative act by the Procurement Agency of adopting biometrics products for its needs, based upon the vendor's self-declaration of conformity to specified standards and requirements
- **accreditation** - Formal recognition that a laboratory is competent to carry out specific tests or calibrations or types of tests or calibrations
- **accreditation authority -** An organization that accredits laboratories that perform conformance testing, interoperability testing, technology testing, scenario testing, operational and usability testing for biometrics products (systems and subsystems) as defined in nationally and internationally recognized biometrics products testing standards of biometric systems and subsystems
- **approved product** – A product approved by an authorization authority for use in the designated set of applications
- **Approved Products List (APL)** – A list of products that are in compliance with the specified version of the appropriate Standards and its supporting list of products
- **assessment -** The administrative act by the QPL/APL owner and/or Conformity Assessment Council of determining conformance of a biometrics product to specified standards and requirements based, at minimum, on test results prepared by the accredited laboratories and submitted by the laboratory at the direction of the vendor
- **authorization authority -** An entity with the authority to make official permission or approvals to use a product for the designated applications
- **base standard** - A fundamental standard with elements that contain options. Base standards can be used in diverse applications, for each of which it may be useful to fix the optional elements in a standardized profile with the aim of achieving interoperability between instances of the specific application. [ISO/IEC 24713-1:2008]
- **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 [ISO/IEC19795-4:2008 - Information technology — Biometric performance testing and reporting — Part 4: Interoperability performance testing]
- **biometric** – a measurable biological (anatomical and physiological) and/or behavioral characteristic that can be used for automated recognition
- **biometric capture device -** Device that collects a signal from a biometric characteristic and converts it to a captured biometric sample
- **biometric capture subsystem -** Biometric capture device(s) and any sub-processes required to execute a biometric capture process
- **biometric feature extraction -** Process applied to a biometric sample with the intent of isolating and outputting repeatable and distinctive numbers or labels which can be compared to those extracted from other biometric samples
- **biometric profile** - Conforming subsets or combinations of base standards used to effect specific biometric functions. Biometric profiles define specific values or conditions from the range of options described in the relevant base standards, with the aim of supporting the interchange of data between applications and the interoperability of systems. [ISO/IEC 24713-1:2008]
- **certification -** Third-party attestation related to products, processes, systems or persons [ISO/IEC 17000:2004, Conformity assessment — Vocabulary and general principles**]**

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

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

- **Certificate of Accreditation -** Document issued by National Voluntary Laboratory Accreditation Program (NVLAP) to a laboratory that has been granted NVLAP accreditation. A Certificate of Accreditation is always issued with a Scope of Accreditation.

- **Certification Authority-** An organization that certifies testing results performed in accordance with procedures approved by that authority

- **Certified Products List** - A products list that is certified by a certification authority as having been tested and found to be in compliance with the published specifications

- **conformance -** The state of an implementation satisfying the requirements and specifications of a specific standard as tested by a test suite or some approved test method

- **conformance testing -** The testing of an implementation against the requirements specified in one or more standards

- **conformity assessment -** An activity to determine that a biometrics process, product or service meets referenced standards or derived test requirements and fulfills recommended technical requirements. The conformity assessment process could imply an acceptance of the biometrics products based upon vendor's declaration of conformity, an assessments process which requires conformance test reports revision, or a combination of both acceptance and assessment processes

- **Conformity Assessment Council -** A group of technical experts in biometrics systems and subsystems, whose members are equal in power and authority, and whose responsibility is to review the conformity assessment technical requirements and to advise the Qualified/Approved Products List owner on the accuracy and correctness of the biometrics products test reports submitted by vendors with their request to have the product listed on the agency's QPL/APL.

- **laboratory -** Organization that performs tests and/or calibrations. When a laboratory is part of an organization that carries out activities additional to testing and calibration, the term *laboratory* refers only to those parts of that organization that are involved in the testing and calibration process.

- **interoperable performance** - Performance associated with the use of generator and comparison subsystems from different suppliers

- **performance interoperability** - Measure of the adequacy of interoperable performance

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

- **qualified product -** A product that has complied with a set of requirements as attested to by an independent testing entity

- **Qualified Products List (QPL)** - A list of products, qualified under the requirements stated in the applicable specification, including appropriate product identification and test reference with the name and address of the manufacturer or distributor, as applicable. Frequently used interchangeably with Approved Products List.

- **QPL/APL Owner** – An entity that is responsible for the listing of products and services that have complied with the requirements as specified by the QPL/APL entity

- **test** - Technical operation that consists of the determination of one or more characteristics of a given product, process or service according to a specified procedure [ISO/IEC Guide 2:2004]

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

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

- **scenario test** - The online evaluation of end-to-end system performance in a prototype or simulated application in which samples collected from test subjects are processed in real time

[ISO/IEC19795-4:2007 - Information technology — Biometric performance testing and reporting — Part 2: Testing methodologies for technology and scenario evaluation]

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

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

- **validation -** The administrative act by the QPL/APL owner and/or Conformity Assessment Council of determining the accuracy, standard and/or test compliance of the testing tools and/or testing harnesses used by the accredited laboratory for the biometrics product testing. When applicable, the validation of a test tool implies the verification, as far as possible, that the test tool behaves properly and produces results that are consistent with the specifications, with any relevant standards and, if applicable, with a previously validated version of the test tool

- **validation authority -** An entity that validates that all of the requirements for a product have been complied with in accordance to stated requirements

5. Acronyms and Abbreviations

AACP	Airport Access Control Performance
ABIS	Automatic Biometric Identification System
ANSI	American National Standards Institute
APL	Approved Products List
BIAS	Biometric Identity Assurance Services
BIMA	Biometrics Identity Management Agency
BioAPI	Biometric Application Programming Interface
BIR	Biometric Information Record
BSP	Biometric Service Provider
CBEFF	Common Biometric Exchange Format Framework
CD-RW	Compact Disc ReWritable
CJIS	Criminal Justice Information Services
COTS	Commercial-Off-The-Shelf
DHS	Department of Homeland Security
DoD	Department of Defense
EBTS	Electronic Biometric Transmission Specification
EPD	Evaluation Program Development
EFTS	Electronic Fingerprint Transmission Specification
FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standard
GOTS	Government-Off-The-Shelf
HSPD	Homeland Security Presidential Directive
IAFIS	Integrated Automated Fingerprint Identification System
ICE	Initial Capability Evaluation (Part of TSA Program)
IDENT	Automatic Biometric Identification System
IDMS	Identity management system
IEC	International Electrotechnical Commission
INCITS	InterNational Committee on Information Technology Standards
ISO	International Organization for Standardization

ITL	Information Technology Laboratory
IXM	IDENT Exchange Messages
JITC	Joint Interoperability Test Command
JPEG	Joint Photographic Experts Group
MRA	Mutual Recognition Agreement
NIST	National Institute of Standards and Technology
NSTC	National Science and Technology Council
NVLAP	National Voluntary Laboratory Accreditation Program
PIV	Personal Identity Verification
PNG	Portable Network Graphics
SMTP	Simple Mail Transfer Protocol
TWIC	Transportation Workers Identification Credential
USG	United States Government
US-VISIT	United States Visitor and Immigrant Status Indicator Technology
WSQ	Wavelet Scalar Quantization
XML	Extensible Markup Language

6. Major Biometric Programs

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

- GSA's FIPS 201 Evaluation Program for credential and identity management
- FBI's fingerprint image quality certification program
- TSA airport access control performance testing program
- TSA TWIC product testing program (under development)
- DoD Biometric Standards Conformity Assessment Program
- NIST WSQ testing program

There are several independent biometric testing programs that use USG standards. Such programs are not addressed in this document. A laboratory accreditation program for biometrics has been initiated by NIST. This program, called the Biometrics Laboratory Accreditation Program (Biometrics LAP) is being developed under the framework established by the NVLAP. This program will accredit laboratories that perform conformance and scenario testing against nationally recognized biometrics standards. In the future, the program is intended to be expanded to include interoperability testing, technology testing, operational and usability testing.

Differences in the testing, accreditation, and certification programs reflect differences in requirements and in the specifications relating to the applicable standards. Applicability of a testing program to a new set of requirements must be determined by the user who will need to validate that the respective requirements and standards specifications are compatible with the intended use of the product. It should be noted that the testing, accreditation, and certification programs make use of testing conducted by other programs. For example many GSA FIPS 201 products rely on FBI image quality certification and some TSA product components rely on FIPS 201 certification.

International and independent programs are not addressed in this document.

7. Biometric Testing and Certification Programs

This section provides a description of the scopes of the USG sponsored biometric testing and certification programs. The scope is defined in terms of the products and/or capabilities that are

addressed by each of the programs. Where appropriate, reference to recommended USG standards is provided.

The testing methods and standards used by the various testing programs typically address different sets of requirements. Sometimes these requirements overlap, at other times they are different, reflecting the needs of the organizations and/or of the testing organizations legacy role assignments and capabilities. Typically, most of the product testing programs use results provided by other organizations such as the FBI and NIST. However, the extent of acceptance of test results by other parties is limited to a small set of capabilities (e.g. Appendix F certification, WSQ certification). The development of this Catalog is intended to help identify potential product similarities in order to encourage greater cross-acceptance of product test results.

In general, the testing programs should utilize, as applicable, available standardized testing methodologies (and tools implementing these methodologies), especially to perform conformance testing to the adopted base standards, biometric performance testing, and biometric sample quality measurement. The results of the tests performed by accredited testing laboratories and certified by established certification authorities, can be recognized and accepted across multiple testing programs (usually engaged in Mutual Recognition Agreements, or MRA) without the need to repeat the testing.

7.1 GSA FIPS 201 Evaluation Program

FIPS 201: Personal Identity Verification (PIV) of Federal Employees and Contractors grew out of the Homeland Security Presidential Directive 12 (HSPD-12) to develop the architecture and technical requirements for a common identification standard for Federal employees and contractors. The standard describes the minimum requirements for a system that meets the control and security objectives of HSPD-12, including detailed specifications that will support technical interoperability among PIV systems of Federal departments and agencies. It describes the card elements, system interfaces, and security controls required to securely store, process, and retrieve identity credentials from the card.

The framework to support the required functionality includes an Evaluation Program that specifies GSA's Evaluation Program Development (EPD) Laboratory (Lab) operation to determine compliance of vendor products and services against the requirements of Federal Information Processing Standard (FIPS) 201 and its related publications. The EPD describes the laboratory documentation, forms and templates, approval procedures, test procedures, and provides linkages to other supporting documents and test tools. The EPD also provides a current listing of all approved products and instructions for product testing and approval.

The FIPS 201 web site[1] provides an extensive listing of the products and services that are evaluated by the EPD[2]. Many of the products or services are not biometric, but are required to support the PIV functionality. Table 1 indicates all products that are tested by the EPD against biometric standards that are included in the USG Registry.

---

[1] See http://fips201ep.cio.gov/
[2] For detailed EPD program description see
http://fips201ep.cio.gov/documents/FIPS201epdCONOPS.pdf

Table 1 – PIV 201 Evaluation Program Products and Services

No	Item	Description	USG Recommended Biometric Standards	Testing Provided By Other Entities
1	Card Reader - Biometric	Device consisting of both a contact smart card reader and a fingerprint capture device. The device authenticates a PIV Cardholder by extracting one (or both) fingerprint biometric template(s) stored on the card and matching it (them) with live fingerprint(s) biometric samples presented by the cardholder at the fingerprint capture device.	FIPS 201-1, 2006 NIST SP 800-76-1, 2007 INCITS 378:2004	FBI certification of fingerprint image quality to PIV-071006[3]
2	Facial Image Capturing (Middleware)	A software component that provides the capability to accept facial images captured by the Facial Image Capturing Camera and to format those images for storage in accordance with NIST SP 800-76-1.	FIPS 201-1, 2006 NIST SP 800-76-1, 2007	
3	Facial Image Capturing Camera	Equipment needed to capture the raw facial image photographs of Applicants as part of the registration process. Additionally, the camera may utilize software to control the functions of the camera, such as optical zoom, contrast, and brightness.	FIPS 201-1, 2006 NIST SP 800-76-1, 2007	
4	Fingerprint Capture Station	Equipment used to electronically capture and transmit a full set of fingerprints for use in the background checks as part of the identity proofing and registration process.	SP 800-76-1 References: FBI EBTS Version 8.1, Appendix F ANSI/NIST-ITL 1-2007, Type 14 INCITS 381:2004Profile Generation	FBI Certification of Appendix F fingerprint image quality
5	Single Fingerprint Capture Device	The Single Fingerprint Capture Device is a biometric capture device that is used for capturing live fingerprint(s) biometric sample(s) in order to authenticate the cardholder (e.g. upon receipt of the PIV Card). NIST SP 800-76-1 minutiae templates may be generated in this device, however matching of the authentication template to the enrollment template does not occur on the device.	FIPS 201-1, 2006 NIST SP 800-76-1, 2007	FBI certification of fingerprint image quality to PIV-071006

---

[3] See http://www.fbibiospecs.org/fbibiometric/iafis_mitre.html

No	Item	Description	USG Recommended Biometric Standards	Testing Provided By Other Entities
6	Template Generator	System that generates a template from a fingerprint image in accordance with NIST SP 800-76-1.	NIST SP 800-76-1 INCITS 378:2004	MINEX testing by NIST in accordance with NIST SP 800-76-1, 2007
7	Template Matcher	Software that matches a live fingerprint template with a stored template in accordance with NIST SP 800-76-1.	NIST SP 800-76-1 INCITS 378:2004	MINEX testing by NIST in accordance with NIST SP 800-76-1, 2007

7.2   FBI's Fingerprint Image Quality Certification Program

The FBI's fingerprint image quality certification program is a foundation for fingerprint scanners' image quality as required by all USG fingerprint identity management systems. The products listed are certified by the FBI as having been tested and found to be in compliance with the FBI's Integrated Automated Fingerprint Identification System (IAFIS) Image Quality Specifications. This program has been recognized and is used nationally and internationally. Table 2 provides a list of the types of products evaluated by the FBI Fingerprint Image Quality Certification Program[4] that are tested against biometric standards that are included in the USG Registry.

The testing for certification only covers basic image quality requirements listed in the applicable standards. Fingerprint segmentation, compression, file formatting, or any later fingerprint processing are not included.

Table 2 – FBI's Fingerprint Image Quality Certification Program

No	Item	Description	USG Recommended Biometric Standards	Additional Testing Provided By Other Entities
1	Live Scan Systems	Fingerprint scanners that can capture images of ten rolled fingers together with a set of plain impressions.[5]	FBI EBTS Version 8.1, Appendix F	
2	Fingerprint card scanning systems	A device that scans a fingerprint card to capture fingerprint images to create a digital record	FBI EBTS Version 8.1, Appendix F	
3	Fingerprint card printers	A printer that formats and prints a fingerprint card from a digital record using a fingerprint printing algorithm	FBI EBTS Version 8.1, Appendix F	

---

[4] For detailed listing of certified products see https://www.fbibiospecs.org/IAFIS/Default.aspx
[5] Devices collecting palmprints in addition to ten-prints or Identification flats may be certified within those categories

4	Integrated products	Integrated fingerprint capture device including the following capabilities: personal computer, hard shell shipping and carrying case, software package including image quality software, rolled and flat live scan fingerprint capture, fingerprint card capture, sequence check, security software, generation of EBTS compliant records, transmission via SMTP email, archive to CD-RW, report generation, bar code reader, signature pad, and uninterruptable power supply.	FBI EBTS Version 8.1, Appendix F ANSI/NIST-ITL 1-2007, Type 14	
5	Identification flats system	A device that captures finger plain impressions (four fingers each hand plus thumbs)	FBI EBTS Version 8.1, Appendix F	
6	PIV Single finger capture devices	Single finger scanner	PIV-071006 (Single finger version of Appendix F)	
7	Mobile ID devices	A mobile device that captures plain impressions of one or more fingers simultaneously	FBI EBTS Version 8.1, Appendix F NIST SP 500-280 PIV-071006	

7.3   TSA Airport Access Control Performance (AACP) Certification Program

TSA designated a private laboratory to conduct biometric device testing during the Initial Phase of the Biometrics for Access Control Qualified Products List. This testing resulted in the initial QPL announced September 2007. DHS has thus far evaluated and qualified one private laboratory to conduct biometric device testing during the Transition Phase currently in progress. The laboratory tests products that can be deployed at airport access points to secure areas[6]. The qualification process and the process for testing are described in a Guidance document issued by TSA[7]. Table 3 lists the types of products to be tested against biometric standards that are included in the USG Registry. It should be noted that the TSA program is open to any biometric modality, is primarily performance oriented and relies on scenario testing. Now with full implementation of the NVLAP accreditation program, testing of AACP products in the Sustaining Phase can be conducted under NVLAP auspices by laboratories accredited by NVLAP.

Table 3 includes only one standard for TSA products. The inclusion of the other standards is not appropriate for the TSA program, as proprietary solutions are acceptable for use with closed airport systems. TSA does make use of other standards, however, these are tailored or modified for TSA applications.

---

[6] For greater detail and to see products on the QPL see http://www.biometricgroup.com/QPL/
[7] To access TSA guidance package see: http://www.tsa.gov/join/business/biometric_qualification.shtm

Table 3 – TSA Airport Access Control Performance Certification Product List

No	Item	Description	USG Recommended Biometric Standards	Additional Testing Provided By Other Entities
1	Biometric Subsystem	A biometric reader capable of being integrated into an access control system. This may include an integrated ID card reader and/or PIN pad.	INCITS 383:2004	None (biometric)
2	Biometrics Enrollment Station	An enrollment station compatible with the Biometric Subsystem including biographic and biometric data acquisition and reference sample/template storage.	INCITS 383:2004	None (biometric)

7.4   TSA TWIC Product Certification Program

The TWIC Reader Hardware and Card Application Specification are currently under review. An Initial Capability Evaluation (ICE) program is in place to evaluate basic functionality of the readers. This evaluation addresses the behavior of the TWIC application requirements for both fixed and portable readers used in conjunction with the TWIC pilot test. At this time the requirements are being evaluated by an operational pilot program. A number of products have completed the ICE evaluation. DHS will implement final reader requirements upon completion of the reader evaluations[8]. The pilot test results will be used to support the second TWIC rulemaking which will establish requirements for TWIC readers. Table 4 lists the types of products to be tested[9].

Table 4 – TSA TWIC Product Certification Program Product List

No	Item	Description	USG Recommended Biometric Standards	Additional Testing Provided By Other Entities
1	Fixed Physical Access Control Reader	A TWIC reader installed in a wall, turnstile or similar type installation. It communicates with an external access control system to control a door, gate, turnstile, etc.	FBI EBTS Version 8.1, Appendix F FIPS 201-1, 2006 NIST SP 800-76-1, 2007	FBI certification of fingerprint image quality to PIV-071006
2	Portable Verification Reader	A handheld TWIC reader that may be used for portable, spot-check identity verification	FBI EBTS Version 8.1, Appendix F	PIV-071006 Fingerprint image quality certification by the FBI

---

[8] To access TSA TWIC evaluated product list see http://www.tsa.dhs.gov/assets/pdf/twic_ice_list.pdf
[9] To access TSA TWIC reader specifications see http://www.tsa.gov/assets/pdf/twic_reader_card_app_spec.pdf

No	Item	Description	USG Recommended Biometric Standards	Additional Testing Provided By Other Entities
3	Fingerprint Enrollment Station	Identification Flats fingerprint scanner	FBI EBTS Version 8.1, Appendix F	Certified by GSA FIPS 201 program

7.5 DoD Biometrics Standards Conformity Assessment Program

The DoD's Biometrics Standards Conformity Assessment Program is currently being documented and submitted for approval. Until then, the Biometrics Identity Management Agency (BIMA) test processes are in place to determine functionality, standards conformance, and integration of biometric-enabled technologies into the DoD Biometric Enterprise and to create the DoD Biometrics Approved Products List. [10] The DoD Biometrics APL provides the Biometrics Community of Interest (COI) with guidance on the selection and qualification processes for Commercial-Off-The-Shelf (COTS) and Government-Off-The-Shelf (GOTS) biometric-enabled technologies and components. The DoD BIMA employs a three-phased approach to assess COTS/GOTS for consideration into the APL. These phases include Selection, assessment in a Lab Environment, and evaluation in an operational environment. Assessment in a Lab Environment includes functionality, performance, and standards conformance, while the evaluation in an operational environment includes standards conformance over operational networks, integration with repositories of biometrics data, and the interoperability testing needed between interfaces conducted by the BIMA and Joint Interoperability Test Command (JITC). A standards conformance certification is provided by the JITC when all standards conformance criteria are met. Table 5 indicates major COTS/GOTS systems and devices tested against biometric standards included in the USG Registry.

Table 5 – DoD Biometrics Standards Conformity Assessment Program APL

No	Item	Description	USG Recommended Biometric Standards	Additional Testing Provided By Other Entities
1	- Tactical Biometric Hand-Held Terminals: - Fusion - Secure Electronic Enrollment Kit for Identification (SEEK ID) - Handheld Interagency Identification Detection Equipment (HIIDE) - Tactical Biometric Collection and	A tactical collect, store, match, and share on device capability that processes plain fingerprint impressions (of one or more fingers simultaneously), facial, and iris images	DoD EBTS v1.2, ANSI/NIST-ITL 1-2000, and ANSI/NIST-ITL 1-2007 *NOTE: Conformance of iris and facial images quality metrics is not complete and development of approved test	Interoperability and standards conformance certification provided by the Joint Interoperability Test Command; Service Operational Test Agencies.

---

[10] To access DoD Approved Products List see http://www.biometrics.dod.mil

No	Item	Description	USG Recommended Biometric Standards	Additional Testing Provided By Other Entities
	Matching System (TBCMS) - System for Intelligence and Identity Management Operations (SIIMON)		tools is on-going.	
2	DoD operational automated biometrics collection and tracking systems - Biometric Automated Toolset (BAT) - Defense Biometric Identification System (DBIDS) - Biometric Identification System for Access (BISA) - Detainee Reporting System (DRS) - Sensitive Site Exploitation (SSE) - Jump Kit Biometric Collection and Identification (BCIE)	Enrollment stations compatible with the Biometric Authoritative Datasource including biographic and biometric data acquisition and reference sample/template storage, matching, and sharing for finger, iris, palm, voice, and face modalities.	DoD EBTS v1.2, ANSI/NIST-ITL 1-2000, and ANSI/NIST-ITL 1-2007 *NOTE: Conformance of iris and facial images quality metrics is not complete and development of approved test tools is on-going.	Standards conformance certification provided by the Joint Interoperability Test Command; Service Operational Test Agencies.
3	DoD strategic authoritative repositories of biometrics data (friendly force, neutral, and adversarial) - DoD Automated Biometric Identification System (ABIS) - Identification Protection To Ensure Confident Transactions (IDProTECT) - International Security Assistance Force	DoD authoritative repositories of biometrics data (finger, face, iris, and palm modalities; emerging capabilities include voice and Deoxyribonucleic Acid)	DoD EBTS v1.2, ANSI/NIST-ITL 1-2000, and ANSI/NIST-ITL 1-2007	Interoperability and Standards conformance certification provided by the Joint Interoperability Test Command; Service Operational Test Agencies.

No	Item	Description	USG Recommended Biometric Standards	Additional Testing Provided By Other Entities
	ABIS			

7.6   NIST WSQ Testing Program

The Wavelet Scalar Quantization (WSQ) Gray-scale Fingerprint Image Compression Algorithm is the standard for the exchange of 8-bit, 500ppi fingerprint images within the criminal justice community.

A certification program has been created by the FBI which allows vendors to download a reference test set created by NIST. A certification request containing the test report, test results, and all generated compressed and reconstructed files are forwarded to the FBI for review and evaluation. This self-test procedure enables a vendor to react quickly to technology advancements and market requirements without being constrained by the FBI's limited personnel resources.

The FBI may request additional information or conduct supplemental tests to determine full compliance with the WSQ Specification. A listing of all the FBI certified WSQ implementations compliant with the WSQ Specification is maintained on the FBI web site[11].

The certification process guidelines and the test process download instructions are described on the NIST web site[12].

Table 6 – NIST WSQ Algorithm Certification Program

No	Item	Description	USG Recommended Biometric Standards	Additional Testing Provided By Other Entities
1	WSQ Compression Algorithm	An algorithm for compressing fingerprint data captured at 500 ppi that is compliant with FBI EBTS specifications.	WSQ Gray-Scale Fingerprint Image Compression Specification, IAFIS-IC-0110(V3), December 19, 1997.	

7.7   Other Certification Programs

The Registered Traveler Technical Interoperability Specification leveraged the FIPS 201 standard to specify the identify management infrastructure requirements for a fully-interoperable, vendor-neutral

---

[11]For a complete list of certified products see
http://www.fbibiospecs.org/wsq/Implementations/Default.aspx
[12] See http://fingerprint.nist.gov/wsq/

Registered Traveler program within the United States. This is not a USG sponsored certification program, however, it relies on USG sponsored product certifications processes.

8. Accreditation and Conformity Assessment Process

Figure 1 provides a generic overview of the Conformity Assessment Infrastructure and the relationship between: the validation/certification bodies, the testing laboratories, the laboratory accreditation bodies, the product developers, and the Qualified/Approved Products List (QPL/APL) owner and list. The success of the accreditation and conformity process requires that the procurement agencies, the laboratories, and the laboratory accreditation authorities have a clear understanding of the requirements and test methods and or test tools mandated by the accreditation authority. The accreditation process provides formal recognition that a laboratory is competent to carry out specific tests or calibrations or types of tests or calibrations.

Figure 1 Conformity Assessment Infrastructure

Figure 2 shows the relationships for the laboratory accreditation process. The key aspect of the process is the identification of the biometric standards, test methods, test tools, and product technical requirements by the procurement agency as they apply to the products to be tested. The laboratory accreditation process determines the laboratory's capability in conducting these tests in accordance to these requirements.
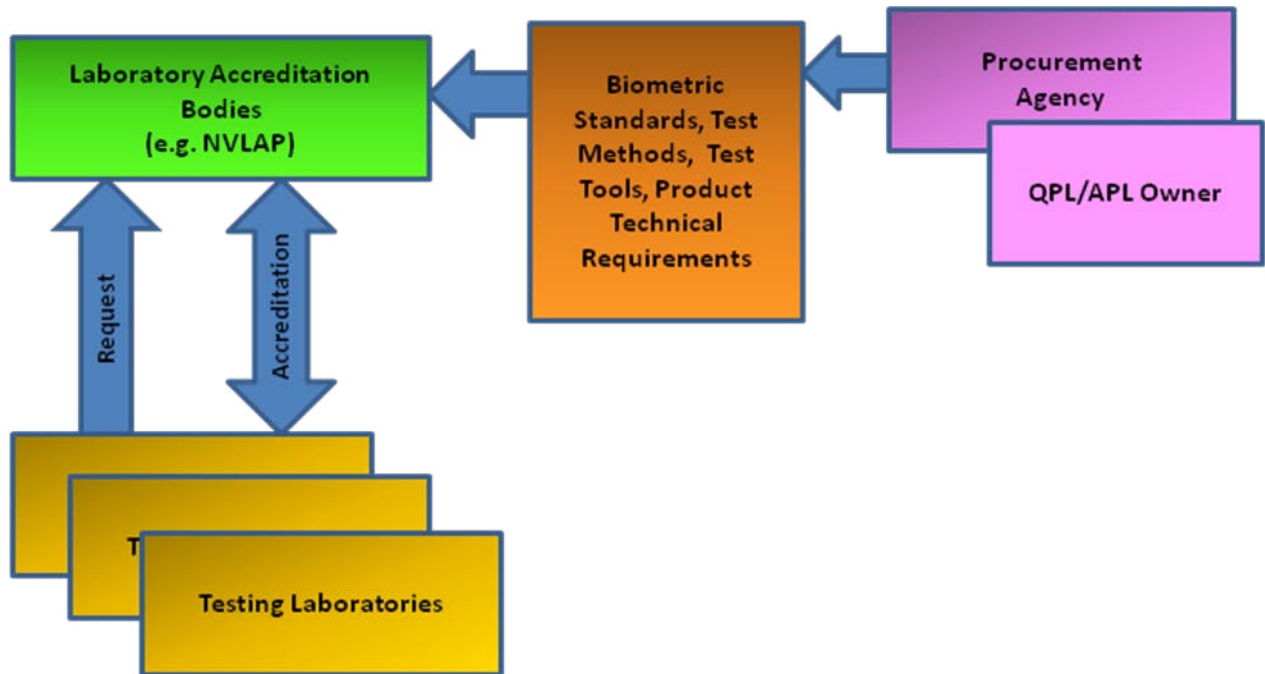
Figure 2: Accreditation Process

The conformance assessment of products is a process that includes the interaction of several organizations, a compliance testing framework, and a reporting process. It requires that an accreditation process be in place. An example of this conformance assessment process is provided in Figure 3. The assessment process starts with the submission by the vendor of the product to a third party accredited laboratory. The laboratory tests the product in accordance with the product requirements and forwards the test results to the vendor. If the results are satisfactory to the vendor, they will be passed by the laboratory to the validation authority designated by the procurement agency in coordination with the QPL/APL owner. These experts will review the test reports and will make a recommendation as to their acceptance to the QPL/APL owner. If the QPL/APL owner agrees with the recommendations, the product will be listed.
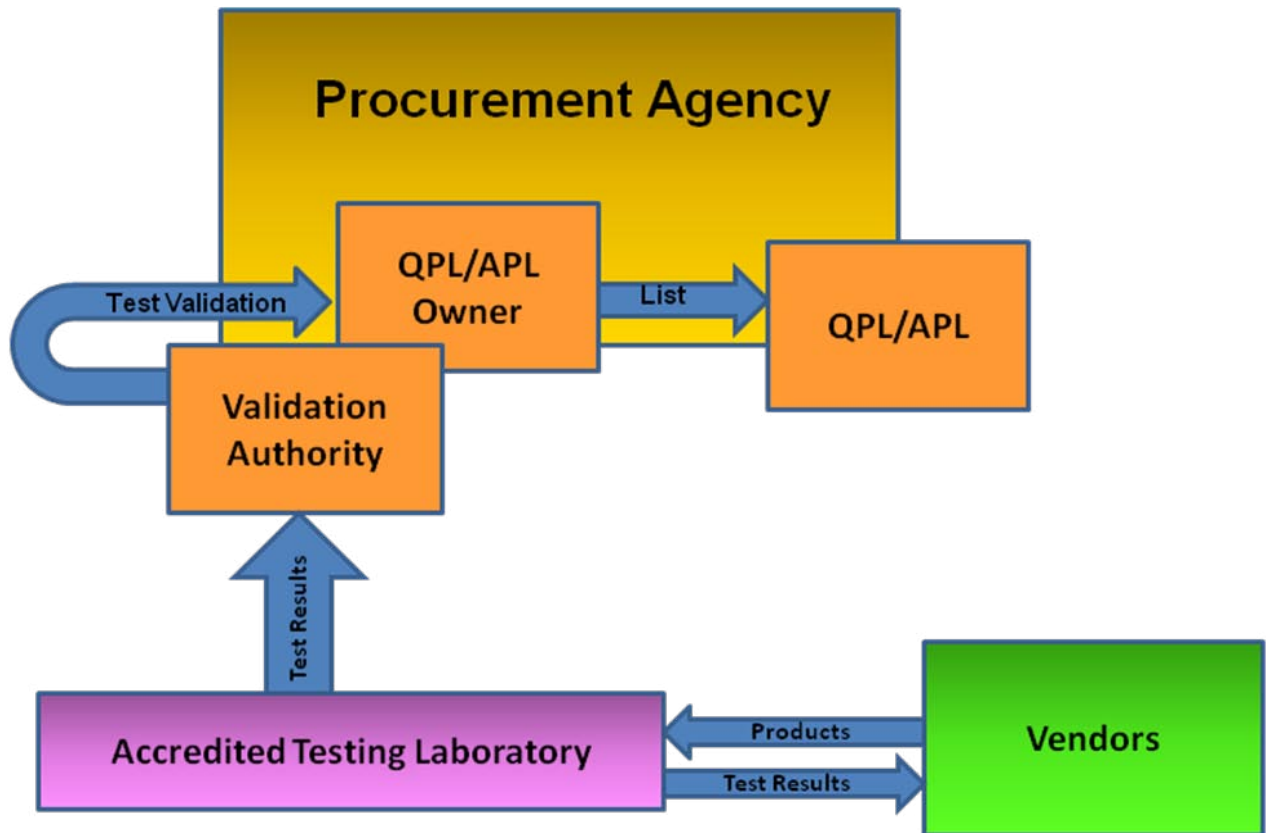
Figure 3: Assessment Process

9. References

For listing of current standards refer to the USG Registry of Biometric Standards, paragraph 13. Additional biometric standards referenced in the Catalog are provided as follows:

Table 7 Additional Standards not Included in USG Registry

1	PIV-071006	Personal Identity Verification (PIV) Image Quality Specifications for Single Finger Capture Devices, FBI Biometric Specifications, 10 July 2006, available at http://www.fbibiospecs.org/fbibiometric/docs/pivspec.pdf