GUIDANCE PACKAGE

Biometrics for Airport Access Control

Response to Section 4011(a)(5)

30 September 2005

This guidance document includes basic criteria and standards that TSA believes biometric products should meet in order to meet the technical requirements of acceptable performance for airport access control systems. These criteria and standards are based on TSA's technical expertise, in consultation with the National Institute of Standards and Technology and representatives of the aviation industry and the biometric identifier industry.   TSA will use these criteria and standards to evaluate biometric sub-systems for inclusion on the Qualified Products List (QPL). Generally, a biometric product that does not satisfy these criteria and standards will not be placed on the Qualified Products List. However, in some cases a device that does not meet all the criteria and standards may be approved for placement on the list if TSA believes its performance will be comparable to devices that meet the criteria and standards. In other cases, it is possible that a device that meets all the standards and criteria may exhibit features that TSA believes make it ineligible for placement on the QPL.

EXECUTIVE SUMMARY

BIOMETRICS FOR AIRPORT ACCESS CONTROL GUIDANCE PACKAGE

Overview

This guidance package addresses biometrics for airport access control. Access control addresses the examination of one or more of three factors regarding an individual's identity: something they know, something they have, or something they are. Biometrics is the field of technology devoted to identifying individuals using biological traits or "something they are." It uses automated methods of recognizing a person based on one or more physiological or behavioral characteristics.

On December 17, 2004, President Bush signed into law the *Intelligence Reform and Terrorism Prevention Act of 2004*. The legislative language of this act in *Title IV – Transportation Security, Section 4011 – Provision for the Use of Biometric or Other Technology*, directs TSA to "issue, not later than March 31, 2005, guidance for use of biometric technology in airport access control systems." TSA encourages airport operators to use this guidance document to improve upon their existing access control systems by incorporating biometric technologies. Such improvements are not required.

Regulations governing airport security: These are found in *Title 49, Code of Federal Regulations (CFR), Chapter XII*, in particular *Part 1542: Airport Security*. Part 1542 requires airport operators to adopt and carry out a security program approved by TSA and requires that an airport operator must, in its security program:

- Establish a secured area – Air Operations Area (AOA) and/or Security Identification Display Area (SIDA);

- Control entry into the secure area via access control systems; and

- Perform the access control functions required and procedures to control movement within the secured area, including identification media.

A majority of airports in the U.S. fall under the Part 1542 regulations and thus have some type of access control system for their secured areas. Currently, very few of these airports have access control systems with biometrics, some of which were implemented through TSA pilot programs at a limited number of access points.

Section 4011(a)(5) of the *Intelligence Reform and Terrorism Prevention Act (the "Intel Bill")* directs the Assistant Secretary of Homeland Security (TSA), in consultation with representatives of the aviation industry, biometric identifier industry, and the National Institute of Standards and Technology (NIST), to issue guidance to establish, at a minimum:

(A) comprehensive technical and operational system requirements and performance standards for the use of biometric identifier technology in airport

access control systems (including airport perimeter access control systems) to ensure that the biometric identifier systems are effective, reliable, and secure;

(B) a list of products and vendors that meet the requirements and standards set forth in subparagraph (A);

(C) procedures for implementing biometric identifier systems to ensure that individuals do not use an assumed identity to enroll in a biometric identifier system and to resolve failures to enroll, false matches, and false non-matches; and

(D) best practices for incorporating biometric identifier technology into airport access control systems in the most effective manner, including a process to best utilize existing airport access control systems, facilities, and equipment and existing data networks connecting airports."

The TSA guidance is primarily directed to two groups: (1) airport operators, who own and operate the access control systems at their airports; and (2) manufacturers of biometric devices, who need to submit their devices for qualification (including performance testing) in order to be potentially placed on a TSA biometric Qualified Products List (QPL). A major component of the TSA guidance is to provide criteria that a manufacturer of biometrics devices will be expected to meet in order to have itself and its device(s) included on the QPL. Manufacturers will find this TSA guidance crucial to understanding the technical and operational requirements that their biometric devices should meet and the standards to which they should conform. (Note that as used in this document, the term "airport operators" may also include other organizations/subcontractors designated and approve to perform access control administrative functions.)

Airport operators who choose to incorporate biometrics are encouraged to use this guidance to procure and integrate the biometric component into their legacy (i.e., existing) access control systems and to update their airport security programs. The end users of biometric access control systems are airport, air carrier and airport tenant employees, who access secure areas of airports.

TSA has generated the following Guidance Package to comply with Section 4011(a)(5) of the Intel Bill. The package is comprised of three major documents, referred to as "Volumes", each with Chapters that address key aspects of the guidance:

VOLUME 1 - REQUIREMENTS DOCUMENT
    Chapter I - Technical Requirements
    Chapter II - Operational Requirements
    Chapter III - Standards

VOLUME 2 - IMPLEMENTATION GUIDANCE DOCUMENT
    Chapter I - Identity Authentication
    Chapter II - Resolving Failures
    Chapter III - Best Practices for Implementation with Legacy Systems

VOLUME 3 - PLAN FOR BIOMETRIC QUALIFIED PRODUCTS LIST (QPL)

Chapter I - Management Plan
Chapter II - Test Plan
Chapter III - Business Model
Chapter IV - Schedule for Initial Qualified Products List (QPL)

These documents delineate what TSA requires to place products on the QPL, as well as other guidance. Each of these guidance documents is briefly described below.

Volume 1 - Requirements Document

The **Requirements Document** addresses paragraph (A) of Section 4011 of the legislation, to establish "comprehensive technical and operational system requirements and performance standards…" This document is focused on the requirements[1] for the biometric sub-system portion of the airport access control function, not on the qualification process for these biometric products.

The **Technical Requirements** chapter contains the technical specification that establishes the total metrics that a manufacturer's device must meet in order to qualify through independently conducted, scenario-based performance tests and other forms of evaluation. Technical Requirements contain quantitative qualification requirements including biometric matching error rates, failure to enroll (FTE) rates, and transaction times; reliability/availability requirements; and power/physical requirements.

The **Operational Requirements** chapter addresses the biometric sub-system from the perspective of the operations of the existing access control systems. This includes guidance on compatibility with existing credentials, new secondary/backup procedures for resolving FTE and False Reject Rate (FRR), biometric sub-system administrative burden, user enrollment requirements (e.g., protocol regarding effort level and duration), "threshold adjustments," and revocation of access privileges (biometrics do not interfere with access control capability).

The **Standards** chapter identifies and summarizes guidance regarding standards from the following organizations: NIST (National Institute of Standards and Technology), ANSI (American National Standards Institute), INCITS (International Committee for Information Technology Standards), and RTCA (formerly the Radio Technical Commission for Aeronautics). It addresses biometrics standards "conformance" issues and establishes a timetable for conformance. This information is aimed at the biometric manufacturers to advise them of standards conformance requirements, and also for the airports to use in future acquisition documents for biometric deployment.

---

[1] In this guidance document, the word "requirement" does not mean a legally-enforceable requirement. Similarly, the phrase "must meet" does not refer to a legal requirement. Rather, these terms refer to technical performance criteria that TSA has determined should characterize products listed on the QPL. Airport operators are not required to use products on the QPL.

Volume 2 - Implementation Document

The **Implementation Document** addresses paragraph (C) of Section 4011(a)(5) of the legislation, to establish "procedures for implementing biometric identifier systems to ensure that individuals do not use an assumed identity to enroll in a biometric identifier system; and to resolve failures to enroll, false matches, and false non-matches;" and paragraph (D), to establish "best practices for incorporating biometric identifier technology into airport access control systems in the most effective manner…". This document is also focused on the airport access control function, not on the qualification process for biometric products.

The **Identity Authentication** chapter provides recommended practices for breeder document authentication. The **Resolving Failures** chapter provides options for resolving enrollment failures, including discussion of false match control and other security layers, and options for resolving false reject. The **Best Practices for Implementation with Legacy Systems** chapter recommends approaches to biometric incorporation that will preserve investment in legacy access control systems.

Volume 3 - Plan for Biometric Qualified Products List (QPL)

The **Plan for Biometric QPL** addresses paragraph (B) of Section 4011(a)(5) of the Intelligence Reform and Terrorism Prevention Act, to establish "a list of products and vendors that meet the requirements and standards set forth in…paragraph (A)." These requirements are embodied in the Technical Requirements chapter of the Requirements Document (Volume 1, Chapter 1). The required Standards are addressed in the Standards chapter of the Requirements Document (Volume 1, Chapter 3). The Plan for Biometric QPL is focused on the process for qualification of the biometric sub-systems, not on the airport access control function.

The **Management Plan** (chapter 1) provides an overview of the process for TSA accreditation, defines the process for manufacturer application for qualification, and describes the required manufacturer data package for TSA review. It also addresses the Conformity Assessment Program.

The **Test Plan** (chapter 2) provides details of "what" will be tested in the regimen of performance-based scenario testing of production biometric sub-systems required for manufacturer/device qualification. It defines Core and Optional Tests, test measures and variables, test crew (e.g., crew size and demographics), and environment and outdoor conditions. It details data collection and reporting requirements.

The **Business Model** (chapter 3) establishes how testing costs will be covered for the initial QPL. It also outlines the long-term model for the continuous process needed to update the QPL.

The **Schedule for Initial Qualified Products List (QPL)** (chapter 4) provides a brief overview of the major activities planned to achieve the initial list of qualified products.

VOLUME 1: REQUIREMENTS DOCUMENT

30 September 2005

EXECUTIVE SUMMARY

BIOMETRICS FOR AIRPORT ACCESS CONTROL

VOLUME 1: REQUIREMENTS DOCUMENT

How Does the Material in the *Requirements Document* Relate to the Legislation?

On December 17, 2004, President Bush signed the *Intelligence Reform and Terrorism Prevention Act of 2004*. The legislative language of this act in *Title IV – Transportation Security, Section 4011 – Provision for the Use of Biometric or Other Technology*, directs TSA to "issue, not later than March 31, 2005, guidance for use of biometric technology in airport access control systems." As this Act requires, *Volume 1: Requirements Document* specifically addresses subparagraph (A) of Section 4011(a)(5) of the legislation to establish, at a minimum:

"comprehensive technical and operational system requirements and performance standards for the use of biometric identifier technology in airport access control systems (including airport perimeter access control systems) to ensure that the biometric identifier systems are effective, reliable, and secure."

The *Requirements Document* is focused on the biometric sub-system portion of the airport access control function, not on the qualification of the biometric devices. Its guidance is therefore directed to both the airport operators, who have interest in the Operational Requirements, and the biometric product manufacturers who have a need to understand the technical and operational system requirements needed to qualify their devices.

What is in the *Requirements Document*?

A major component of the TSA guidance is to provide criteria that airport operators need to know in order to integrate biometric devices into their access control systems, and also what a manufacturer of biometrics devices must meet in order to have itself and its device(s) listed on the QPL. Airport operators will find that they need to understand the biometric devices' technical and operational requirements and the performance standards to which they must conform to be on the list. This understanding is necessary for their operations and as well as to revise their security plans, if necessary. Manufacturers will find this TSA guidance crucial particularly to understanding the technical requirements that their biometric devices must meet in order to qualify.

The *Requirements Document* consists of 3 chapters:

> Chapter I - Technical Requirements
> Chapter II - Operational Requirements
> Chapter III - Standards

These chapters describe the total requirements for biometric device qualification and evaluation and standards conformance. Each of these Chapters is briefly described next.

The **Technical Requirements** chapter contains the technical specification that establishes the total metrics that a manufacturer's device must meet in order to qualify through independently conducted, scenario-based performance tests. Technical Requirements contain quantitative qualification requirements including biometric matching error rates, failure to enroll (FTE) rates, and transaction times; reliability/availability requirements; and power/physical requirements.

The **Operational Requirements** chapter contains issues of interest to airport operators on the interface to existing access control systems. This includes compatibility with existing credentials, secondary/backup procedures for resolving FTE and False Reject Rate (FRR), biometric subsystem administrative burden, user enrollment requirements (e.g., protocol regarding effort level and duration), "threshold adjustments," and revocation of access privileges (biometrics do not interfere with access control capability).

The **Standards** chapter identifies and summarizes guidance regarding standards from the following organizations: NIST (National Institute of Standards and Technology), ANSI (American National Standards Institute), INCITS (International Committee for Information Technology Standards), ISO (International Organization for Standardization) and RTCA (Radio Technical Commission for Aeronautics). It addresses biometrics standards "conformance" issues and establishes a long-term goal for conformance.

How Should the Reader Use the *Requirements Document*?

Airport Operators will want to consult the ***Requirements Document*** in order to know about the technical and operational requirements that a manufacturer's biometric device has had to meet in order to be listed on the Qualified Products List (QPL), and the performance standards to which the device should conform in order to be integrated successfully into an airport access control system. Airport operators may use this document to help interpret the QPL when they decide which biometric device(s) they will consider for purchase, and to help understand the costs associated with using biometric sub-systems and incorporating them into their airports.

Manufacturers need to consult the Technical Requirements chapter in order to know what they must do to achieve qualification for their devices and be included in the Qualified Products List (QPL). They will also want to understand the Operational Requirements chapter in order to understand the total requirements by which airport operators will evaluate their biometric devices. Manufacturers will also need to be aware of the standards to which their devices should conform in order to be incorporated successfully into airport access control systems.

VOLUME 1 – REQUIREMENTS DOCUMENT

CHAPTER 1

TECHNICAL REQUIREMENTS
For
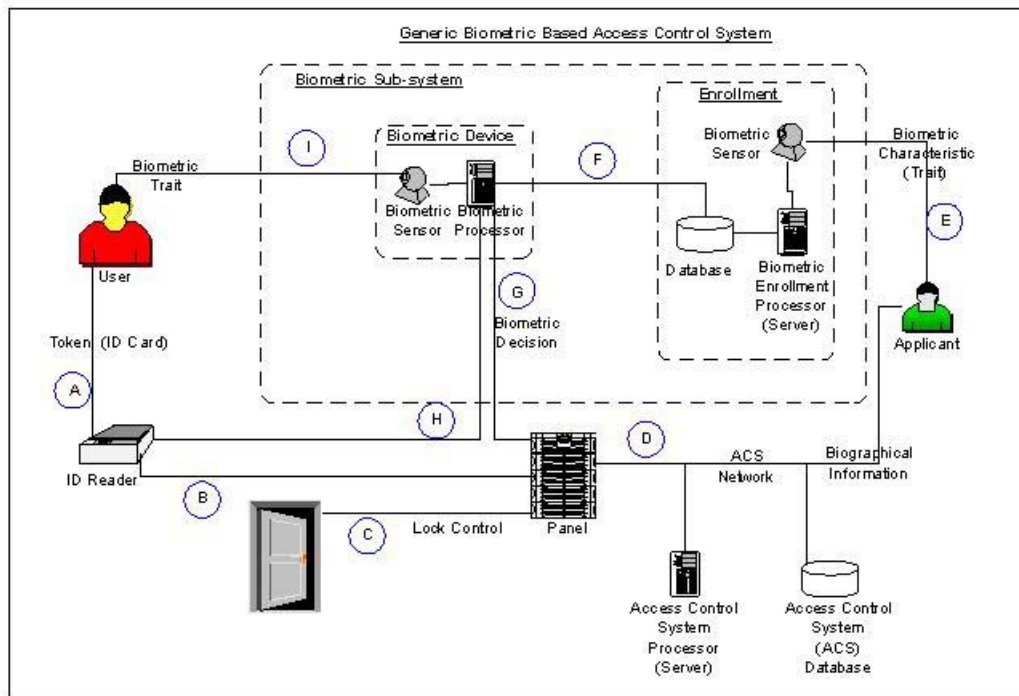## Biometric Sub-System

30 September 2005

1.0 PURPOSE

1.1 SCOPE

This document establishes requirements for a biometric sub-system and biometric device that is intended to be integrated with physical access control systems for airport employee/tenant access control. The use of the term, "shall" denotes a requirement, while the use of the term, "should" reflects a goal.

1.2 SYSTEM PERSPECTIVE

The following diagram provides a graphical view of the relationship between the airport access control system (as a whole), the biometric sub-system boundary, and the biometric device. Note that this is a generic diagram and that specific implementations may vary from this particular depiction.

KEY: A - Any form of machine-readable credential (airport ID, TWIC, proximity card) presented by the user to the ID reader to claim an identity.

B - User identity code (ID number, card number, ACS ID) read from the token by the ID reader and sent to the panel for the ACS to determine access privilege (part of typical legacy ACS).

C - Electrical signal from the panel used to command the door electromechanical locking mechanisms. This path may also include other signals such as door-open indicators, emergency lock override, etc. (part of typical legacy ACS).

D - (Physically) communication channel (Ethernet, RS485, etc.) enabling data interchange between the panel and ACS processor and database. (Logically) depends on site-specific implementation and includes user identity code from panel and user access authorization from ACS processor.

E - Body part or human behavior presented by the applicant to the biometric sensor during enrollment (e.g., fingerprint, iris, voice, signature). This function may also include interactions between applicant and sensor, i.e., indicator lights, audio cues.

F - Biometric template data from enrollment database to biometric processor for implementations using server-stored templates. (This flow is architecture-specific, may be per user transaction or periodic pre-loads.)

G - Y/N indication (electrical signal or message) from biometric processor to panel conveying the result of the user verification transaction.

H - User identity code (ID number, card number, ACS ID) read from the token by the ID reader and sent to the biometric processor as claim of identity (also includes user template data for template on card architectures).

I - Body part or human behavior presented to the biometric sensor during an access transaction (e.g., fingerprint, iris, voice, signature). This may also include interactions between applicant and sensor such as indicator lights or audio cues.

J - Applicant-supplied information (name, address, etc.) obtained during ACS enrollment via the ACS processor (part of typical legacy ACS).

1.3 CHANGES   (none)

2.0   APPLICABLE DOCUMENTS

2.1   UL 294, Standard for Safety of Access Control System Units

2.2   EN 50081-1 (1992), European Standard, "Electromagnetic Compatibility – Generic Emission Standard, Part 1: Residential, Commercial and Light Industry"

2.3   IEC 60068-2-64, "Environmental Test – Part 2: Test Methods – Test FH: Vibration Broadband Random (Digital Control) and Guidance

2.4   IEC 61000-6-1 "Electromagnetic Compatibility – Generic Immunity Standard, Part 1: Residential, Commercial and Light Industry"

2.5   IEC 61000-4-2 (Electrostatic Discharge)

2.6   IEC 61000-4-3 (Radiated RF Immunity)

2.7   IEC 61000-4-4 (Electrical Fast Transient/Burst)

2.8   IEC 61000-4-6 (Radio Frequency Common Mode)

2.9   IEC 61000-4-5 (Surges)

2.10   IEC 61000-4-8 (Power Frequency Common Mode)

2.11   IEC 61000-4-11 (Voltage Dips and Interruptions)

2.12   IEC 68-2-27 (1987), International Electrotechnical Commission, "Basic Environmental Testing Procedures, Part 2: Tests – Test Ea and Guidance: Shock"

2.13   IEC 68-2-29 (1987), International Electrotechnical Commission, "Basic Environmental Testing Procedures, Part 2: Tests- Test Eb and Guidance: Bump"

2.14   OSHA Regulation 1910.147 De-energizing Equipment

3.0   REQUIREMENTS

3.1   IDENTITY VERIFICATION FUNCTION

The basic purpose of utilizing a biometric sub-system as part of an access control system is to verify the identity of the person attempting to gain access to a secure area. There are several fundamental metrics that quantify the performance of a biometric sub-system:

- Identity matching error rates (expressed as "false accept" and "false reject" errors)
- Enrollment failures (expressed as "failure to enroll" errors)
- Time required using the biometric device (referred to as transaction time)

3.1.1 PERFORMANCE – VERIFICATION ERROR RATES

To qualify as an acceptable biometric device, testing must indicate that the device can operate at error rates at or below the levels shown in Table A-1 of Appendix A.

3.1.2 PERFORMANCE – ENROLLMENT RATES

To qualify as an acceptable biometric sub-system, testing must indicate that the sub-system can operate at failure to enroll (FTE) rates at or below the levels shown in Appendix A, Table A-2. These levels must be achieved with an enrollment effort policy as defined in the Test Plan, Section 4.9 (Volume 3, Chapter 2). After an enrollment template is generated, the immediate enrollment verification must also be successful to be determined to be a successful enrollment. Enrollment in this context refers only to the biometric data, it is not all inclusive of the background check processing requirements.

3.1.3 PERFORMANCE - TRANSACTION TIME

To qualify as an acceptable biometric device, testing must indicate that the device can process biometric device transactions with an average duration at or below the levels shown in Appendix A, Table A-3. The average total time required to process an identity verification transaction will be computed offline. The start time for the transaction will be the presentation of the claim of identity (such as card swipe, presenting smart card or bar code). The end time for the transaction is when a verification decision is reached.

3.2 OPERATIONAL AVAILABILITY

Biometric device reliability (Mean-Time-Between-Failure), maintainability (Mean-Time-To-Repair), and maintenance concept as designed should yield at least a **99.86%** operational availability rate (A_o), whereas the *cumulative* down-time per unit during operational duty hours for all maintenance should not exceed 10 duty hours annually assuming a 20-hour duty day for 365 days each year. A_o is defined as:

$$A_o = \frac{\text{Uptime}}{\text{Uptime} + \text{Downtime}} \quad \text{for any single device, any duty day}$$

Downtime is the total amount of time the unit is not available for use during the duty day. Downtime can be caused by three events:

(a) A critical failure (Any failure where the device cannot perform its mission for greater than 10 minutes and maintenance is contacted);

(b) A non-critical failure (Problem occurs and the fault condition is cleared within 10 minutes or is cleared without contacting maintenance); and

(c)   Recalibration (Following either critical or non-critical failure, time spent restoring the biometric device to operational status, including running through calibration or checkout sequence/procedure.)

3.3 POWER LOSS RECOVERY

Biometric sub-system shall possess a means of storing, retrieving and automatically recalibrating to the properly calibrated biometric sub-system configuration after disruption of power.

3.4 CONTROLS & DISPLAYS

3.4.1 OPERATOR/ADMINSTRATOR CONTROLS

Access to operator controls shall require a password or an electronically read card. Operator controls shall prohibit the unauthorized use of the enrollment sub-system to alter, delete or replace biometric enrollment data. Only a limited number of administrators should be permitted to change system parameters.

3.4.2 USER INDICATORS / DISPLAYS

3.4.2.1 POWER / DEVICE STATUS

Biometric device should clearly and continuously display power status (on and ready or out of service) to the user. Biometric device *should* possess display(s) to control user entry using standard access control symbols or indicators. Biometric device shall indicate to the user when it is running its start-up built-in test. Biometric device should provide displays to support supervisor/maintenance functions.

3.4.2.2 POWER / DEVICE STATUS (for portable devices)

Portable or hand-held biometric devices shall have a clear and continuous display of battery charge level, or low battery warning indicator to the user.

3.4.2.3 USER INTERACTION INDICATORS

Biometric device should provide an intuitive interface with the user. Interactive indicators should be clear and easily understood by the target population.

3.5 TEST FUNCTIONS

3.5.1 BUILT-IN TEST (BIT)

Biometric device shall possess a built-in test function activated during startup.

3.6 SAFETY

3.6.1 GENERAL SAFETY

Biometric device shall comply with all applicable safety requirements.

3.6.2 ELECTRICAL SAFETY

Biometric device shall comply with UL 294, Standard for Safety of Access Control System Units, or internationally recognized equivalent.

The QPL will list the biometric components of access control systems (see Volume 3 Chapter 2 clause 3.5). It is recommended that the vendor state that the addition of such

components to existing or new access control devices or enrollment system will not preclude future UL 294 certification or re-certification of that device or system.

3.6.3 ERGONOMIC SAFETY

Biometric device shall not possess: (1) sharp corners or edges that can puncture, cut, or tear the skin or clothing or otherwise cause bodily injury; (2) external wires, connectors, or cables except the power cable and data cable; or (3) loose covers and cowlings. Biometric device corners and edges should have at least a 1mm exposed radius of curvature.

3.7 PRIVACY

Biometric sub-system displays shall not allow access to images, data or templates other than to the intended processing systems associated with the biometric sub-system.

3.8 INPUT POWER

Biometric device shall permit operation using 115 VAC / 60 Hz power line with up to ± 15% voltage tolerance and up to ± 5% in frequency tolerance or 12V DC ± 10% voltage tolerance.   See Para 3.4.2.1 for power/ device status reporting. Biometric device shall be installed to securely route the power and data cables (if applicable) to protect from tampering.

3.9 PHYSICAL REQUIREMENTS

3.9.1 DEVICE DIMENSIONS

There are no specific recommendations regarding device dimensions. For practicality, the biometric device should be reasonably compact and versatile as to mounting in relation to the access point being controlled.

3.10 IMPACT RESISTANCE

3.10.1 SHOCK

Biometric device shall survive a shock event defined by IEC 68-2-27 (1987) using one half-sine pulse with a nominal peak acceleration of 5 g ($50m/s^2$) and nominal pulse duration of 30 ms with no observable change in performance. Equivalent commercial practice or analysis may be substituted.

3.10.2 BUMP

Biometric device shall survive 100 bumps defined by IEC 68-2-29 (1987) each with a nominal peak accelerating of 10 g ($100 \ m/s^2$) and nominal pulse duration of 16 ms with no observable change in performance. Equivalent commercial practice or analysis may be substituted.

3.11 ELECTROMAGNETIC / VIBRATION COMPATIBILITY

3.11.1 ELECTROMAGNETIC COMPATIBILITY

Biometric devices shall comply with the following requirements. For immunity tests the equipments shall operate normally or if operation is interrupted it shall not grant access.

- **47CFR18 and/or CISPR 11 (Emissions)**

- **IEC 61000-4-2 (Electrostatic Discharge)**

  Contact Discharge Mode at 2 kV and 4 kV
  Air Discharge Mode at 2 kV, 4 kV and 8 kV
  Assumes 8 to 10 equipment discharge test points plus coupling planes, positive and negative discharge waveform polarities.
  Performance Criteria B

- **IEC 61000-4-3 (Radiated RF Immunity)**

  10 V/meter, 80 MHz to 1 GHz,
  Four sides of EUT, 1% steps, 2.8 sec. dwell. AM Mod., 80%, 1 kHz.
  Performance Criteria A

- **IEC 61000-4-4 (Electrical Fast Transient/Burst)**

  AC and DC Power Ports at 0.5kV, 1kV and 2kV
  Signal Lines over 3 meters at 0.25 kV, 0.5kV and 1kV
  Performance Criteria B

- **IEC 61000-4-6 (Radio Frequency Common Mode)**

  10 Vrms, 150 kHz to 80 MHz,
  Power ports and signal lines over 3 meters, 1% steps, 2.8 sec. dwell.
  Performance Criteria A

- **IEC 61000-4-5 (Surges)**

  AC power port at 2kV line to earth, 1kV line to line at 0, 90 and 270 deg.
  DC Power Ports at 0.5 kV line to earth, 0.5 kV line to line
  Signal Lines over 30 meters at 1 kV line to earth
  Positive and negative polarity, 5 surges per mode of appearance.
  Performance Criteria A

- **IEC 61000-4-8 (Power Frequency Common Mode)**

  30 A/m, 50 or 60Hz
  Performance Criteria A

- **IEC 61000-4-11 (Voltage Dips and Interruptions)**

  30% reduction for 0.5 periods (10 ms), Performance

Criteria B
60% for 5 periods (100 ms), Performance Criteria C
60% for 50 periods (1 sec), Performance Criteria C
95% for 250 periods (5 sec), Performance Criteria C

3.11.1 VIBRATION IMMUNITY

Biometric device identification function (Para 3.1) shall not be degraded by low frequency vibration typical at airport terminals stemming from sources such as aircraft departure/landings, heavy foot traffic, electric carts, large HVAC systems, sub-floor bag conveyors, and outdoor truck traffic. Alternatively, Biometric device manufacturer may base compliance on IEC 60068-2-64 or equivalent commercial practice or analysis.

3.12 SPECIAL TEST MODES/TOOLS

3.12.1 TBD

APPENDIX A

The following values are the TSA required level of performance for qualification. Also note the following section (note 2) on statistical analysis that prescribes how pass/fail criteria will be analyzed.

Table A-1 – Verification Error Rate Values (for up to 3-attempt transactions)
False Accept Rate - less than 1.0%
False Reject Rate - less than 1.0%

Table A-2 – FTE Levels for Qualification
Failure to Enroll Rates – less than 3.0%

Table A-3 Verification Transaction Time Levels for Qualification
Verification Transaction Time – less than 6 seconds [1]

Notes:
1. The value for transaction time is set to allow qualification of lower throughput devices that may be suitable for some low volume airport situations. This is intentional so as to not exclude biometric devices (possibly inexpensive ones) that are slower, but fully security capable. An airport's requirement for transaction time may, in some instances, be much more demanding than this qualification level.

2. Application of Statistical Analysis for Pass/Fail Decision

Due to the variability inherent in human subject based testing, it is necessary to use statistical analysis based on confidence intervals and the variability in the measured test data to arrive at a defendable Pass/Fail decision. Otherwise, it would be possible for a device to be tested, and then re-tested, and the two qualification decision results may be opposite. To avoid this undesirable situation, the measured performance will need to be "significantly" (in the statistical sense) better than the required qualification values stated above.

The extent to which a device's test measures must be better than the qualification level is described in the equations below. This analysis uses an 80% confidence level that true device performance (not just this limited test measured performance) is below the qualification levels.

Let X_i be the number of errors by the ith individual, m_i be the number of attempts by the ith individual, (i=1,…,n) and n be the total number of individuals.

Then for an error rate, $\hat{\pi}$, to be considered significantly less than 0.01, it is necessary for the error rate to be less than 0.01 - 0.842*SE where

$$SE = \frac{\hat{\pi}(1-\hat{\pi})(1+(m_0-1)\hat{\rho})}{n\overline{m}} \ , \quad \hat{\pi} = \frac{\sum\limits_{i=1}^{n} X_i}{\sum\limits_{i=1}^{n} m_i} \ , \quad \overline{m} = \frac{1}{n}\sum\limits_{i=1}^{n} m_i$$

$$\hat{\rho} = \frac{\sum\limits_{i=1}^{n}\left\{ X_i(X_i-1) + 2\hat{\pi}(m_i-1)X_i + m_i(m_i-1)\hat{\pi} \right\}}{\sum\limits_{i=1}^{n} m_i(m_i-1)\hat{\pi}(1-\hat{\pi})} \ , \text{ and } m_0 = \overline{m} - \frac{1}{n\overline{m}}\sum\limits_{i=1}^{n}(m_i-\overline{m})^2$$

Typically, for test with the crew size and number of verification attempts defined in this test plan, the passing values for FAR and FRR should be in the range of 0.6 to 0.8%, but each device will have different statistics and each will be determined based on its own data.

APPENDIX B

VERIFICATION REQUIREMENTS for QUALIFICATION

This attachment outlines how biometric sub-system specification requirements will be verified, and defines the level, method and delivery of substantiation that are required as part the manufacturer's Certificates of Conformance.

TSA will accept two Certificate of Conformance (CoC) packages, one with the Application for Qualification Data Package (Volume 3, Chapter 1), and the second accompanying the delivery of test units. Paragraph numbers refer to this Biometric Sub-System Technical Requirements specification.

CERTIFICATE of CONFORMANCE

The 4th column in Table B-1 indicates that a Certificate of Conformance (CoC) signed by the manufacturer's Program or Test Manager is required for all requirements listed in the Biometric Sub-System specification {Section 3}. However, only one of these CoC's requires substantiation; all others can be addressed without providing substantiation in a single letter.

FINAL SUBSTANTIATION

The right most column in Table B-1 identifies three specification paragraphs requiring substantiation that must be submitted with the initial test article submission:

TABLE B-1 Verification Requirements

#	Paragraph	Requirement	Minimum Data Required for Application	Required for Qualification
1	3.1	Identity Verification Function	**CoC***	**P**
2	3.2	Operational Availability	CoC	**CoC ***
3	3.3	Power Loss Recovery	CoC	CoC **See Note (1)**
4	3.4	Controls & Displays	CoC	CoC **See Note (1)**
5	3.5	Test Functions	CoC	CoC **See Note (1)**
6	3.6	Safety	CoC	CoC **See Note (1)**
7	3.7	Privacy	CoC	**CoC***
8	3.8	Input Power	CoC	CoC
9	3.9	Physical Requirements	CoC	CoC
10	3.10	Impact Resistance	CoC	CoC
11	3.11	Electromagnetic / Vibration Compatibility	CoC	**CoC***
12	3.12	Special Test Mode	tbd	**tbd**

KEY

CoC   = manufacturer certification of conformance (substantiation <u>not</u> required)
CoC *   = manufacturer certification of conformance (substantiation required)
P   = passing score in a Government Qualification Test

CoC is a formal manufacturer claim that a method, such as test, demonstration, inspection, analysis, or simulation was used to verify compliance to the specified requirement (substantiation is <u>not</u> required). However, those denoted as CoC * require substantiation.

Note (1)   biometric sub-system manufacturer is required to demonstrate this function to the Government test team (no substantiation required).

VOLUME 1 – REQUIREMENTS DOCUMENT

CHAPTER 2

OPERATIONAL SYSTEM REQUIREMENTS

30 September 2005

1.0 PURPOSE

1.1. BACKGROUND

PL 108-458, Section 4011(a)(5) directs TSA to develop guidance for the use of biometric technologies in airports, including operational system requirements for the use of biometrics in airport access control systems (including airport perimeter access control systems) to ensure that the biometric systems are effective, reliable, and secure. Technical system requirements and performance standards are addressed separately.

1.2 SCOPE

The intent of this Operational Requirements guidance is to assist airport operators to ensure that biometric sub-systems they are evaluating for their airports will work well in normal airport operating conditions. Biometric sub-system effectiveness will be contingent upon an understanding of and responsiveness to the operational needs of TSA-regulated U.S. airports. The following presents several significant operational issues that airport operators should consider.

2.0 OPERATIONAL REQUIREMENTS

2.1 SUB-SYSTEM CAPABILITIES

2.1.1 MAINTAINABILITY OF BIOMETRIC SUB-SYSTEM
Normal maintenance options for biometric product selection should be considered to ensure current and future operational needs are addressed.
1) Firmware / Software / Hardware upgrade accessibility.
2) Adequacy of operational documentation.
3) Adequacy of training material & availability.
4) Repair procedures.
5) Warranty issues. Airport Access Control Sections would be well advised to seek manufacturer/vendor warranties addressing the coverage needs addressing the wear and tear specifically associated with airport environments.

2.1.2 BACKUP PROCEDURES FOR RESOLVING FTE, FRR
1) The Biometric Sub-system documentation provided by the manufacturer or vendor should identify the most common causes for Failure to Enroll by their product, as well as recommendations for procedures to reduce or mitigate the impact of enrollment failures.
2) The Biometric Sub-system documentation provided by the manufacturer or vendor should also identify the most likely causes for False Rejections by their system and provide guidance for reducing or mitigating the impact of the most common causes of False Rejections.
(Note – See Volume 2, Chapter 2 for related information on methods for resolving errors)

2.1.3 BIOMETRIC SUB-SYSTEM ADMINISTRATIVE BURDEN

1) The Biometric Sub-system supplier should provide accurate documentation outlining the nature and frequency of staffing support that will be required to allow the Airport Operator to make informed choices.

2) Data Base Maintenance needs of the Biometric Sub-system should be clearly identified and described. The effort and frequency required for updating and maintaining Biometric Sub-system databases should be considered in the acquisition and selection process.

2.1.4 ADJUSTABLE SECURITY LEVELS BASED ON THREAT

Any Biometric Sub-system selected should support the need to rapidly (and possibly centrally) adjust matching thresholds when necessitated by changes in DHS or local threat levels.

2.1.5 SUB-SYSTEM METRICS

A user-friendly capability to support centrally generated reports is a highly desirable trait in Biometric Sub-systems and will allow Airport Access Control Sections to validate and quantify the security benefits of the system. Report options and instructions should be included in system documentation. These reports, for example, should be used to identify airport users with frequent "false reject" statistics, as they are prime candidates for re-enrollment.

2.1.6 SYSTEM TESTING/AUDITS

To verify that minimum established performance requirements (see Technical Requirements, Volume 1, Chapter 1) are met, the selected biometric sub-system should be capable of convenient system testing by Airport administrators and TSA inspectors. Results of such testing should be available in either electronic or hard copy format and identify access level, time, and location of testing. Examples of such tests are long term sensor performance degradation and sustained intrusion resistance. These tests would be performed by an airport "test crew" of subjects used repeatedly over time, with careful record keeping, to discover trends over time of sensor performance (exhibited as a quality score change or shift in matching performance) or changes in false accepts (crew acting as imposters).

2.1.7 SYSTEM FAILURES

Biometric sub-systems should be designed and installed in a manner that will allow for the independent operation of the legacy access control system, in case of failure of the biometric sub-system, until the sub-system problem is resolved. A user message or indication should be generated at each affected location so that valid users are not unnecessarily diverted to other locations to enter or exit. The Airport Access Control Section or their designee should be immediately notified of system failures by location. System reports on failures should be immediately available to Airport Database Administrators.

2.2 SUB-SYSTEM INTEGRATION

2.2.1 INTERFACE TO EXISTING ACCESS CONTROL SYSTEMS
1) Devices must be easily integrated into legacy access control system infrastructure and architecture.
2) Devices should comply with all applicable legal requirements, including Americans with Disabilities Act (ADA) requirements.
3) Biometric devices, when not integrated into existing readers, should be placed in close proximity to (e.g. in tandem with) legacy Access Control readers to avoid inconvenience to users. (This may also facilitate the use of existing facility cabling infrastructure.)
4) Biometric devices should occupy as small a footprint as possible and feature a user-friendly size interface.
5) Biometric devices should feature durable and intuitive user interface methods to promote user acceptance and compliance.

2.2.2 COMPATIBILITY WITH EXISTING ACCESS CONTROL CREDENTIALS
1) Biometric sub-systems that offer maximum flexibility in acceptance of (or compatibility with) existing access control credentials will minimize burdens associated with re-badging the user population.
2) As the Access Control Section will already have an established user database for the legacy access control system, those biometric sub-systems flexible enough to allow for importation or exportation of data will minimize unnecessary duplication of effort. The capability of a Biometric Sub-system enrollment process to accept commonly used database formats is likely to be a significant factor to the Access Control Section.

2.2.3   BIOMETRIC SUB-SYSTEM ROLLOUT
The installation and implementation of Biometric Sub-systems at smaller airports is not likely to present a significant challenge. At larger airports, however, a rollout may need to be implemented in different stages depending on the user enrollment schedule. The Biometric Sub-system should provide secure options for phasing in users. Rollout needs should be analyzed to prevent negative impacts on normal operations. For example, in a large airport it might be advisable to plan a rollout by geographical sectors.

2.2.4   USER ENROLLMENT REQUIREMENTS
1) Effort: Initial enrollment of system users should be capable of being achieved in manageable phases to prevent undue burdens on Airport Access Control Sections. Sub-system features should include, at a minimum, the ability to assess the quality of the user biometrics at the time of enrollment and solicit additional samples when needed.
2) Staffing: Manufacturers or vendors should provide information from which the airport operator can determine whether use of the system will necessitate the hiring of additional staff by the Airport Access Control Department. User enrollment processes should be flexible enough to allow for decentralized collection of user data

if the Airport Access Control Section chooses to allow selected tenants (e.g. air carriers or other large tenant organizations with appropriate space and support elements) to undertake enrollment for their respective organizations.

3) Portable Support: In many cases, Airport Access Control Sections will face the challenge of implementing a timely and efficient enrollment of a large existing population of users already cleared for the Airport's legacy access control system. In large complex airports, the user population is spread out by location and schedule. Since initial enrollment will present the greatest challenge, Airport Access Control Sections would be well advised to seek out an enrollment system that is portable and can be deployed to locations of large airport tenant populations and administered by approved tenant staff.   Note that special attention must be paid to information privacy in portable or distributed enrollment situations.

4) Duration: A Schedule describing the user enrollment Plan of Operation, and training requirements should be developed by the integration team to provide the Airport Access Control Section the information they will need to develop an estimate of the time need to conduct the enrollment process.

5) Storage Format: Enrollment data should (at a minimum) be stored in image form. This will mitigate the impact of any potential re-enrollment in another biometric of the same modality. (See Volume 1 Chapter 3 for applicable standards).

2.2.5   USER TRAINING
Training in the use of the Biometric Sub-system plays an integral role in maximizing the security benefits and user acceptance of the technology.

1) Airport employees represent a very broad range of educational levels, and user training should not require excessive amounts of instruction.

2) Stand-alone training (e.g., CBT, video, DVD) that can be administered by tenant trainers authorized by the Airport Access Control Section (e.g., air carrier, ground handlers, LEOs, Fire Department) will prevent unusual training burdens on the Airport Operator. Training material containing sensitive security information as defined by TSR Parts 15 and1520 should be protected and handled accordingly.

3) A training package that incorporates a knowledge test and the capability to record training results (that can be imported to the Airport's training record database) will relieve the Airport Access Control Section of unnecessary administrative burden.

2.2.6   EMERGENCY PERSONNEL AND EQUIPMENT ACCESS
Like the existing legacy access control system, the Biometrically enabled access control systems should allow for unimpeded access of Emergency Personnel and their equipment under conditions described in the Airport Security and Emergency Programs.

2.2.7   THROUGHPUT LEVELS
User acceptance of biometric device additions to existing access control systems will be strongly affected by the relative perceived benefits or disadvantages it places on their ability to arrive to or exit from their work place on time.

1) Desired throughput rates at access control points will vary based on location and time. Work shift start and end times place the greatest demands on any access control system. The addition of a biometric device to the legacy access control system

should not result in a significant decrease in throughput rates. Projected throughput rates associated with the biometric device should be made available by the manufacturer/vendor to the Airport Access Control Section.

2) Like the legacy access control system it supports, the biometric device should be able to accommodate unusually high levels of throughput when necessary (e.g., emergency evacuations.)

3) When considering throughput options, it should be recognized that if device settings are adjusted to meet increased threat levels, there might be consequential increases in processing times and decreases in throughput rates.

2.2.8   REVOCATION OR ADJUSTMENT OF ACCESS PRIVILEGES

Any Biometric Sub-system should have the capability to support Airport Access Control Section's ability to immediately and centrally revoke or adjust access privileges as well as to support verification of such changes in an electronic or hard copy report. In no way should the biometric sub-system prevent or override the revocation action of the access control system.

2.2.9   TECHNICAL COMPATIBILITY WITH TWIC

This guidance package is directed to the use of biometrics in local access control environments and not necessarily issuance of a secure credential (i.e., TWIC); however, the ability to use a secure credential within an airport access control system is desirable. TWIC is a biometrically-enabled high-assurance identity credential that is being tested in a Prototype Phase at 26 facilities in the US. The TWIC conforms to the latest technical standards and federal guidelines related to the use of biometrics and secure (integrated circuit chip (ICC)-based) credentials. If desired, technical compatibility with TWIC in an airport Physical Access Control System (PACS) may be achieved by conforming to the Technical Implementation Guidance for Smart Card Enabled Physical Access Control Systems, v2.2 (see http://smart.gov), which is the standard TSA is sending within this guidance for airport access controls..

Additionally, strong consideration should be given to recently published Federal Information Processing Standard (FIPS) 201 (see: http://csrc.nist.gov/plv-project/) and associated Special Publications such as SP 800-73. SP 800-73 includes provisions for issuer-controlled biometrics for operational use in the local access control environment. TWIC currently supports multiple biometric modalities for operational use. For minutiae-based biometric templates, biometric standard ANSI/INCITS 378 is used, which is the standard TSA is sending within this guidance.

2.2.10 AUTHENTICATION OPTIONS

The Biometric Sub-system should offer flexible options for authentication to meet the needs of each airport. In some situations, a complete ACS design including biometric authentication may require creative authentication approaches.

1) Single Point Authentication & Badge activation: An access control system in which the user authenticates at a single point, upon positive match system activates, RFID or other technology, badge for predetermined time period, i.e., regular working hours. System allows access to restricted areas to authorized personnel without additional

authentication. System automatically deactivates access privileges when user leaves approved area(s). User must re-authenticate prior to regaining access privileges at same point of entry. The authentication kiosk could be manned for back-up authentication. This option would work well in low-security areas and facilities with low-user populations and allowing access for emergency personnel.

2) Multi-Point Authentication & Badge activation – Same system as described above but with two or more integrated authentication kiosks.

3) Full Coverage - All Points Authentication – every access point requires biometric authentication prior to granting access. This system would work well in High-security areas, areas and facilities with low user populations and low number of access points.

VOLUME 1 – REQUIREMENTS DOCUMENT

CHAPTER 3

REQUIRED STANDARDS
For
Biometric Sub-System

30 September 2005

1   Overview of Standards

1.1 Introduction

The near-term and long-term solution for the deployment of biometric devices for access control in US domestic airports relies on the use of approved or stable standards. Within the US, standards are developed and recognized by the American National Standards Institute (ANSI), by the National Institute for Standards and Technology (NIST) within the US Government, and by the RTCA (for airports). It is the customary practice of ANSI to adopt International Organization for Standardization (ISO) standards as direct replacements for corresponding ANSI standards when such standards are approved by ISO (usually one to two years after approval of the US standard due to the International nature of ISO standards). This section will describe the current ANSI standards as developed by the International Committee for IT Standards (INCITS), and where equivalent current ISO standards or projects exist, it will be noted. It will also discuss current relevant NIST and RTCA standards. As new standards evolve, it can be expected that this guidance will be updated to take into consideration the new standards.

1.2 Distinction between Requirements and Standards

Requirements are stated by the purchaser of the system, during the procurement process, or by regulation. Standards are developed by Standards bodies, by government agency, or by private sector consortium. The normal development process includes one (or more) public review(s) and the use of ANSI/ISO approved due process rules (including advanced meeting announcements, agendas, and publication of meeting minutes). Participation in the standards development process by vendors is voluntary.

1.3 Standards Development Organizations

1.3.1   ISO

In the field of information technology, ISO and IEC have established a Joint Technical Committee 1: ISO/IEC JTC 1 on Information Technology. In June 2002, JTC 1 established a new Subcommittee 37 on Biometrics. The goal of this new JTC 1 SC is to ensure a high priority, focused, and comprehensive approach worldwide for the rapid development and approval of formal international biometric standards. These standards are necessary to support the rapid deployment of significantly better, open systems standard-based security solutions for purposes such as homeland defense and the prevention of ID theft.

Within ISO, a common naming convention exists for standards under development. Each has an approximate time frame associated with it in terms of the time it takes to get to the next stage. They are identified as follows:

> NP – New Project Proposal (3 months for project approval)
> WD – Working Draft (12 months to 18 months for approval)

CD – Committee Draft (6 months to 12 months for approval)
FCD – Final Committee Draft (6 months to 12 months for approval)
FDIS – Final Draft International Standard (6 months for approval)

1.3.2   INCITS

The Executive Board of INCITS established Technical Committee M1, Biometrics, in November 2001 to ensure a high priority, focused, and comprehensive approach in the United States for the rapid development and approval of formal national and international generic biometric standards. The M1 program of work includes biometric standards for data interchange formats, common file formats, application program interfaces, profiles, and performance testing and reporting. The goal of M1's work is to accelerate the deployment of significantly better, standards-based security solutions for purposes, such as, homeland defense and the prevention of identity theft as well as other government and commercial applications based on biometric personal authentication. Other organizations, such as the Biometric Consortium, participate indirectly in the work of M1.

M1 serves as the U.S. Technical Advisory Group (U.S. TAG) for the international organization ISO/IEC JTC 1/SC 37 on Biometrics, which was established in June 2002. As the U.S. TAG to SC 37, M1 is responsible for establishing U.S. positions and contributions to SC 37, as well as representing the U.S. at SC 37 meetings.

Projects are initiated within INCITS by the submission of a Project Proposal by one or more committee members. Approval of the project can be accomplished at the next meeting of the committee, with subsequent approval by the parent committee (INCITS Executive Board). Approval is automatic unless a member of the Executive Board perceives a contradiction with an existing project or standard.

A working draft standard is progressed on a technical level by contributions from members until such time as the committee determines by vote that the technical work is substantially complete. At that time, The INCITS staff will initiate a 45-day public review to ensure that all interested parties (whether members of the committee or not) have an opportunity to review and comment on the proposed standard. During this time, ANSI editorial staff will perform an initial editorial oversight of the standard and recommend changes as required to comply with ANSI editing rules. If substantial editorial or technical changes are required as a result of comments received in public review, a second public review after committee review and approval of proposed changes will occur. This second (and subsequent if required) public review is 45 days in length. After final review and approval by the originating committee, the draft standard is submitted to the INCITS executive Board for final approval after ensuring that all rules of due process have been followed. After Board approval, the final standard is submitted to ANSI for approval of the Board of Standards Review and publication. This final approval cycle is completed within two weeks.

From start to finish, depending on the maturity of the initial working draft document, the time required to complete a standard is from 1.5 years to 2.5 years. A Fast Track process has been instituted within INCITS that can reduce this process time to 6-months if the original working draft is substantially complete prior to submission. The Executive Board approves this process on an individual basis.

1.3.3   NIST

Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.

1.3.4   RTCA

RTCA, Inc. is a private, not-for-profit corporation that develops consensus-based recommendations regarding communications, navigation, surveillance, and air traffic management (CNS/ATM) system issues. RTCA functions as a Federal Advisory Committee. Its recommendations are used by the Federal Aviation Administration (FAA) as the basis for policy, program, and regulatory decisions and by the private sector as the basis for development, investment and other business decisions.

Organized in 1935 as the Radio Technical Commission for Aeronautics, RTCA today includes roughly 300 government, industry and academic organizations from the United States and around the world. Member organizations represent all facets of the aviation community, including government organizations, airlines, airspace user and airport associations, labor unions, plus aviation service and equipment suppliers.

1.4 Summary of Required Standards

It is recognized that Biometrics represents a component of an access control system. Other components include data base management, communications, encryption, security management, and specific application requirements. This document does not address these additional components, but recommends that where either national or international standards exist that address these elements, they be considered by the purchasing agency as a part of the overriding requirements to be met by the selected vendor.

1.4.1   Table of Required Standards

While use of biometrics is not mandatory, airports will be able to use TSA's QPL for selecting systems and can be assured that the QPL systems meet TSA established standards. The following table summarizes TSA's requirements for the use of standards in the qualification of biometric sub-systems for use in airport access control. The table is organized by the "Category" of standard, then a brief title for the standard. The Reference number (Ref) points to the paragraph in section 2 of this chapter where a

summary of the standard is found. The Required column (Reqd) indicates TSA's position on the required use of this standard, and the Status column provides the development status (as of March 2005) for each standard. The last two columns indicate TSA's expectation for the manner of determining Conformance to these standards for the "initial" QPL and the longer term "goal" or end state to be achieved in the years ahead.

Category	Standard	Ref	Reqd	Status	Conformance (initial)	Conformance (goal)
Interface	BioAPI*	2.1.1	Y	Published	Vendor Claim (4.2)	Test – third party
	CBEFF	2.1.2	Y	Published	Vendor Claim (4.2)	Test – third party
Data Formats	FP Pattern	2.2.1	IA	Published	Vendor Claim (4.1)	Test – third party
	FP Minutiae	2.2.2	IA	Published	Vendor Claim (4.1)	Test – third party (2.4.2)
	Iris	2.2.3	IA	Published	Vendor Claim (4.1)	Test – third party
	FP Image	2.2.4	IA	Published	Vendor Claim (4.1)	Test – third party (2.4.3)
	Face	2.2.5	IA	Published	Vendor Claim (4.1)	Test – third party
	Sign/Signature	2.2.6	IA	Development (2006)	Vendor Claim (4.1)	Test – third party
	Hand geometry	2.2.7	IA	Published	Vendor Claim (4.1)	Test – third party
Profile	Transportation Workers	2.3.1	Y	Published	Vendor Claim (4.2)	Test – third party

IA – If Applicable to vendor's device
* Note:
BioAPI is not optimum for a micro-controller environment such as (embedded) within a door reader unit. It is more suitable when there is a general-purpose computer available. The framework has been ported to Win32, Linux, Unix, and WinCE.
There are places within a PACS environment where it would be applicable such as enrollment. Another is if any part of the operation is done outside the door reader itself (e.g., server based matching). Also, some door readers do contain a more general-purpose processor or an auxiliary processor. In that event, BioAPI is applicable. A long-term solution to this is under development within ISO, known as "BioAPI Lite".

1.4.3 Test Facility Related Standards

Category	Standard	Ref	Reqd	Status (expected)	Conformance (initial)	Conformance (goal)
Performance Measurement and Reporting	Framework (ISO 19795 Part 1)	2.5.1	Y	Review (2005)	TSA Inspection	NIST Lab Accreditation

	Scenario Testing (ISO CD 19795-2)	2.5.5	Y	Review (2006)	TSA Inspection	NIST Lab Accreditation
	Access Control Device (ISO NP 19795-5	3.5.3	Y	Pre-Review (2006)	TSA Inspection	NIST Lab Accreditation

1.4.4 Airport Implementation Related Standards

Category	Standard	Ref	Reqd	Status (expected)	Conformance (initial)	Conformance (goal)
Access Control	RTCA DO230a	2.7.1	Y	Published	Airport Inspection	Airport Test

2.   ANSI/INCITS M1 Standards – NIST Standards – RTCA Standards

The following sections list the national biometric standards that will be required by TSA to meet the TSA QPL requirements, and when available, the equivalent ISO/IEC JTC 1 SC 37 draft standard number is be included (in parenthesis after the title).

2.1   Interface Standards

2.1.1   ANSI INCITS 358-2002, BioAPI Specification (ISO/IEC FCD 19784-1)

The BioAPI is intended to provide a high-level generic biometric authentication model; one suited for any form of biometric technology.

It covers the basic functions of Enrollment, Verification, and Identification, and includes a database interface to allow a biometric service provider (BSP) to manage the Identification population for optimum performance.

It also provides primitives that allow the application to manage the capture of samples on a client, and the Enrollment, Verification, and Identification on a server.

Status: Published

 Note:

   BioAPI is not optimum for a micro-controller environment such as (embedded) within a door reader unit. It is more suitable when there is a general-purpose computer available. The framework has been ported to Win32, Linux, Unix, and WinCE.

   There are places within a PACS environment where it would be applicable such as enrollment. Another is if any part of the operation is done outside the door reader itself (e.g., server based matching). Also,

some door readers do contain a more general-purpose processor or an auxiliary processor. In that event, BioAPI is applicable. A long-term solution to this is under development within ISO, known as "BioAPI Lite".

2.1.2   NISTIR 6529-A, CBEFF (ISO/IEC FCD 19785-1)

The Common Biometric Exchange Formats Framework (CBEFF) describes a set of data elements necessary to support biometric technologies in a common way. These data can be placed in a single file used to exchange biometric information between different system components or between systems. The result promotes interoperability of biometric-based application programs and systems developed by different vendors by allowing biometric data interchange. This specification is a revised (and augmented) version of the original CBEFF, the Common Biometric Exchange File Format, originally published as NISTIR 6529.

Status: Published*

* NISTIR 6529-A has been published as INCITS 398 March 2005. The contents are the same as NISTIR 6529-A.

2.2   Data Format Standards

2.2.1   INCITS 377-2004 – Finger Pattern Based Interchange Format (ISO/IEC FCD 19794-3)

This ANSI/INCITS Standard specifies the interchange format for the exchange of pattern-based fingerprint recognition data. This standard specifies an interchange format for the exchange of pattern-based fingerprint recognition data. It describes the conversion of a raw fingerprint image to a cropped and down-sampled finger pattern followed by the cellular representation of the finger pattern image to create the finger-pattern interchange data.

Status: Published

2.2.1   INCITS 378-2004 – Finger Minutiae Format for Data Interchange (ISO/IEC FCD 19794-2)

This Standard specifies a concept and data format for representation of fingerprints using the fundamental notion of minutiae. The data format is generic, in that it may be applied and used in a wide range of application areas where automated fingerprint recognition is involved. No application-specific requirements or features are addressed in this standard. The Standard contains definitions of relevant terms, a description of where minutiae should be defined, a data format for containing the data, and conformance information.

Status: Published

2.2.3 INCITS 379-2004 – Iris Interchange Format (ISO/IEC FCD 19794-6)

This Standard specifies two alternative image interchange formats for biometric authentication systems that utilize iris recognition. The first is based on a rectilinear image storage format that may be a raw, uncompressed array of intensity values or a compressed format such as that specified by the JPEG standard. Images may be monochrome or color with 256 or more intensity levels (gray or per-color), and vary in size depending on field of view and compression. Typical size is 25 –30 Kbytes for JPEG format.

The second format is based on a polar image specification that requires certain pre-processing and image segmentation steps, but produces a much more compact data structure that contains only iris information. The record size can be as small as 2 Kbytes. The polar image may be either raw or compressed format. Data that comply with either one of the iris image formats specified in this standard are intended to be embedded in a CBEFF-compliant structure in the CBEFF Biometric Data Block (BDB).

Status: Published

2.2.4 INCITS 381-2004 – Finger Image Based Interchange Format (ISO/IEC FCD 19794-4)

This standard specifies a data record interchange format for storing, recording, and transmitting the information from one or more finger or palm image areas within a CBEFF data structure. This standard could be used for the exchange and comparison of finger image data. It defines the content, format, and units of measurement for the exchange of finger image data that may be used in the verification or identification process of a subject. The information consists of a variety of mandatory and optional items, including scanning parameters, compressed or uncompressed images and vendor-specific information. This information is intended for interchange among organizations that rely on automated devices and systems for identification or verification purposes based on the information from finger image areas. Information compiled and formatted in accordance with this standard can be recorded on machine-readable media or may be transmitted by data communication facilities.

Status: Published

2.2.5 INCITS 385-2004 – Face Recognition Format for Data Interchange (ISO/IEC FCD 19794-5)

This biometric data interchange format specification accommodates:
1) Detailed human examination of facial images
2) Human verification of identity by comparison of persons against facial images
3) Computer automated identification (one-to-many searches)

4) Computer automated verification (one-to-one searches)

This standard specifies the record format. The cryptographic protection of the biometrical data structures defined in this document is out of scope.

Status: Published

2.2.6   INCITS 395-2005 – Signature/Sign Image Based Interchange Format (ISO/IEC WD 19794-7)

This Standard specifies a concept and data interchange format for representation of digitized sign or signature data, including time-series-based X, Y coordinate data and, optionally, data representing pressure and pen angle, for the purposes of biometric enrolment, verification or identification. The data interchange format is "generic", in that it may be applied and used in a wide range of application areas where electronic signs or signatures are involved. No application-specific requirements or features are addressed in this standard. The Standard contains definitions of relevant terms, a description of what other data are captured, a data format for containing and exchanging the data and, in an Informative Annex, examples of these data records, a description of best practices and a method of achieving a basic level of Interoperable Matching. Also included in the Standard are a definition of Common Feature Data and a definition of Raw Signature/Sign Sample Data. It should be noted that systems that support only one of these Data definitions might not be interoperable with systems that support only the other.

Status: Published

2.2.7   INCITS 396-2004 – Hand Geometry Interchange Format (ISO/IEC WD 19794-10)

This standard specifies a data record interchange format for storing, recording, and transmitting the information from a hand silhouette within a CBEFF data structure. This standard could be used for the exchange and comparison of hand geometry data. It defines the content, format, and units of measurement for the exchange of hand silhouette data that may be used in the verification or identification process of a subject. The information consists of a variety of mandatory and optional items, including data capture parameters, standardized hand position, and vendor-specific information. This information is intended for interchange among organizations that rely on automated devices and systems for identification or verification purposes based on the information from hand geometry. Information compiled and formatted in accordance with this standard can be recorded on machine-readable media or may be transmitted by data communication facilities.

Status: Published

Separate from the standards above, the reader may be interested in reviewing the following standards applicable to government issued biometric cards.

2.2.8 NIST Special Publication 800-73 Interfaces for Personal Identity Verification (see http://csrc.nist.gov/piv-project/index.html)

FIPS 201 defines procedures for the PIV lifecycle activities including identity proofing, registration, PIV Card issuance, and PIV Card usage. FIPS also specifies that the identity credentials must be stored on a smart card. SP 800-73 contains technical specifications to interface with the smart card to retrieve and use the identity credentials. These specifications reflect the design goals of interoperability and PIV Card functions. The goals are addressed by specifying PIV data model, communication interface, and application programming interface. Moreover, this specification enumerates requirements where the standards include options and branches. This document goes further by constraining implementers' interpretation of the standards. Such restrictions are designed to ease implementation, facilitate interoperability, and ensure performance, in a manner tailored for PIV applications.

Special consideration should be given to credential numbering schemes as specified in the Card Holder Unique ID (CHUID).

Status: Published

2.2.9 NIST Special Publication 800-76 Biometric Data Specification for Personal Identity Verification (see http://csrc.nist.gov/piv-project/index.html)

This document specifies technical acquisition and formatting requirements for the biometric credentials of the PIV system and is a companion document to FIPS 201. It enumerates required procedures and formats for fingerprints and facial images by restricting values and practices included generically in published biometric standards. The primary design objective behind these particular specifications is universal interoperability. Specifically, SP 800-76 involves the preparation of biometric data suitable for transmission to the Federal Bureau of Investigation (FBI) for background checks. It also provides requirements for formatting of the biometric data on the PIV card.

Status: Draft as of 09/2005

2.2.10 U.S. General Services Administration Federal Identity Management Handbook (see http://www.cio.gov/ficc)

For the Federal government to fully realize the benefits of electronic government, a ubiquitous and consistent method of providing identity credentials is necessary for both electronic security (logical access) and building security (physical access) within the Federal sector. This handbook is offered as guidance for government agency credentialing managers, their leadership, and other stakeholders as they pursue compliance with HSPD-12 and FIPS 201. The handbook provides specific implementation direction on course of action, schedule requirements, acquisition planning, migration planning, lessons learned, and case studies.

Status: Draft as of 09/2005

2.2.11 Technical Implementation Guidance for Smart Card enabled Physical Access Control Systems 2.2 (see http://smart.gov.)

Government agencies in the United States have been making significant strides in the area of secure credentialing for personnel, contractors, and visitors. These efforts are increasing the security of facilities, property, data, and most importantly people. The TIG SCEPACS v2.2 provides for:

- a standardized credential that would help agencies procure a card that would meet the goals of the envisioned government-wide interoperability,
- a standardized numbering scheme for use on agency-issued credentials such that a card issued by one agency could be used when that cardholder visits a facility run by another agency,
- a range of assurance profiles associated with an extensible data model on credential cards.

This guidance provides a basis for numbering and access control environment solutions as specified in NIST SP800-73. These number schemes are critical for enabling common physical access control systems procurement at airport facilities.

2.3 Profile Standards

2.3.1 INCITS 383-2004 – Application Profile – Interoperability and Data Interchange – Biometric Based Verification and Identification of Transportation Workers

(ISO/IEC CD 24713-2 is similar but not identical to INCITS 383-2004)

In the interest of implementing a more secure personal verification system, this INCITS Standard establishes a transportation system-wide application profile to meet current and future physical and logical access requirements for all personnel of all modes of transportation and levels of responsibility. This INCITS Standard is a uniform transportation-wide effort to defend against and/or prevent against unauthorized access through the improvement of identity verification capabilities using biometrics for individuals seeking physical and logical access to secure areas.

Status: Published

Note: INCITS 383-2004 is required by the Transport Workers Identification Card (TWIC) program of TSA.

2.4 Conformance Standards

The following standards are under development. Other projects are just starting within M1 to define additional Conformance tests, such as for INCITS 377-2004. The discussion below is provided for informational purposes only.

2.4.1 INCITS Project 1703-D, Information technology – Conformance Testing Methodology for ANSI/INCITS 358-2002, BioAPI (ISO/IEC WD 24709-1)

This Standard:
a) Establishes a framework for Conformance Testing Methodology for BioAPI conformant Biometric Service Providers components that can be adapted for validation of these products, and would provide implementations of the BioAPI specification the ability to verify conformance with the specification.

b) Defines requirements and guidelines for specifying conformance test suites and related test methods for measuring conformity of Biometric Service Provider components to BioAPI specification, define procedures to be followed before, during, and after conformance testing.

Status: Review (2006)

2.4.2 INCITS Project 1704-D Information technology – Conformance Testing Methodology for ANSI INCITS 378-2004 Finger Minutiae Format for Data Interchange (ISO/IEC

This document specifies the testing activities required to assure a vendor's application or service's conformance to the Minutia Interchange Format. After reading this document, a user should be able to:
- Setup an environment to run tests
- Run tests and log results
- Understand what the tests are testing

Status: Review (2006)

2.4.3 INCITS Project 1705-D Information technology – Conformance Testing Methodology for ANSI INCITS 381-2004 Finger Image Based Data Interchange Format (ISO/IEC

This technical contribution establishes a foundation for and highlights of the standard, "Conformance Testing Methodology for INCITS 381-2004, Information Technology – Finger Image Based Data Interchange Format." This standard, when completed, will present an overview of conformance testing methodology that could be adapted to validate Finger Image Based Data Interchange Format-conformant files.

This standard is concerned with conformance testing of biometric data to the Finger Image-Based Data Interchange Format specification as per INCITS 381-2004. It is not concerned with testing of other characteristics of biometric products or other types of testing of biometric products (i.e., acceptance, performance, robustness, security). Any

organization contemplating the use of test methods defined in this standard should carefully consider the constraints on their applicability.

This standard is applicable to the development and use of conformity test method specifications, conformity test suites for ANSI/INCITS 381-2004, and conformance testing programs for INCITS 381-2004-conformant products. It is intended primarily for use by testing organizations, but may be applied by developers and users of test method specifications and test method implementations.

Status: Review (2006)

2.5   Performance Measurement and Reporting Standards

2.5.1 INCITS 409.1-2005 Information technology – Part 1: Biometric Performance Testing and Reporting – Framework (ISO/IEC FDIS 19795-1)

This standard addresses testing the accuracy of identification and verification devices, algorithms, and systems. This standard does NOT address related performance issues such as throughput, turnaround-time, cost of ownership, lifetime cycle costs, user implementations, environmental impact, cost/benefit breakpoints, etc. This framework part of the multi-part Biometric Performance Testing and Reporting standard is intended to describe the remaining parts of the standard and show their relationships and common aspects. An overview of the primary testing protocols, biometric applications, and performance metrics is presented. It also provides guidance on data analysis techniques, recording of results, and performance reporting measures available.

Status: INCITS 409.1-2005 Approved

2.5.2 INCITS 409.2-2005 Information technology – Part 2: Biometric Performance Testing and Reporting – Technology Testing and Reporting (ISO/IEC CD 19795-2)

This document is intended to be a prescriptive exposition of standardized methods for the offline testing of biometric systems and devices. It constitutes a specialization of a biometric testing framework in that it is concerned only with the offline use of *archived* biometric samples, and not the interaction of the human with the biometric sensor(s). The standard covers:
• Comparative or absolute testing of performance of biometric algorithms, components, or systems;
• Comparison of biometric data sets;
• Prediction of elements of deployed online performance;
• Assessment of performance available from complex data samples including repeated sample and multi-modal data.

Status: INCITS 409.2-2005 Approved

2.5.3 INCITS 409.3-2005 Information technology – Part 3: Biometric Performance Testing and Reporting – Scenario Testing and Reporting (ISO/IEC WD 19795-3)

The objective of this standard is to establish requirements for scenario-based biometric testing and reporting.

The goal of scenario testing is to determine the overall system performance in a prototype or simulated application. 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, care will be required that data collection across all tested systems is in the same environment with the same population. Test results will be repeatable only to the extent that the modeled scenario can be carefully controlled.

Status: INCITS 409.3-2005 Approved

2.5.4   INCITS Project 1602-D Information technology - Part 4: Biometric performance Testing and Reporting – Operational Testing and Reporting

While no draft currently exists for this standard, it is recommended that each purchasing agency perform some form of operational testing before and after full deployment of the selected biometric sub-system. As this standard evolves it may provide guidance to the agency on how best to conduct such tests.

Status: Pre-review (2006)

2.5.5   NP 19795-5: Biometric Performance Testing and Reporting –Part 5: Performance Testing for Biometric Devices for Access Control

This is a new project initiated within ISO/IEC JTC1 SC37 by the USA and is based on the work done within the TSA that is included in this guidance document as the Test Plan (Volume 3, Chapter 2).

Status: Pre-review (2006)

2.6   Credentialing Standards

This section is provided for information related to, but not required by this guidance.

2.6.1   FIPS PUB 201: Personal Identity Verification (PIV) for Federal Employees and Contractors (see http://csrc.nist.gov/piv-project/index.html)

This standard specifies the architecture and technical requirements for a common identification standard for Federal employees and contractors. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of an individual seeking physical access to Federally-controlled Government facilities and electronic access to Government information systems. The

standard identifies the problems to be solved, defines a common identity verification architecture, and describes the components, interfaces, support services, and life-cycle management functions needed to achieve requisite levels of security assurance for applications that require different levels of protection. The standard also incorporates and refers to other technical and operational standards necessary to achieve interoperability among identification cards, electronic card readers, communication systems, and access control systems interfaces.

Status: Published (02/2005)

Note:
In addition to the procedure for identity proofing and enrollment in Volume 2 Chapter 1, Annex A of FIPS 201 identifies two additional means to achieve this goal. The first method is described as Role Based Identity Authentication and uses identity source document inspection and background checks to establish assurance of identity. The process provides the minimal functional and security requirements for achieving a uniform level of assurance for identity credentials. The second method is a System Based Model that employs an automated identity management system where the employee is first registered and subsequently enrolled in the system allowing for card production, issuance, and activation in a controlled system environment. This model is recommended where a completely new system is being deployed, whereas the first method is recommended for use in conjunction with existing access control systems. It is recommended that airports follow the System Based Model referenced in Appendix A.2 of FIPS 201.

2.7   Airport Standards

2.7.1   RTCA DO 230A: Standards for Airport Security Access Control Systems

The document provides guidance on acquiring and designing an ACS, testing and evaluating system performance, and operational requirements. It should be emphasized that these guidelines and performance standards are not regulatory in nature, but represent the industry's derived consensus on minimum performance standards to be met in achieving consistency and interoperability in an airport access control environment.

This updated document incorporates the latest technological advances in ACSs technologies, addressing smart cards and biometrics. Since the original DO-230 release, there have been major developments in the access control technologies used and evolving standards to ensure robust system architecture and common subsystem communications platforms and interfaces. Rapid advances in the field of biometrics and chip technology have necessitated the need to include detailed guidance in these areas, as provided in Appendix A.

Status: Published (Note that plans exist for another revision of DO230 based on this TSA guidance)

3 ISO/IEC JTC1 Standards

In addition to the standards indicated above, JTC1 SC37 has a number of projects under development. It is customary that these standards will be adopted by ANSI when they are completed. There are no equivalent domestic projects currently under development within the US. This information is provided for your information and may not be required.

3.1 Interface Standards

3.1.1 WD 19784-2: BioAPI-Biometric Application Programming Interface – Part 2: Biometric Archive Function Provider Interface

3.1.2 FDIS 19785-2: Common Biometric Exchange Formats Framework – Part 2:Procedures for the Operation of the Biometrics Registration Authority

3.1.3 WD 24708: Protocol for Inter-working Between a System Supporting a Biometric Device and a Central Repository of Biometric Data

3.1.4   WD 24722: Multi-Modal Biometric Fusion

3.2 Data Format Standards

3.2.1   FCD 19794-1: Biometric Data Interchange Format – Part 1: Framework

3.2.2   FCD 19794-8: Biometric Data Interchange Format – Part 8: Finger Pattern Skeletal Data

3.2.3   NP 10794-9: Biometric Data Interchange Format – Part 9: Vascular Biometric Image Data

3.3 Profile Standards

3.3.1   FCD 24713-1: Biometric Profiles for Interoperability and Data Interchange-Part 1:Biometric Reference Architecture

3.4 Conformance Standards

3.4.1   WD 24709-2: BioAPI Conformance Testing – Part 2: Test Assertions

3.5 Performance Measurement and Reporting Standards

3.5.1   WD 19795-3: Biometric Performance Testing and Reporting –Part 3: Specific Testing Methodologies

3.5.2   CD 19795-4: Biometric Performance Testing and Reporting –Part 4: Interoperability and Data Interchange Formats

4.   Conformance Testing Options

Conformance testing options are evolving as the technology matures and standards are completed. In the case of base standards, conformance tests are under development or are planned for development in the near future. Eventually, all base standards will have conformance tests available and the metrics defining pass/fail will be specified. As the committees gain experience in developing these kinds of standards, the development time can be expected to be reduced. At this time, conformance tests are being defined in from 1.5 to 3 years. It is expected that this activity will be substantially complete for the existing published standards within the next two years (late 2006 or early 2007). Until that time, the purchasing agency will have several options available.

4.1   Vendor Claim of Intent to Conform

It is reasonable to expect that for some period of time vendors of some biometric sub-systems will have implemented their products using a previous standard. In such cases, the vendor may be unable to claim conformance to the procurement specified standard, but should be expected to respond to a purchasing agency with a plan to bring the product within conformance to the new TSA QPL standard. Decisions to deploy such non-conformant devices are the responsibility of the purchasing agency, however, it is recommended that such deployment be for a short pre-agreed period of time, with the intent of a planned upgrade.

4.2   Vendor Claim of Conformance

INCITS 383-2004 (Biometric Profile for Transportation Workers) contains a Requirements list and Annex A for the Base Standards, and an Implementation Conformance Statement (ICS) in Annex B. Conformance with this standard requires that the vendor complete the ICS for the products being supplied and this constitutes **a vendor claim of conformance** with the applicable base standards.

4.3   Vendor Tested for Conformance

In addition to the vendor claim of conformance, the purchasing agency may require the vendor to supply tangible proof that the implementation has been tested for conformance. Such proof may include vendor test records (including testing methodology) and audit trails. Test tools may include approved testing standards or vendor test regime until such standards are agreed and available. If a standardized testing regime exists, the purchasing agency should require that this regime be used in vendor initiated self-testing.

4.4   Third party Testing for Conformance

Third party test facilities will likely come into being as a result of the deployment of biometric solutions and the availability of standardized test suites. Its neutrality in the procurement process, representing neither the vendor nor the purchasing agency, characterizes such a facility. This level of testing represents the goal for conformance testing of biometric access control devices. Access control solutions tested in such a manner will be identified and be placed on a Qualified Products List (QPL) to be established by the TSA. This will enable purchasing agencies to select such products with confidence that they have been tested to conform to the base standard.

4.5   Accreditation of Third Party Testing – NIST

Third party testing is only as successful as their test regime is complete and actually tests for conformance. Such a determination can only be made by a recognized accreditation organization such as the NIST, National Voluntary Laboratory Accreditation Program. These organizations have developed over time the capability to accredit third party testing laboratories based on ISO/IEC 17025 and testing specific competence criteria. This is expected to be the final step in the conformance test program for biometric access control devices, and a necessary component in providing confidence to purchasing agencies that the QPL is reliable and has been assembled consistent with best practices.

4.6   Interoperability

Interoperability of biometric devices for airport access control is not a predominant issue since each airport's implementation is largely stand alone. The interoperability across airports (such as for aircrew and other multi-airport employees) is a function supported by the TWIC program, and while not mandatory, interoperability with the TWIC standard is in fact desirable. In the case where an airport may choose to select multiple different suppliers of biometric devices for use in the same airport deployment, then interoperability between the chosen devices is essential to successful operations.

Note: third party testing and qualification by NIST does not guarantee interoperability of multiple vendor solutions in a given installation. This is beyond the scope of conformance testing and purchasing agencies should be aware that potential undiscovered problems may occur when more than one vendor is supplying equipment for use with the same modality, for example, two different vendors of Fingerprint biometric subsystems.

5.   Performance Testing

INCITS 409.1-2005 Information technology – Part 1: Biometric Performance Testing and Reporting – Framework and ISO/IEC 19795-1: Principles and Framework, state generally applicable testing and reporting requirements, and that different systems and applications may require differences in test methodology. These standards provide the basic principles for conducting and reporting a performance evaluation.

INCITS 409.3-2005 Information technology – Part 3: Biometric Performance Testing and Reporting – Scenario Testing and Reporting, and Clause 6 of 19795-2 (Testing Methodologies) deal with Scenario testing and is relevant to the biometric sub-system

testing suitable for qualifying products for use in airports. Scenario testing is designed to evaluate end-to-end performance of a biometric system in a simulated application with controlled conditions. Scenario test planning is contingent on the type of data required to enable proper evaluation of the performance characteristics of biometric subsystems for access control. Scenario testing provides opportunities for introducing environmental conditions and constraints, given the use of a specific test population providing data specifically for the purpose of biometric testing.

6.   Guidance on the use of Standards

The following guidance is provided on the use of standards in the procurement of biometric access control devices.

6.1   Base Standards

Only those base standards that have been published or are at least at the level of final review should be specified in procurement of biometric access control devices.

6.2   Conformance Demonstration

Vendor claims of conformance (or intent to conform) may be the initial form of conformance demonstration, but it is recommended that all such claims of conformance be accompanied by a complete description of the degree of commitment to conformance to this standard and if applicable a planned schedule for achieving conformance.

As test standards become available, it is recommended that third party testing be initiated as soon as possible with certification of the third party tester(s) by NIST.

6.3   Performance Testing

Performance testing by third party testers should be planned and directed by TSA to formulate the initial QPL. The plans, protocols, and procedures developed by TSA will precede the ANSI or ISO process for developing approved standards in these areas. All generic standards for biometric performance testing and reporting should be required and conformed to by the testing organization.

VOLUME 2:
IMPLEMENTATION GUIDANCE DOCUMENT

30 September 2005

EXECUTIVE SUMMARY

BIOMETRICS FOR AIRPORT ACCESS CONTROL

VOLUME 2: IMPLEMENTATION GUIDANCE DOCUMENT

How Does the Material in the *Implementation Guidance Document* Relate to the Legislation?

On December 17, 2004, President Bush signed the Intelligence Reform and Terrorism Prevention Act of 2004. The legislative language of this act in Title IV – Transportation Security, Section 4011 – Provision for the Use of Biometric or Other Technology, directs TSA to "issue, not later than March 31, 2005, guidance for use of biometric technology in airport access control systems." As this Act requires, *Volume 2: Implementation Guidance Document* specifically addresses, from Section 4011 (a) 5 subparagraphs (C) and (D) of the legislation:

Subparagraph (C) requires TSA to establish, at a minimum, "procedures for implementing biometric identifier systems to ensure that individuals do not use an assumed identity to enroll in a biometric identifier system; and to resolve failures to enroll, false matches, and false non-matches"; Subparagraph (D) requires TSA to establish "best practices for incorporating biometric identifier technology into airport access control systems in the most effective manner…"

The *Implementation Guidance Document* (Volume 2 of the Guidance Package, "Biometrics for Airport Access Control") is focused on the biometric sub-system aspects of the airport access control function (not on qualification of biometric devices). Its guidance is therefore primarily directed to airport operators and the contractors (such as systems integrators) chosen to deploy these devices.

What is In the *Implementation Guidance Document*?

A major component of the TSA guidance is to provide all the concepts that airport operators need to understand in order to best integrate biometric devices into their access control systems, and also what operational criteria for using biometric devices in access control systems should be addressed in their airport security plans.

The *Implementation Guidance Document* consists of 3 chapters:

> Chapter I - Identity Authentication
> Chapter II - Resolving Failures
> Chapter III - Best Practices for Implementation with Legacy Systems

These chapters delineate guidance that TSA has identified on how to incorporate biometric devices into airport access control systems and certain technical issues that must be addressed in that process. Each of these chapters is briefly described next.

The **Identity Authentication** chapter provides recommended practices for breeder document authentication. This issue is not directly related to the deployment of biometric functionality, but is a significant security consideration in the context of overall employee identity management.

The **Resolving Failures** chapter provides discussion of and options for resolving enrollment failures, including discussion of false match control and other security layers, and options for resolving false rejects.

The **Best Practices for Implementation with Legacy Systems** chapter recommends approaches to biometric incorporation that will preserve the investment in legacy access control systems.

How Should the Reader Use the *Implementation Guidance Document*?

Airport operators will want to become acquainted with the procedures regarding failures to enroll, false matches, and false non-matches. False matches in particular are a difficult challenge and the guidance will help them learn how to deal with this aspect.

Airport operators have a sizeable investment in their legacy access control systems. They do not want to have this investment in their legacy systems rendered obsolete because of the introduction of biometric technology. This chapter details steps the airport operator can take to get the benefit of the new biometric technology without having to make unwelcome trade-offs in the process.

System integrators who incorporate biometric technology into access control systems will likewise want to understand the implementation guidance.

Volume 2 – IMPLEMENTATION GUIDANCE DOCUMENT

BACKGROUND

On December 17, 2004, President Bush signed the Intelligence Reform and Terrorism Prevention Act of 2004. The legislative language of this act in Title IV – Transportation Security, Section 4011 – Provision for the Use of Biometric or Other Technology, directs TSA to "issue, not later than March 31, 2005, guidance for use of biometric technology in airport access control systems." As this Act requires, *Volume 2: Implementation Guidance Document* specifically addresses, from Section 4011 (a) 5 subparagraphs (C) and (D) of the legislation:

Subparagraph (C) requires TSA to establish, at a minimum, "procedures for implementing biometric identifier systems to ensure that individuals do not use an assumed identity to enroll in a biometric identifier system; and to resolve failures to enroll, false matches, and false non-matches"; Subparagraph (D) requires TSA to establish "best practices for incorporating biometric identifier technology into airport access control systems in the most effective manner…"

The *Implementation Guidance Document* is focused on the biometric sub-system aspects of the airport access control function (not on qualification of biometric devices). Its guidance is therefore primarily directed to airport operators and the contractors (such as systems integrators) chosen to deploy these devices.

CHAPTER 1 - IDENTITY AUTHENTICATION

1. SCOPE

Chapter 1 addresses the portion of the section 4011(a)(5) of the Act that directs TSA: to establish, at a minimum, "procedures for implementing biometric identifier systems to ensure that individuals do not use an assumed identity to enroll in a biometric identifier system…"

2. GUIDANCE FOR IMPLEMENTATION

A secure credentialing program is supported through an overarching "chain of trust" model that is designed and implemented to provide a recognized level of trust in the credential. That credential can then be trusted to represent and assure the identity of an individual who presents it. This "chain of trust" is a multi-step process beginning with tying the individual to the claimed identity, and subsequently to the specific identity assurance procedures in place (i.e. ID document validation, background check, biometric search, etc.), and finally to the issued credential containing a biometric identifier. An individual carrying the issued credential can authenticate his identity to any receiver upon presentation. The use of biometric identifiers on (or associated with) the credential completes and strengthens the chain of trust by linking the holder directly to the credential and, assuring that the holder is who he presents himself to be through positive biometric authentication.

Homeland Security Presidential Directive-12 (HSPD-12) presents requirements for identity authentication and credentials for use in logical and physical access control systems. Federal Information Processing Standard (FIPS) 201 is the US government standard that implements HSPD-12. It provides a secure credentialing program with "chain of trust" management for identity proofing and biometric information management. FIPS 201 represents the latest improvements with regard to "best practices" for strong identity proofing and credentialing. It is strongly recommended that airport access control systems follow this standard.

Office of Management and Budget (OMB), in coordination with GSA and NIST, will provide guidance to support implementation of FIPS 201. The implementation guidance is anticipated in July 2005. These documents will provide details for conformance and acquisition, configuration management, and system implementation.

The information provided herein represents the most current guidance available in both the federal government and commercial industry. As this information and guidance is revised, or new information is made available, this document may be modified as a result.

2.1 Breeder Document Validation

The Intelligence Reform and Terrorism Prevention Act of 2004 contains four separate provisions related to standards for identification documents -- Sec.7209, documentation for travel into the United States; Sec.7211, standards for birth certificates; Sec.7212, standards for driver's licenses and other personal identification; and Sec.7220, standards for identification documents required of domestic commercial airline passengers. These provisions are expected to yield baseline recommendations for acceptable personal identification documents and are expected to be published later in the year. Airport authorities are encouraged to review these standards and consider adopting them in support of enrollments into the airports credentialing process.

Making this element of the identity proofing process effective requires careful attention to reviewing each document as an identity verification resource. Organizations in law enforcement and border security have significant training and experience with these documents. One of the most comprehensive sources for guidance in the use of breeder documentation and their validation is the American Association of Motor Vehicle Administrators (AAMVA). AAMVA has made available to its licensing jurisdictions established best practices in various subject areas related to identity management, to include a resource list of acceptable verifiable documents and the reliable data elements associated with each. (See table below) Additionally, AAMVA and other organizations have established useful educational programs which teach established criteria and procedures to personnel tasked with handling personal ID validation documentation during program enrollment.

The AAMVA documents describe best practices for the past 5 years. (see http://www.aamva.org/IDSecurity/idsDLIDSecurityFramework.asp) Standards such as FIPS 201 and recent legislation (i.e. Intelligence Reform and Terrorism Prevention Act of 2004) augments these documents to update and enhance the process in the use of AAMVA practices.

The use of automated document validation technology can be applied to validate certain classes of documents automatically. These systems can capture text, images, OVDs, and other encoded machine-readable data from driver's license, passports, visas, and other document types, and can also determine the presence of overt and covert anti-tampering/counterfeiting features. Other available systems use information-based individual authentication/threat assessment services to provide parallel analyses on the name, address, date of birth, and other personal identifiers. These services provide a risk score, and can return codes identifying high risk factors such as disconnected phone numbers, prison mail receiving addresses, or use of a Social Security Number (SSN) associated with a deceased person. Individuals who show no personal history in the public data stream, or whose data is not internally consistent will be flagged, thereby helping to identify attempts at identity fraud by applicants.

It is important that any presented documents used for ID validation are electronically captured and included in the enrollment record. Wherever possible, documents should be machine-read to auto-capture data in an effort to avoid manual keying mistakes.

Doc file #	AAMVA Document Title
--	AAMVA DL/ID Security Framework (2/2004)
02-42-03	White Paper on Over-the counter, Central and Hybrid Issuance
04-43-03	Internal Controls Driver Licensing and Identification Processing BP
06-51-03	Appendix 1 to Internal Controls Best Practices
03-43-03	Appendix 2 to Internal Controls Best Practices
--	Using the Acceptable Verifiable Resource Lists
--	Appendix 1 U.S. Resources List
10-63-03	Social Security Number verification best practices
11-6.3-03	Address Verification Best Practices
12-6.3-03	Third Party Verification Best Practices
14-7.1-03	Requirements for Name Collection, Use and Maintenance
15-7.2-03	Tying End of stay (EOS) date to expiration date of driver license or identification card
18-7.4-03	Business Requirements for the Unique Identifier
19-7.4-03	AAMVA UID9 Biometric Identification Report
21-74-03	Biometric Technology Information Needs (v1.4 - 12/03)

2.2 Background Check

A background check is an important part of the secure chain of trust to further assure the identity of the individual, as well as other appropriate criteria. Today, unescorted access to secure areas of the transportation system is restricted by the Aviation Transportation Security Act (ATSA), the Maritime Transportation Security Act (MTSA), and the Patriot Act[2]. Individuals that need unescorted access to these areas now require a background

---

[2] USA PATRIOT Act of 2001 Pub. L. 107-56 Sec.1012 - Amends the Federal transportation code to prohibit States from licensing any individual to operate a motor vehicle transporting hazardous material unless the Secretary of Transportation determines that such individual does not pose a security risk warranting denial of the license and requires background checks of such license applicants by the Attorney General upon State request.
Aviation and Transportation Security Act of 2001 (ATSA) Pub. L. 107-71 Sec.106 -Requires the Under Secretary of Transportation to work with airport operators to strengthen access control points in secured areas and consider the deployment of biometric or similar technologies that identify individuals employed at such airports. Section 114 (f) (12), ATSA and requires background checks for airport security screening personnel, individuals with access to secure areas of airports, *and other transportation facilities*.   In addition, ATSA includes broad authority for security in all modes.
Maritime Transportation Security Act of 2002 (MTSA) Pub. L. 107-295 Sec 102 §70105 - Requires the issuance of biometric transportation security cards and the completion of background checks for entry to any secure area of a vessel or facility. It also should be noted that the Homeland Security Act of 2002, Pub. L. 107-296, Sec 1123, adds immigrant aliens to those persons barred under 18 USC 842 from shipping or transporting explosives, absent a waiver granted by the Bureau of Alcohol, Tobacco, Firearms and Explosives (sic).

check to gain access. The type and nature of any background check can vary depending on program policies and/or security requirements. Background checks usually incorporate an FBI criminal history check using fingerprints, or may include a terrorist threat check, or a LexisNexis search for example. A name based check against federal terrorist watchlists is relatively new, but certainly has become increasingly important.

Another element to consider related to background checks is the frequency with which they are revalidated. This duration may impact the longevity of any issued credential tied to such a check. Although there is no standard, current practices typically require a refresh every three to five years.

2.3 1:N Biometric Check

One of the key uses for biometric technology in credentialing systems is in the prevention of false identities. This is a critical piece of a strong trust model. The inclusion of a biometric sample (typically a fingerprint biometric) in the enrollment record allows that data to be compared against all accumulated enrollments to confirm that the individual is not already enrolled in the system. This is referred to as a "one to many" search, and is designed and implemented to assure that only one credential is issued per person.   This not only raises the level of security and is a deterrent to identity fraud but also prohibits duplicate alias enrollments. Any matches that may occur would be adjudicated to determine validity according to program protocol.

CHAPTER 2- RESOLVING FAILURES

1. SCOPE

Chapter 2 addresses the portion of the Act that states: to establish, at a minimum, "procedures for implementing biometric identifier systems …to resolve failures to enroll, false matches, and false non-matches;"

2. GUIDANCE FOR IMPLEMENTATION

It is important that the use of biometric authentication is properly considered as a security layer so that biometric match failures are not judged to be catastrophic. While biometric systems are capable of highly reliable personal identification and verification, they do not provide 100% accuracy. Therefore, a security system designed to use biometrics technology must be robust enough to handle special situations. Matching error rates and enrollment failures are an intrinsic statistical reality in biometric recognition systems. The process of comparing biometric data using mathematical algorithms results in a numeric match score that is basically transposed into a confidence level as to a person's identity. Both 1:1 biometric verification systems and 1:N identification systems have recognized percentage of matching errors. Also, different biometric modalities like finger, face, hand and iris for example, provide different statistical performance even in similar environments. These are measurable performance parameters that may be affected or influenced in one or any combination of ways to minimize matching errors, but biometric errors cannot be resolved to 0%.

2.1 Failure to Enroll

A Failure to Enroll (FTE) occurs when an individual is unable to provide a biometric sample capable of providing successful match results. The biometric FTE occurrence, though usually infrequent, exists in all modalities and can be the result of disease, age, race, occupation, missing samples (finger, hand, eye, etc.), operator error, etc. (For example, cataracts or very poor vision may inhibit iris enrollment, older persons with very dry skin may be unable to enroll in fingerprint systems, manual laborers such as masons may have very worn fingerprints, and certain ethnic groups may have difficulty enrolling in fingerprint, iris or face recognition systems.) The selection of the biometric modality can be considered to maximize the system's efficacy if the intended population is older, or works at a manual trade for example.

In programs or systems using biometrics, FTE can be problematic. In such cases, it is a simple reality that persons who cannot provide a usable biometric sample must use alternative methods to authenticate themselves. These alternatives may include a secondary biometric or, more often a PIN is assigned to that individual and the special circumstance is documented in the enrollment record (and elsewhere as necessary). Security administrators should anticipate and plan for these occurrences and maintain alternate authentication technologies, and policies to address them. Consider too, that

systems have not always used biometric authentication and would be well advised not to rely on it exclusively.

Additionally, those individuals not able to submit a usable biometric sample may be unable to have their records used for a biometric 1:N search. A clear policy to address these special cases is important to develop and would place more weight on the other identification validation processes. These are predictable circumstances and should be handled in an appropriate fashion, remembering that no system can rely on biometrics exclusively.

2.2 Equal Error Rates (EER)

Biometric technology performance is typically measured using two key statistical metrics that are applied to determine an equal error rate (EER) of the matching system. The False Reject Rate or FRR (Type I error) occurs when an individual's biometric doesn't match to the enrolled biometric sample. Similarly, the False Accept Rate or FAR (Type II error) occurs when an individual's biometric incorrectly matches another. Both of these type errors have obvious security implications. A Type I error is an inconvenience and can cause a system to be judged poorly because the right people are denied access. The occurrence of a Type II error is the most worrisome because it could allow access to the wrong person.

All biometric systems have measurable error rates. The rate at which these errors occur can be adjusted in the matcher technology by changing the matcher's scoring thresholds. For example, increasing the scoring threshold would lower the occurrence of Type II errors. In other words, the matcher would need a higher match score (higher probability) for a positive match result, thereby reducing the occurrence (chance) of a false match. This improves security by making it harder for the wrong people to gain access. On the other hand, a higher threshold setting increases the occurrence of Type I errors, denying access to the right people because the matcher needs higher match scores.

Biometric manufacturers have developed their technologies using statistical tools to "balance" performance between these kinds of errors. The EER is a graphic point where the two plotted error rate curves intersect. This is typically what is stated to compare the performance of biometric systems. Many factors can influence performance accuracy in biometric systems, and the adjustment of thresholds can be applied to correct or enhance performance depending on integration, environmental or security factors.

2.3   Resolving False Match Errors

While it is true that if a biometric sub-system makes a false match error, it has absolutely no indication of the error (if it did know, then it would not have made the error). In the event of a false match, as infrequent as that may be, there are other layers of security that assist in resolving that error.

The most profound layer of security that can resolve false match errors is the SIDA challenge rule. All airport employees are trained to be aware of individuals in the secure area who appear not to belong in the area. One of the techniques for detecting such an intruder is looking for and examining an individual's ID badge, always worn on the outside of their clothing while in the secure area.

Note also that the "window of opportunity" for a security breach due to a false match is limited to the period of time that a lost or stolen badge goes unreported. If an intruder acquires an employee's card and attempts to gain access (hoping for a false match on the biometric), the attempt will be defeated by the access control system, even if the false match occurs, so long as the badge has been reported as missing and the ACS administrator has revoked the privileges previously granted to the holder of that ID.

2.4 Resolving False Non-match Errors

Since the number of "genuine" attempts to gain access (that is, attempts by valid employees, using their own ID) is very large relative to the number of terrorist "imposter" attempts, the error most frequently occurring is the false non-match or false reject. This error does not result in a security breach, but rather is a form of inconvenience.

Resolving false rejects can be accomplished in a number of different ways, including:
- Providing an intercom at the entry point to contact the Security Operations Center
- Providing an attended entry point (nearby) where a guard can verify identity using the photo ID
- Providing an alternate biometric
- Providing a user PIN number as a backup

None of the backup procedures to resolve false rejects are as good as having a true accept. However, these errors are a fact of biometric life and must be provided.

Note that record keeping on individuals with a higher frequency of false rejects can be useful to identify candidates for re-enrollment, as the quality of a users enrollment can be the source of false rejects. Also, as time elapses after enrollment, the rate of false rejects may tend to increase, again prompting re-enrollment.

CHAPTER 3 - BEST PRACTICES FOR IMPLEMENTATION WITH LEGACY ACCESS CONTROL SYSTEMS (ACS)

1. SCOPE

Chapter 3 addresses the portion of the Act (subparagraph (D)) that states: to establish "best practices for incorporating biometric identifier technology into airport access control systems in the most effective manner…"

2. GUIDANCE FOR IMPLEMENTATION

Congress has recognized that biometric technologies are a sound method of restricting access to secured areas. TSA is aware that some airport operators may be unwilling to implement biometric secured areas because TSA has not yet identified technologies that it believes perform acceptably. The QPL is designed to provide that information. Airport operators may choose to upgrade their existing ACSs by purchasing and using the technologies to be listed on the QPL.

Put into proper context, biometric technology is another security layer in a designed physical access system. This layer adds a powerful authentication feature to assure the identity of system users, and is often referred to as a sub-system in itself. If treated as a sub-system, it would be logical that biometric authentication could be "retro-fitted" into legacy ACS. This practice may be the ideal way to upgrade an ACS, depending on its age and whether it has the infrastructure to support the technology advance. This upgrade logic also supports the notion of saving money by extending the useful life of existing systems, while the concept is sensible, successfully implementing biometric systems is a challenging exercise that needs careful consideration, especially if it is to be hybridized into legacy ACS technologies.

The increasing use of biometrics technologies has improved the level of understanding and has moved the industry forward. Examples of successful biometric implementations for ACS can be found in legacy system environments where, 1) security management has carefully assessed its options in upgrading an existing system and is prepared to do the work necessary to make the systems effective, and 2) a complete overhaul is the best option in an older systems deemed too expensive and problematic to maintain, or has become too cumbersome to operate.

There are four important steps to integrating a biometric identification system to a legacy physical access control system. These steps are described below.

2.1 Prepare a Business Case

All security systems require the expenditure of time, energy, and money in their planning, design, architecture and deployment. A successful security system will consider every dimension, option and contingency in its design. And, it seems that stronger security environments have provided an opportunity for biometric placements. However, fascination with the technology does not make a strong business case. Because biometric technology is relatively new on the scene, it is very important to properly design its application into a security architecture. It can be shown that often biometric efforts have been judged as too costly and performed poorly, not because of deficiencies in the technology, but because the business case for its use was not made properly, and, the integration was improperly executed. Biometrics technologies are certainly not "plug and play". Integrating biometrics with legacy systems can be very attractive and effective. In any event, several points must be kept in mind in preparing the business case:

- Critical decisions must be made either to overhaul all or part of the system, or build onto the existing system
- All security systems, especially using biometrics technology, require time, money, and energy to plan, deploy and run. In addition to set-up and operational costs, system throughput rates must be carefully considered. Keep in mind that enrollment sessions for all users will be required. The time and cost of training for users, enrollment personnel and administrators need to be considered.
- Biometric systems require a strong ID management component.
- Some persons will not be able to use the biometric system successfully every time. This implies that backup systems for "exception handling" will be required.
- Studies of user attitudes have shown user acceptance of biometric technology to well exceed 90 percent. Nonetheless, there will always be a few people who object to any new technology.
- Choose the system integrator very carefully. Hardware/software integration will prove to be the most difficult task. Biometric technologies are not "plug and play." Even ideal technologies will fail if the devices cannot talk to the database or open the gate. Systems integration may require changes in other pieces of hardware not considered at first glance to be part of biometric technology.
- Know the history and track record of the technology vendor. The industry is in development so that commercial products and vendors are changing. It is possible that the technology invested in today may not have vendor support next year.

Deciding to use biometric technology will have an impact on the business and systems operations. The addition of biometrics or substitution for another component will require a change in some business processes. Beyond the obvious software/hardware integration there is the issue of "change management" to consider in integrating the use of biometrics into the existing processes.

2.2 Classify Application

 Properly assessing the security application environment is a critical step in selecting a technology. The various biometric modalities are strongly differentiated by their

technical and functional applicability to different environments. It is important to establish the following concepts:

- Will users be habituated or non-habituated? That is, after a period of time, will the average user be accessing the technology regularly or sporadically? Some biometric modalities require greater user involvement and practice than others.
- Will users be supervised or unsupervised? Systems vary in the level of required supervision and/or user prompting at enrollment and during operation. The level of training required by enrollment personnel also varies among the modalities
- Will users be employees or people otherwise organized under the domain of the system administrator, or will users be part of a larger domain, multiple domains, or larger enterprise system?
- Will the system be required to operate with systems operated by different management (open) or will it operate standalone (closed)?
- Is the application indoors or outdoors, or in an otherwise harsh physical environment? System weatherproofing can be a challenge.   Also consider that people in outdoor environments cover themselves in varying and unpredictable ways that may hamper convenient utility, and the weather itself may impact utility.
- Are there data storage limitations in the system? For instance, biometric template sizes vary among the technology providers making some technology options unsuitable for on-card storage.
- How much system reporting will be required?   The ability of the vendor software to generate reports differs widely. A good understanding of audit trail requirements in the system design is necessary.
- Throughput rate requirements must be established for both enrollment and operations taking into account the population size and deployment schedule. Biometric systems require proper enrollment protocols be followed. Also, the operational throughput should be considered for all locations (portals) where biometrics will be used.
- How will the system handle "exceptions" in cases where users cannot enroll a biometric or the system encounters a false rejection error? Also, how many errors can be tolerated in a given period?   Exception handling will greatly decrease system throughput. False acceptance errors will erode the perceived integrity of the system. Errors can be decreased through more careful enrollment and more quality control feedback to the user.
- How long can enrollment images be expected to remain usable before a refresh is required? Some modalities will experience performance degradation more rapidly than others.   The aging process affects all biometric systems considering that a person's physical and behavioral characteristics naturally change over time.
- What is the budget? Systems can vary greatly in price, and value can be hard to determine. A well-considered design is a key aspect to realizing a successful value add.

2.3 Determine System Requirements

Biometrics technology requires a particular level of infrastructure in order to operate properly.   It is important to know the basic functional requirements of the upgrade

technology so that the system will be able to perform as intended. In these circumstances, legacy systems can be a design enhancement or a design flaw.
 Many access control systems currently in use may not be able to accept the addition of a biometric. Some access control systems either were created or installed prior to any open standards being established or are proprietary in nature and will not accept the addition of a biometric. Even some standards based systems may not be compatible with certain biometric identification systems.   However, in the most cases, biometric systems can be adapted to be synergistic with ACS behaviors.

2.4 Create Integration Plan

With the end goal of a higher level of security with a minimum impact to the efficiency or effectiveness of the access control system, the path to integrating a biometric identification system requires the diligent use of change management. Process re-engineering is a step that should be completed before any work is initiated. This may include the best location for the installation of a reader or a redesign of a queue to make a biometric reader more accessible. The most challenging task, however, is the education of the personnel requiring access. Effective training and education can significantly reduce the time required for enrollment or for access to secured areas. Proper training can also reduce or eliminate concerns over privacy or health risk from using certain biometric devices.

VOLUME 3:

PLAN FOR BIOMETRIC QUALIFIED PRODUCTS LIST (QPL)

30 September 2005

EXECUTIVE SUMMARY

BIOMETRICS FOR AIRPORT ACCESS CONTROL

VOLUME 3: PLAN FOR BIOMETRIC QUALIFIED PRODUCTS LIST (QPL)

What is In the *Plan for Biometric QPL* Document?

A major component of the TSA guidance is to provide instructions for manufacturers of biometrics sub-systems who wish to have TSA place the product on the QPL. Manufacturers will find this TSA guidance crucial to understanding the testing and evaluation practices that will be involved in the overall product qualification project. The *Plan for Biometric QPL* consists of 4 Chapters:

> Chapter I - Management Plan
> Chapter II - Test Plan
> Chapter III - Business Model
> Chapter IV - Schedule for Initial Qualified Products List (QPL)

These chapters delineate the near-term and longer-term actions that TSA will undertake in order to issue the QPL. Each of these Chapters is briefly described next.

The **Management Plan** chapter provides an overview of the management activities and processes required for TSA to formally-establish QPL. The Plan describes processes that biometric device manufacturers must follow in order to apply for TSA qualification testing. Specifically, the Plan defines manufacturer application processes for qualification, and describes the required manufacturer data package to be submitted for TSA review. In addition, the conformity assessment program is defined. This addresses processes for assuring manufacturer conformance and accreditation of "Qualification Test Organizations". Organizations can apply for certification that allows them to offer qualification testing services, related to airport access control, to the biometric device community.

The **Test Plan** chapter provides details of "what" will be tested in the regimen of performance-based scenario testing of production biometric devices required for manufacturer/device qualification. It defines Core and Optional Tests, test measures and variables, test crew (e.g., crew size and demographics), and environment and outdoor conditions. It details data collection and reporting requirements. The Test Plan specifies what will be examined in determining specific biometric device qualification based upon the requirements provided in Chapter, 1 Technical Requirements and Chapter, 2 Operational Requirements of Volume 1, Requirements Document of the TSA Guidance Package.

The **Business Model** chapter establishes how testing costs will be covered for the initial QPL.

The **Schedule for Initial Qualified Products List (QPL**) chapter provides a high-level view of the activities expected in the post-March 31, 2005 timeframe. It identifies the period for public review of guidance, indicates manufacturer application timing, and establishes a target date for availability of the initial QPL.

How Should the Reader Use the *Plan for Biometric QPL*?

Manufacturers of biometric devices who wish to qualify for device applications related to airport access control should use the *Plan for Biometric QPL* to understand the application process for device performance qualification testing and prepare their device for testing.

Appendix A of *Chapter 1, Technical Requirements* from *Volume 1: Requirements Document* of the TSA Guidance Package delineates the specific quantitative technical qualification test specifications.

Chapter 2, Operational Requirements of *Volume 1: Requirements Document* of the TSA Guidance Package delineates the operational qualification test specifications.

In brief, to be placed on the TSA QPL, a manufacturer's device will be expected to meet minimum qualification performance in terms of error rates, enrollment rates and transaction times. In addition, the manufacturer's biometric device will be examined for qualification based upon parameters in Appendix B of *Chapter 1, Technical Requirements* in *Volume 1: Requirements Document* or attested through manufacturer certification of conformance alone, manufacturer certification of conformance with substantiation required, or independent / accredited certification of conformance with substantiation required depending upon the parameter being considered.

VOLUME 3 – PLAN FOR BIOMETRIC QUALIFIED PRODUCTS LIST (QPL)

CHAPTER 1

MANAGEMENT PLAN
For
Biometric Sub-System

30 September 2005

EXECUTIVE SUMMARY

The Transportation Security Administration (TSA) is charged with countering threats to aviation security with technologies and procedures that will prevent, deter, or render ineffective any attempt to sabotage civil aviation. Part of this mission involves improving the capability of airport security to control access to secure parts of the airport based on the identity of the individual requesting access.

The purpose of this management plan is to outline the framework of the TSA biometric qualification test program, and to define the documentation and processes that will be used by TSA in conducting the qualification test program. The TSL test director is responsible for developing this management plan as well as the biometric sub-systems test plan, approving procedures and overseeing all tests.

TABLE OF CONTENTS

Page

LIST OF FIGURES

ACRONYMS

CFR	Code of Federal Regulations
CI	Configuration Item
CTO	Chief Technology Officer
NIST	National Institute of Standards and Technology
NTIS	National Technical Information Service
QDP	Qualification Data Package
QPL	Qualified Products List
RMA	Reliability, Maintainability and Availability
SSI	Sensitive Security Information
T&E	Test and Evaluation
TSA	Transportation Security Administration
TSL	Transportation Security Laboratory
WJHTC	William J. Hughes Technical Center

1. INTRODUCTION

The Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458, requires the Transportation Security Administrator to develop a list of biometric products that satisfy TSA requirements for use in U.S. airports. TSA's approach is to qualify commercial biometric sub-systems by evaluation that includes performance testing. A biometric sub-system is comprised of biometric authentication device(s) and related enrollment stations.

TSA has developed Volume 1, Requirements Document that contains the specific quantitative performance and operational requirements, hereafter referred to as "the criteria," for qualification of a biometric sub-system. The Requirements Document is focused on the biometric sub-system portion of the airport access control function. It is directed to both the airport operators, who have interest in the Operational Requirements, and the biometric product manufacturers who have a need to understand the technical and operational system requirements needed to qualify their devices.

The purpose of this Management Plan is to outline the framework for the TSA biometric sub-system qualification program, provide information and guidelines to biometric sub-system manufacturers, system integrators and other concerned interests, and to define the documentation and processes which will be used by TSA in conducting the qualification program. This plan addresses the following topics:

a.   Qualification program overview
b.   Manufacturer application instructions and qualification data requirements
c.   Appendix A contains:
    1.   Conformity assessment program
    2.   Management of biometric sub-system qualified product list (QPL)

This plan is specific to biometric sub-systems and addresses all activities necessary to evaluate each biometric sub-system against the requirements specified in the criteria.

TSA's Test Director is responsible for developing this Management Plan as well as the Biometric Test Plan and overseeing the test program upon which the approval of biometric sub-system to be placed on a TSA QPL will be based.

The Qualification Program consists of two phases.

Phase one is the Product Pre-Qualification. Section 3 of this Management Plan defines the level, methods, test data and substantiation required from the vendors that will allow TSA to determine if the biometric sub-system is likely to meet the criteria and eligible for qualification testing.

Phase two is the conduct of qualification tests and government evaluation of the qualification data. These tests will verify selected biometric performance requirements and will be conducted by laboratories and test facilities approved by the Test Director.

2. QUALIFICATION PROGRAM OVERVIEW

This section provides a high-level description of qualification activities, organizational responsibilities, documentation, and health and safety requirements.

2.1 Purpose

The purpose/objectives of the qualification test program are to:

a. Evaluate the functional and performance capabilities of a biometric sub-system, under controlled operating conditions, against standardized technology specific criteria.
b. Provide an orderly progression of qualification test activities that are consistent, unbiased and repeatable for all biometric sub-systems submitted for TSA qualification.
c. Ensure appropriate configuration management and quality assurance controls and accurate documentation of evaluation results throughout the process.
d. Observe and document data related to operational considerations identified in the criteria.
e. Issue recommendations for placing qualified biometric sub-systems on the TSA QPL.

2.2 Applicable Documents

a. Volume 1, Chapter 1 – Technical Requirement for Biometric Sub-systems
b. Volume 1, Chapter 2 – Operational System Requirement
c. Volume 1, Chapter 3 – Required Standards
d. Volume 2 – Implementation Guidance

2.3 Qualification Activities

Specific activities performed as a part of the qualification program are depicted in Figure 1, TSA Biometric sub-system Qualification Test Program Flow, and include the following:

a. TSA release of the criteria and this Management Plan for Biometric Sub-systems Qualification Testing to qualified vendors.
b. TSA Receipt of vendor request including the qualification data package (QDP).
c. TSA review of manufacturer's documentation, and substantiation of test data.
d. TSA and test facility preparation for qualification testing.
e. Vendor installation, checkout and training.
f. Qualification test and evaluation.
g. Vendor briefing on qualification testing results and system deficiencies.
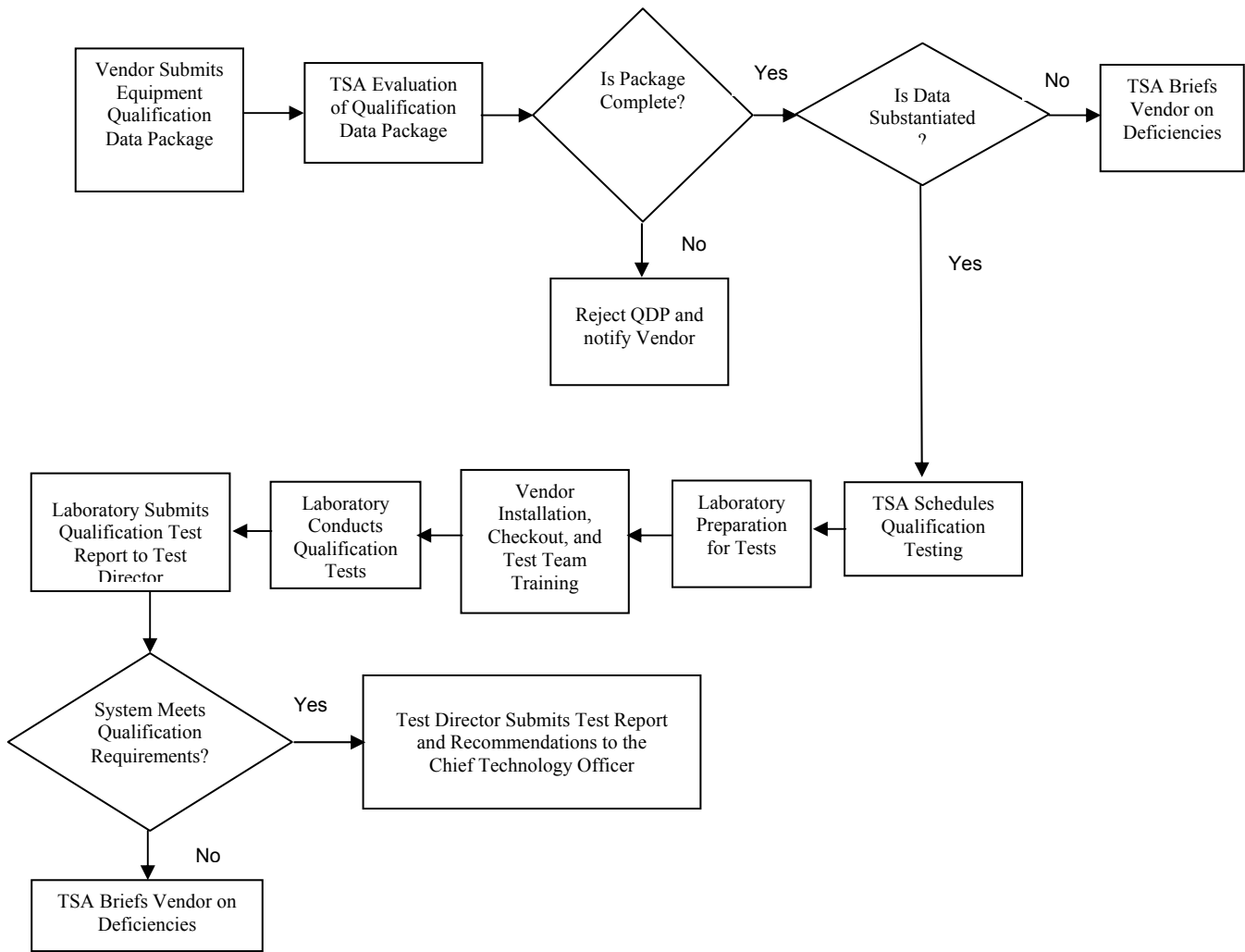h. Issuance of letter of recommendation for placing the Biometric sub-system on the QPL.

Figure 1. TSA Biometric Sub-system Qualification Test Program Flow

2.3.1 Manufacturer Request for Qualification Testing

Biometric sub-system manufacturers that plan to submit biometric sub-systems to TSA for qualification must submit an application by way of the TSA web site, requesting qualification of their biometric sub-systems. In order for the request to be processed, the manufacturer must submit a complete manufacturer technical QDP.

Vendors that plan to submit sub-systems to TSA for qualification testing must respond to and follow the instructions in the criteria and in this Management Plan. Accordingly, vendors must submit a complete QDP, or the entire QDP may be rejected as non-responsive.

When received, each request will be annotated with the time and date received. Consideration of requests will be in the order received.

If it is determined at any time during the qualification program that the biometric sub-system fails to meet the criteria, testing may be terminated and the vendor will be notified. Based on the needs of TSA, vendors may re-submit the sub-system for qualification by re-applying, submitting an updated QDP and a new or modified subsystem. The updated QDP must provide sufficient evidence that the re-submitted product will meet the criteria previously failed.

2.3.2 Evaluation of Vendor QDP

QDPs will be reviewed by TSA and evaluation reports will be prepared in the order that the data packages are received. The primary objectives of the evaluation are to ensure that the vendor has provided all data required and to verify that the vendor data substantiates that the sub-system may meet the criteria.

The biometric sub-system design will be evaluated for suitability and technical merit. Additionally, the manufacture's measurement techniques, configuration management practices, and test methodologies will be evaluated.

The primary objectives of the evaluation are to:

a.   Ensure that the manufacturer has provided all data required by the instructions;

b.   Verify that the manufacturer data provided substantiates that the biometric sub-system is likely to meet the criteria, and

c.   Verify that the manufacturer has conducted internal testing using a production or production-representative biometric sub-system. The sub-system used to develop vendor data must be representative of delivered systems and not specifically produced or selected for testing purposes.

Sufficient time is required, usually not more than seven days, to complete the review and develop a report on each data package. (Note that during the Initial QPL development in 2005, the review time may be lengthened depending upon the number of applications received.)

The QDP evaluation team will review the QDP, and a decision will be made whether to reject the QDP due to incomplete or unsubstantiated data, or to proceed with the qualification process. Substantiation and test data will be examined for sufficiency, accuracy, validity, and associated substantiation detail. The evaluation team will prepare a QDP Evaluation Report documenting the evaluation results. (Note that for the initial set of qualification applications, this process shall be used to prioritize the testing order, with the most significantly substantiated devices tested first.)

2.3.3   TSA Preparation for Qualification Testing

Once the decision to proceed with qualification testing is made, the Test Director will coordinate with the testing facilities to establish a schedule for system installation, test team training, and formal qualification testing in the order in which the QDP evaluations are completed. Technical training must be to the level that is necessary and sufficient to enable test team personnel to operate the sub-systems and to make all test measurements and analysis needed to verify that the sub-system meets the criteria.   Test team training will be completed prior to beginning the qualification testing.

2.3.4   Vendor Installation and Checkout

The vendor shall be responsible for shipment of biometric sub-systems to the designated test facilities and for performing installation, checkout and training prior to the start of formal qualification testing. One laboratory location/room will be used for enrollment purposes and another will be used for verification evaluation. The installations will be coordinated with the designated test facilities personnel.   TSA may observe installation and checkout activities performed by the vendor. Installation and checkout shall include a configuration audit witnessed or conducted by TSA, and verification that the sub-systems are calibrated and functioning properly and ready for formal qualification test. Once installed and checked out, the biometric systems must remain unaltered and secured, with tamperproof seals installed prior to the start of the qualification tests.

The vendor shall provide technical training that must be to the level that is necessary and sufficient to enable test team personnel to operate the biometric sub-system and to instruct the test team members on the use of the device and to make all test measurements and analysis needed to verify that the biometric sub-system meets the criteria. The operator training provided must be equivalent to the training planned for operational personnel who would operate and maintain the biometric sub-system.

Biometric sub-systems configuration control and problem tracking will be established and maintained throughout qualification activities beginning with submittal of the vendor QDP and vendor submittal of biometric sub-systems for evaluation at the test facilities. Hardware and software configurations of each sub-system including make, model and revision level submitted for qualification testing shall be controlled and maintained by the vendor, reported to TSA, and closely monitored by the test team during all qualification testing activities. The vendor must coordinate all configuration changes required after submittal of the QDP with the TSA Test Director for review and approval prior to implementation of any change. Configuration changes may result in rescheduling of the qualification test.

2.3.5 Qualification Test and Evaluation

Following completion of training and familiarization at the test site, the facility test team will prepare sub-system test procedures by incorporating the steps specific to each biometric sub-system into the general test procedures. Test team training and development of sub-system specific test procedures must be completed prior to beginning the qualification testing.

The test procedures will be developed utilizing the general test procedures, which will be identical for all biometric sub-systems tested (except as may be required to account for fundamental differences in biometric modalities or different test facilities).

TSA intends to require the conduct of qualification tests to evaluate the biometric capabilities under controlled operating conditions representative of an indoor airport environment. Therefore, the sub-system configuration, adjustable settings and variable parameters must reflect those expected in that environment. The manufacturer is responsible for setting the matching threshold value to be used throughout the test (based upon the technical requirements cited in the criteria). The biometric sub-systems must be stable and invariable during the conduct of the qualification tests.

The candidate subsystems will only be allowed to host one version of the biometric software program during the qualification test. Recording or logging of test events or test subjects by the biometric subsystem for vendor use will not be allowed. If recordings are made, they will be the property of the TSA and will be transferred to magnetic media or printed and purged from the biometric sub-systems upon completion of the tests.

The core tests will be conducted under controlled indoor operating conditions using live human test subjects. Additionally, the manufacturer may submit a request for outdoor testing of a device submitted for the core qualification test. Information substantiating the outdoor capability of the device, and all modifications or supplements used to accommodate outdoor environments must be provided in the QDP.

The test team will use a demographically controlled set of subjects for qualification testing of all biometric sub-systems. The manufacturer will not be allowed to be present during the qualification tests, however they will be called upon for technical and maintenance support, as required.

All biometric sub-system malfunctions or anomalies encountered during qualification test activities will be classified by type, documented and tracked. Problems will be reviewed with the vendor for disposition and corrective actions as required. Additionally, the TSA will brief the vendors concerning deficiencies that result in failure of the sub-system to meet the qualification criteria. These deficiency briefings will be conducted at two stages in the qualification process, as necessary.

The first will be conducted upon completion of TSA evaluation of the vendor documentation and test data, and the second following completion of TSA qualification tests. The TSA test results and sensitive data relative to the deficiency briefings will only be provided to vendor personnel

on a need to know basis. The details of the tests including subjects used will not be disclosed to the vendor.

Qualification testing will be terminated if the biometric sub-system malfunctions and cannot be repaired or replaced within three working days, unless the Test Director approves additional time. TSA may allow re-test or regression testing of a subsystem to verify the integrity following a repair or replacement of parts, or any software modification.

Upon completion of the test, test data and analysis results will be evaluated against the criteria and documented in the "Biometric Sub-system Qualification Test Report."

After qualification testing has been completed, the testing facility or the vendor, as determined by TSA, shall be responsible for the removal and return of sub-systems that did not meet the criteria within one week after notification from the Test Director, unless additional time has been approved by the Test Director.

TSA will notify the manufacturer of sub-systems that meet the qualification requirements.   Details of the qualification test activities are defined in Biometric Sub-System Test Plan

2.3.6   Qualification Recommendation

Each biometric sub-system that has met the criteria and has no significant operational deficiencies during the testing will be recommended by the Test Director for inclusion on the QPL. Any restrictions on use or deployment and specific constraints and controls required with respect to configuration changes to such equipment will be included in the qualification.

For biometric sub-systems that do not meet the criteria, the Test Director will report to the manufacturer on the performance deficiencies. These deficiencies must be corrected and the changes documented before a biometric sub-system can be re-submitted for qualification.

2.3.7   Qualified Products List

A listing of all qualified products (with associated restrictions) will be recorded by TSA on a QPL of Biometric Sub-systems for Airport Access Control.

2.4   Qualification Test and Evaluation Costs

Manufacturer shall pay for the costs associated with the testing, including:

a.   Established laboratory testing fee (paid directly to the testing laboratory).

b.   Shipping of equipment to and from the test facility.

c.   Assembly, set up, installation, checkout, calibration, disassembly and removal of equipment from the test facility, including any health and safety inspections, licenses and/or permits required by cognizant authorities.

d.   On-site training of test team personnel.

e.   Technical support and maintenance of equipment at the test facility.

2.5   Documentation Requirements

Vendors must abide by the requirements of the criteria regarding the format for preparation of documentation and all documentation and data must contain the required information and be presented in a manner that is clear, concise, and unambiguous. The vendors must use proprietary and SSI markings according to standard marking procedures. SSI must be handled according to 49 CFR Parts 15 and 1520. TSA has instituted procedures to safeguard proprietary data that is used during proposal and QDP evaluation.

Qualification test results will be documented by the test team including vendor data evaluation, test conduct, data recording, data reduction and analysis, and test results. This includes all documents necessary to maintain internal data integrity and to conduct, record, analyze and report the status of the qualification activities.

2.6   Qualification Program Schedules

Once the Initial QPL is developed in 2005, it is anticipated that the TSA qualification process will not exceed 107 days to complete from receipt of the QDP to final determination of qualification. (Note that this schedule assumes that the testing facility can accommodate the testing without additional scheduling delay.) This period is estimated to consist of the following:

a.   Not greater than seven calendar days for vendor documentation and test data evaluation and reporting.

b.   Not greater than 70 calendar days for vendor system installation and checkout, TSA training, and conduct of qualification test and evaluation.

c.   Not greater than 30 calendar days for data reduction, analysis, and generation of final report and recommendation.

2.7   Organizational Roles and Responsibilities

TSA will perform qualification test design and evaluation activities in consultation with the National Institute of Standards and Technology (NIST), and with the aviation and biometrics industry.

The roles and responsibilities of the TSA organizations involved in the qualification program are defined below.

2.7.1 Chief Technology Officer (CTO)

a. Develop and issue Qualification Criteria for biometric sub-systems.
b. Approve the Management Plan for Biometric sub-systems qualification tests.
c. Oversee the qualification process.
d. Issue Biometric sub-systems qualification documents and QPL.

2.7.2 Transportation Security Laboratory Test Director

a. Develop the Management Plan for Biometric sub-systems Qualification Testing.
b. Develop Test Plan for Biometric sub-systems testing.
c. Evaluate vendor QDP and prepare evaluation reports.
d. Review and approve specific test procedures for each biometric sub-system and qualification test.
e. Schedule, coordinate, and oversee biometric sub-systems qualification testing.
f. Provide TSA and support contractor personnel necessary to implement this Test Management Plan including independent witnesses of test activities.
g. Oversee the qualification test process and provide periodic status reports on progress of qualification testing of candidate systems.
h. Approve methods and oversee data reduction and analysis of test data.
i. Prepare TSA test reports and issue recommendations to CTO for placement of products on the QPL.
j. Brief vendors of biometric sub-systems that fail qualification testing.

2.7.3 Test Organizations and Facilities

a. Obtain and maintain laboratory accreditation.
b. Provide and maintain biometric sub-system testing infrastructure.
c. Develop specific test procedures for each biometric sub-system and qualification test.
d. Coordinate and conduct qualification tests.
e. Perform data reduction and analysis of test results.
f. Develop test reports and recommendations.
g. Participate in manufacturer briefings as requested by the Test Director.

2.7.4 Manufacturers

a. Apply for qualification by submitting application and QDP.
b. Provide equipment, installation and training at test facilities.
c. Certify that installed devices are functioning properly and ready to test.
d. Provide on-site service as required.
e. Pay testing fees to testing facility.

3. VENDOR INSTRUCTIONS AND QUALIFICATION DATA REQUIREMENTS

3.1 Purpose

This section specifies the qualification application preparation instructions, contents and format of the QDP, which the manufacturer must submit to TSA in order to begin the process for qualification of a biometric sub-system.

Additionally, the manufacturer may submit a request for outdoor testing of a device submitted for the core qualification test. Information substantiating the outdoor capability of the device, and all modifications or supplements used to accommodate outdoor environments must be provided in the data package.

3.2 QDP Requirements

The QDP submitted by the vendor (via the TSA web site application process) must include all material specified in the criteria and this Management Plan. This includes identification of the specific biometric sub-systems tested, associated specifications and technical documents, test plan and procedures used during the vendor and independent verification, actual test data, and analysis results as defined in the criteria. The QDP must include all information and data necessary to validate that the biometric sub-systems can meet the criteria. All documentation shall be provided to TSA in PC readable form on a CD or as specified on the web-based application process). Use of Adobe pdf file format is recommended.

The data package must address all topics identified in the Technical Requirements Document.

In addition, the QDP must include the following material:

a. Product identification information.
b. Product maturity and vendor experience indicators.
c. Product documentation.
d. Performance substantiation testing results.
e. Product cost information.
f. Reliability, maintainability and availability data.
g. Additional information (such as outdoor capability).

3.2.1 Identification of Biometric sub-systems Used to Collect Substantiation Test Data

Complete identification of the Biometric sub-systems used to collect the substantiation test data must be provided in the QDP. This includes:

a. Model number(s) of equipment tested.
b. Serial number(s) of equipment tested.
c. Software version(s).
d. Firmware version(s), if applicable.
e. An inventory of hardware configuration items (CIs), software CIs and firmware CIs with configuration identification data.

f.   Identification of all variable and adjustable parameters and adaptation data used to tailor or tune the system as well as their settings and values. Adaptation data refers to variables used to configure or adjust the system to specific environments or uses.

3.2.2   Biometric Product Maturity and Experience Indicators

Product line and specific model within the product line information must be provided that identifies the level of maturity of the product and the manufacturer's experience with this product. Information provided shall include (but not be limited to):

a.   Number of model and current version produced to date.
b.   Period of production of model and product line.
c.   Number of units deployed – this product line.
d.   Number of units deployed – this model.
e.   Largest single site deployment size.
f.   Example of deployment most similar to airport access control.
g.   Information regarding experience integrating this model with legacy access control systems.

3.2.3. Biometric Product Technical Documentation

The manufacturer must provide existing deliverable documentation that would be provided to airports purchasing this sub-system.

A sub-system description must be included which provides a description of the technology(s) and the sensing method(s), the matching algorithm concept, the enrollment template size and characteristics, and the operating system software and firmware. The environmental limits, reliability, maintainability, and availability (RMA), safety, logistics, and computer human interface (CHI) requirements of the biometric sub-system must be included.

Specifications shall include all functional and performance capabilities of the biometric sub-system. Details regarding the capability and flexibility to interface to access control systems must be provided.

A sub-system design overview document may be provided in order to clearly describe the overall sub-system design and functionality.

Instruction manuals, operations manuals, training manuals and other engineering documents must be included to assist the TSA in its evaluation of the equipment.

3.2.4   Test and Evaluation Data

The vendor must submit a QDP that contains all test data specified in the Criteria and this Management Plan. This includes all data that the vendor used to verify that the biometric sub-systems meet the criteria.

Vendors must conduct tests using the parameters listed in the corresponding section of the criteria. Vendors must supply all test data in the appropriate level of detail and format. In cases where

substantiation from an independent/accredited third party source is provided, test data must be provided with a similar level of detail.

Test data must include the results of quantitative tests including biometric matching error rates, failure to enroll (FTE) rate, and transaction times; reliability/availability requirements; power/physical requirements and interface to existing access control systems.

All FTE and matching error rate data must be identified in terms of the threshold parameter settings, and the relationship of that setting to the threshold value that will be used for TSA qualification testing.

This data should include error rate data from a large sample of actual human test subjects. Additionally, any other data that substantiates the fact that the biometric sub-system meets the criteria should be included.

Test data may be obtained from various sources including:

a.   Technology tests (such as the NIST's FRVT).
b.   Scenario tests such as third party commercial product evaluations.
c.   Vendor in-house controlled environment tests.
d.   Operational tests at functional installations.
e.   Outdoor tests (required if applying for outdoor qualification).

In addition to testing data and results, the manufacturer shall include detailed information describing the testing methodology and conditions.

TSA recognizes that manufacturers may not have conducted, or have the capabilities to fully test their biometric sub-system(s) at its internal facilities and therefore may rely on testing/analysis conducted by third parties to substantiate their claims. In this event, the manufacturer must submit Certificates of Compliance (CoC) and third party data that will substantiate performance claims. These may include component quality design data, sensor capabilities, analyses, reports and any other relevant data that demonstrates product quality and performance. All such supporting data shall be included in sufficient detail to enable evaluation of the validity of the claims.

3.2.5   Test Configuration(s)

The vendor must define the specific test configuration(s) used to collect QDP test data, including all hardware, software, firmware, and test equipment utilized. Variable parameter settings and site adaptation data must also be provided. Configuration documentation and data must be associated with specific biometric sub-systems configurations used during the vendor's and third party testing. The system configuration inventory must be reported at the configuration item level.

TSA anticipates that there may be cases where the configuration of the system(s) and components used to collect the vendor data submitted in the QDP differs from the configuration of the system and components that will be submitted for qualification tests. In these cases, two system inventories must be provided, one identifying the configuration of the data collection

system(s) and one identifying the configuration of the system to be submitted for qualification tests. The difference between these configurations must be made evident and the vendor must describe the impact of the differences on the ability of the system to meet the criteria. Significant differences between configurations and significant impact on the system design, performance or capabilities may result in rejection of the vendor data package.

3.2.6   Test Plan and Procedures

The vendor must submit the test plan and procedures that defines the vendor's approach, strategy and T&E activities performed. The test plan and procedures shall include, but not be limited to the following:

a.   Brief description of each test including the descriptive title, subjects used, test objectives, test approach, test conditions, threshold settings and specific test configuration(s);
b.   List of test equipment and tools required for each test and calibration requirements;
c.   Test subject descriptions, including total number of subjects, characteristics of test subjects and any other data relevant to the specific test;
d.   Rationale for test subject selection and preparation methods;
e.   Data analysis approach and methods and calculations used;
f.   Requirements traceability matrix, which relates specific tests to the elements of the criteria and the method of verification. Acceptable verification methods include test, demonstration, inspection, and analysis. The preferred verification method is "test."
g.   Where verification methods other than test are used, the vendor must provide comprehensive definitions and descriptions of the methods used.

3.2.7   Test Report

The vendor must provide a test report that contains, as a minimum, the following information:

a.   Identification of the sub-system(s) tested.
b.   Identification of associated test plan and procedure(s).
c.   System calibration results including calibration procedures.
d.   Descriptions and listing of all data collected during the test including manually recorded and electronic or computer generated outputs.
e.   Any deviations from the test plan or procedure(s), anomalies observed during testing, or other problems encountered and their potential effect.
f.   Summary of results and conclusions.

Test reports containing data on FAR and FRR, and countermeasures are sensitive and must be identified and handled accordingly.

3.2.8.   Reliability, Maintainability and Availability (RMA) Data

The manufacturer must provide RMA and supportability data for the biometric sub-system submitted for qualification. Information pertaining to any redundancy provided by the hardware, software, and/or interfaces must be included. RMA data must be provided for the overall biometric

sub-system and for all line replaceable units of the biometric sub-system including routine/preventative maintenance requirements and corrective maintenance required. Supportability data must include logistics, training, and operational support requirements. If validated RMA and supportability data is not available, preliminary data or estimates and analysis must be provided, including substantiation data or rationale.

3.2.9. Biometric Device Producibility

The manufacturer shall provide production rate and schedule information, to include current lead time(s), specifically identifying minimum, sustainable and maximum production levels.

3.2.10. Additional Information

The manufacturer should provide other information not previously required in the paragraphs above, which will aid TSA in determining the readiness and suitability of the product for qualification testing. This additional information may include, but is not limited to:

a. Information regarding data protection and privacy.
b. Information regarding interoperability with other sub-systems:
    1. Interoperability across products within manufacturer.
    2. Interoperability across other manufacturers, if data is available.
c. Information regarding experience integrating with legacy access control systems.
d. Statement of conformance with Biometric Standards (see Vol. 1, Chapter 3).
e. Status of evaluation/testing of sub-system security (Common Criteria, NIAP, etc.).

APPENDIX A - CONFORMITY ASSESSMENT PROGRAM

1. OVERVIEW

This Appendix provides a Biometric Sub-system Conformity Assessment Program Outline, which can be developed into a more complete and detailed program definition at a future date.

2. PURPOSE

The purpose of a Conformity Assessment Program is to enhance the confidence that biometric access control equipment used for airport security applications meet and continue to meet performance and technical requirements.

3. ASPECTS OF TECHNICAL REQUIREMENTS

For the purpose of this section, the following numbered outline of the different aspects of biometric sub-system level evaluation will be adopted to clarify the conformity processes that apply to each aspect. The five aspects are:

a.   Performance
b.   Conformance to standards (biometric, EMC, vibration and bump)
c.   Safety (including basic performance, environment of use and emergency egress)
d.   Information security
e.   Interoperability

4. QUALIFICATION PROGRAM ELEMENTS FOR EACH ASPECT

4.1 Aspect 1 – Performance

Certification program consisting of:
- Type testing by third party laboratory (see note 1)
- Product conformity decision by TSA (based on report from third party lab)
- Attestation of conformity by TSA via Qualified Products List (QPL)
- Factory surveillance via assessment/audit of manufacturers required biometric performance and software quality management system (**requirements in development**)
- (see note 2) conducted in conjunction with third party quality management system (see note 3) registration/certification by a registrar accredited by a recognized accreditation organization.

Note 1 – Third party laboratories for conducting biometric performance testing will:
- In the short term, declare their compliance with ISO/IEC 17025, General Requirements for the Competence of Calibration and Testing Laboratories, and their competence to conduct biometric performance testing to and in accordance with specified performance testing and reporting standards (see Volume 1, Chapter 3).
- In the long term be accredited to ISO/IEC 17025 and specific requirements for laboratories conducting biometric performance testing (**to be developed**) by recognized laboratory

accreditation organization such as the National Institute of Standards and Technology (NIST), National Voluntary Laboratory Accreditation Program (NVLAP).

Note 2 – Biometric performance and software quality management plan surveillance to include:
(1) Assessment to determine manufacturer has a quality management plan to meet the requirements of the biometric performance and software quality management requirements including, but not limited to:

- capability of producing compliant products
- necessary equipment and competence to test/calibrate each unit where applicable
- calibration system for necessary test equipment, has system for quarantining, reworking and/or scrapping non-compliant products where applicable
- has an adequate quality management system for software revisions and

(2) Periodic audits to:

- ensure that equipment being manufactured and distributed as qualified products are represented by type tested units that were found to comply
- witness baseline human verification performance tests to ensure ongoing compliance and performance of qualified products (protocol to be developed) where applicable
- audit manufacturers biometric performance and software quality management system implementation to ensure that minor software revisions are adequately designed, validated, documented and implemented and that major software revisions are type tested (guidance to be developed to identify major vs. minor revisions)

Note 3 – The biometric performance and software quality management plan may be part of a broader quality management system. When a third party registration is used to demonstrate conformity with this requirement the scope of registration must include the required elements of the biometric performance and software quality management system. The third party registrar must provide the results of assessments and audits that pertain to the software quality management plan and its implementation directly to TSA not more than 30 days after each assessment and/or audit is conducted. The software quality management plan must be submitted with the QPL application to TSA for assessment.

4.2 Aspect 2 - Conformance to Standards

Formal supplier's declaration of conformity (see note 4) in accordance with ISO/IEC 17050-1, Supplier's Declaration of Conformity – Part 1: General Requirements and supported by a technical file in accordance with ISO/IEC 17050-2, Supplier's Declaration of Conformity – Part 2: Supporting Documentation. For example, test data to support the declaration for EMC, vibration, and bump shall be conducted by an accredited third party laboratory.

Note 4 - Third party laboratories for conducting biometric standards conformance testing will:

- In the short term, declare their compliance with ISO/IEC 17025 and their competence to conduct biometric standards conformance testing to specified standards.
- In the mid term successfully participate in round robin proficiency testing programs if and when established and coordinated by organizations such as NIST.

- In the long term be accredited to ISO/IEC 17025, General Requirements for the Competence of Calibration and Testing Laboratories, and specific requirements for laboratories conducting biometric conformance testing (**to be developed**) by a recognized accreditation organization.

4.3 Aspect 3 – Safety

Certification by a Nationally Recognized Testing Laboratory (NRTL) whose scope of accreditation includes appropriate safety standard(s).

4.4 Aspect 4 – Information Security

Formal supplier's declaration of conformity in accordance with ISO/IEC 17050-1 and supported by a technical file in accordance with ISO/IEC 17050-2.

4.5 Aspect 5 – Interoperability

Reserved for future use.

5. MANAGEMENT OF BIOMETRIC SUB-SYSTEM QUALIFIED PRODUCTS LIST

5.1 Overview

This Section provides an outline of the plan for TSA to manage the QPL, which will be developed into a complete process at a future time.

TSA will manage the content and distribution of the Qualified Products List (QPL) and the supporting policies and processes.

5.2 QPL Content

The QPL will contain basic qualification information and supplemental information. Basic information includes:

a.   Detailed product and manufacturer identification
b.   Qualification date, facility

Supplemental information includes:

a.   Outdoor suitability claims.
b.   Outdoor suitability testing results.
c.   Operability testing findings.
d.   Standards conformance information.
.

Information contained in this QPL will be <u>objective</u> information only.

VOLUME 3 – PLAN FOR BIOMETRIC QUALIFIED PRODUCTS LIST (QPL)

CHAPTER 2

TEST PLAN
For
Biometric Sub-System

30 September 2005

EXECUTIVE SUMMARY

Section 4011(a)(5) of the Intelligence Reform and Terrorism Prevention Act of 2004, which was signed into law by President Bush on December 17, 2004, requires the Assistant Secretary of Homeland Security (Transportation Security Administration [TSA]), in consultation with representatives of the aviation industry, biometrics identifier industry, and the National Institute of Standards and Technology, to issue guidance by March 31, 2005, for the use of biometrics in airport access control systems (ACSs). This guidance should:

a.   Establish comprehensive technical and operational system requirements and performance standards.
b.   Establish a list of products and vendors that meet such requirements and standards.
c.   Establish procedures for implementing biometric systems:
      1.   To ensure that individuals do not use an assumed identity to enroll.
      2.   To resolve failures to enroll, false matches, and false non-matches.
d.   Establish best practices for incorporating biometric technology into airport ACSs.

This test plan lays out the requirements for test planning, and the technical, performance, and demographic characteristics of the test process. The test organization will use the test plan to generate performance information to allow TSA to qualify biometric products for airport access control, resulting in a Qualified Products List of biometric sub-systems and their manufacturers.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

ACS	Access Control System
CFR	Code of Federal Regulations
DHS	Department of Homeland Security
DOT	Department of Transportation
DR&A	Data Reduction and Analysis
EER	Equal Error Rate
FAR	False Accept Rate
FIPS	Federal Information Processing Standard
FRR	False Reject Rate
FTA	Failure to Acquire Rate
FTE	Failure to Enroll Rate
ID	Identification
IEC	International Electrotechnical Commission
INCITS	International Committee for Information Technology Standards
ISO	International Organization for Standardization
JTC	Joint Technical Committee
NPL	National Physical Laboratory (Middlesex, England)
PC	Personal Computer
PDA	Personal Digital Assistant
PRESS	Program for Rate Estimation and Statistical Summaries
QA	Quality Assurance
QPL	Qualified Products List
RTCA	Radio Technical Commission for Aeronautics
SC	Subcommittee
SQL	Structured Query Language
TSA	Transportation Security Administration
TSL	Transportation Security Laboratory
TT_V	Transaction Time at Verification
TWIC	Transportation Worker Identification Credential

1. INTRODUCTION

1.1   Background

In conformance with Section 4011(a)(5) of the Intelligence Reform and Terrorism Prevention Act of 2004, the Transportation Security Administration (TSA) plans to compile a list of biometric sub-systems and their manufacturers (Qualified Products List [QPL]) that meet requirements and standards established by TSA and are available for use in airport access control systems. Airport operators are currently required to have access control restrictions in place. Current TSA regulations require the delineation of secured areas and methods to control entry into the secured area via ACSs that:

a.   Ensure that only those individuals authorized to have unescorted access to the secured area are able to gain unescorted entry.
b.   Ensure that an individual is immediately denied entry to a secured area when that person's access authority for that area is withdrawn.
c.   Provide a means to differentiate between individuals authorized to have access to an entire secured area and individuals authorized access to only a particular portion of a secured area.
d.   Take measures to perform the required access control functions and procedures to control movement within the secured area, including identification media (see 49 CFR 1542.103 and 1542, Subchapter C).

Congress has recognized that biometric technologies are a sound method of restricting access to secured areas. TSA is aware that some airport operators may be unwilling to implement biometric secured areas because TSA has not yet identified technologies that it believes perform acceptably. The QPL is designed to provide that information. Airport operators may choose to upgrade their existing ACSs by purchasing and using the technologies to be listed on the QPL.

1.2   Purpose

The purpose of this document is to define specific activities that will be performed during qualification testing of biometric sub-systems on which the QPL is based. Details of the specific activities are discussed in this test plan and in section 2.3 of the Management Plan. These activities encompass formal qualification testing that begins following the successful completion of the manufacturer data package evaluation.

1.3   Goal and Scope

The goal of the test plan is to provide an independent, unbiased qualification of the production biometric component (or sub-system) of an airport ACS. The scope of the test plan is to evaluate each biometric device at the biometric sub-system level, treating it as a "black box," while providing required inputs and grading the resultant output. System access control functions are considered to be external and outside the scope of this test.

2. REFERENCES

The following documents provide information related to biometric sub-system testing requirements or best practices. The standards to which the test facility must conform are identified in Volume 1, Chapter 3, Required Standards.

a.   INCITS/M1-04-0570, "Project INCITS 1602-D Part 3: Scenario Testing and Reporting."
b.   ISO/IEC 17025, "General Requirements for the Competence of Testing and Calibration Laboratories."
c.   ISO/IEC JTC1/SC37 N684, Text of CD 19795-1, "Biometric Performance Testing and Reporting - Part 1: Principles and Framework."
d.   ISO/IEC JTC1/SC37 N683, 2nd working draft 19795-2, "Biometric Performance Testing and Reporting - Part 2: Testing Methodologies."
e.   RTCA DO 230a, "Standards for Airport Security Access Control Systems."
f.   "Best Practices in Testing and Reporting Performance of Biometric Devices," Version 2.01 NPL Report CMSC 14/02.

3. QUALIFICATION TESTING

3.1   Philosophy

The goal of biometric sub-system testing is to ensure that the technical and operational performance of every biometric product is evaluated fairly and accurately against the qualification criteria. Core testing will be performed in a consistent, unbiased manner under controlled and representative (indoor) operating conditions. Test controls will be applied to ensure reproducible test results to the extent possible (considering the use of human test subjects). To accomplish this, every candidate biometric sub-system will be tested in accordance with the same general test protocol. The general test protocol was developed under the guidelines established in this test plan.

To facilitate the testing of a specific biometric product, a unique biometric product test procedure will be developed. It will be identical to the general procedure with the exception of additional information that may be required to operate the particular biometric subsystem. This specific biometric product test procedure will be developed by the TSA qualification test team upon completion of system familiarization at the test facility.

In the actual airport application, these biometric devices will be used to verify the identity of the end user. But in the context of testing these products, the identity verification of crew members used for testing will be limited to verification of their "assigned identity", that is the identifier (e.g. crew id number or code) that uniquely identifies that crew member. This provides anonymity of the data collected and enhances the privacy aspects of the testing. Throughout this plan, identity verification refers to this crew member's assigned identity rather than their true identity.

3.2   Methodology

The type of testing performed will be controlled scenario performance tests of biometric sub-systems for access control. A "core test" is established as a minimum required test suite. Options for additional tests are also defined.

There are two environmental conditions under which devices may be tested: airport indoor (controlled with little to no variance in conditions) and (optional) airport outdoor (variance in conditions commensurate with typical outdoor usage).

TSA's specific core test type and environmental parameters for performance testing of biometric devices for airport access control will be the indoor setting that includes controlled environmental conditions. Optional tests (manufacturer's option) include the capture of test metrics outdoors under either real or simulated conditions. This is explained more fully in section 4.3.2, Operational Environment.

Since the indoor test is the core test upon which the manufacturer's qualification will be based, the outdoor test is optional and mainly for informational purposes. The results of the outdoor test will be reported, but a manufacturer whose biometric device qualifies indoors will not be disqualified by the results of potential subsequent outdoor test participation with the same device. The measurements of outdoor device performance encompass both performance and operability issues. Performance issues include failure rate metrics. Operability issues cover individual end-user interaction with the biometric identification device.

The core test consists of three sets of measurements taken indoors under controlled conditions:

a.   Enrollment Metrics, in which the crew member's identity and relationship to his/her personal biometric is established, obtained, and stored (or capable of being stored) externally to the biometric device. This process also includes same day enrollment verification. The biometric verification results will be available to the enrollment operator in near real time to confirm enrollment success. The metric for this measurement is the Failure to Enroll (FTE) rate.
b.   Biometric Verification Metrics, in which the identity is re-established after enrollment by verifying the identified biometric template against the real time biometric sample. Here, the capture (by the test facility data collection method) of the associated false accept rate (FAR) and the false reject rate (FRR) is used to determine the accuracy of the biometric device. Three revisit sessions with 5 genuine verification transactions and 5 imposter verification attempts will be made by each crew member. Data from transactions (up to 3 attempts) will be captured. The metric for this measurement is the FRR (False Reject Rate) value and a corresponding FAR (False Accept Rate).
c.   Transaction Time Metrics, in which the transaction time is the period required from the crew member's claim of identity to the reporting of the result of the biometric verification process.

To better assess operational issues and for laboratory utilization logistics, the specific manufacturer device used for enrollment must be separate from the device used for verification.

3.3   Determination of Test Completion

Core testing consists of exercising the enrollment and verification processes of biometric sub-systems using a test crew representative of airport employees. For a given production biometric sub-system, test completion is defined as the point where the entire test crew has completed their run-through of enrollment, verification of enrollment, and, several days/weeks later, repeated the verification process. For the optional outdoor tests, the entire outdoor test crew performs the verification process repeatedly within the optional environment. This completes the operational portion of the test. Test data are then analyzed; qualification decisions are reached; an out-briefing between TSA, the manufacturer, and test facility experimenters is completed; and the results are reported to TSA. The test sequence is now complete.

3.4   Success Criteria

This test plan will be considered successful if through its execution, stakeholders receive high quality, independent, unbiased decision support information regarding the qualification and other characteristics of the production biometric component suitable for use as part of an airport ACS.

3.5   Test Boundaries

Although the "Intelligence Reform and Terrorism Prevention Act of 2004" addresses broad transportation security issues, this test plan addresses only performance testing of biometric devices intended for airport access control. Access controls and the associated policies that they enforce are considered to be outside of the boundaries of this performance test.   Other characteristics not tested by this plan include:

a.   Device safety (Underwriters Laboratories [UL] or other certification).
b.   Conformance to biometrics standards.
c.   Information security.
d.   Device interoperability.
e.   Reliability, maintainability, and availability.

3.6   Relationship of Biometric Device/Subsystem to Access Control System

Figure 1 illustrates component and information flow in an ACS that includes a biometric device.

KEY: A - Any form of machine-readable credential (airport ID, TWIC, proximity card) presented by the user to the ID reader to claim an identity.

B - User identity code (ID number, card number, ACS ID) read from the token by the ID reader and sent to the panel for the ACS to determine access privilege (part of typical legacy ACS).

C - Electrical signal from the panel used to command the door electromechanical locking mechanisms. This path may also include other signals such as door-open indicators, emergency lock override, etc. (part of typical legacy ACS).

D - (Physically) communication channel (Ethernet, RS485, etc.) enabling data interchange between the panel and ACS processor and database. (Logically) depends on site-specific implementation and includes user identity code from panel and user access authorization from ACS processor.

E - Body part or human behavior presented by the applicant to the biometric sensor during enrollment (e.g., fingerprint, iris, voice, signature). This function may also include interactions between applicant and sensor, i.e., indicator lights, audio cues.

F - Biometric template data from enrollment database to biometric processor for implementations using server-stored templates. (This flow is architecture-specific, may be per user transaction or periodic pre-loads.)

G - Y/N indication (electrical signal or message) from biometric processor to panel conveying the result of the user verification transaction.

H - User identity code (ID number, card number, ACS ID) read from the token by the ID reader and sent to the biometric processor as claim of identity (also includes user template data for template on card architectures).

I - Body part or human behavior presented to the biometric sensor during an access transaction (e.g., fingerprint, iris, voice, signature). This may also include interactions between applicant and sensor such as indicator lights or audio cues.

J - Applicant-supplied information (name, address, etc.) obtained during ACS enrollment via the ACS processor (part of typical legacy ACS).

Figure 1. Relationship of Biometric Device/Subsystem to Access Control System

3.7   Privacy

In accordance with TSA policy and Public Law, all necessary steps shall be taken to protect the privacy of the test crew members.

3.7.1   Privacy Impact Assessment

The TSA plans to develop and publish, with support from the DHS Privacy Office, a Privacy Impact Assessment. In accordance with TSA policy, Public Law, and the Privacy Impact Assessment, the Qualification Test will be conducted to ensure that the crew identity and all biometric data collected are protected from misuse. All necessary steps will be taken to protect the privacy of test crew members.

3.7.2   Data Protection

All technical measures and operational procedures will be aligned with federal law and DHS policy to provide information security strategy, technology and process documentation, management and operational policies, and application rules.

These measures will be applied to communications between component systems, interfaces between component systems and external systems. A periodic assessment of technical, administrative and managerial controls to enhance data integrity and accountability may be required.

Where possible, the biometric and other personal information will be collected directly from the individuals and the biometrics will only be used for the intended purpose of the collection. Information will only be collected that is relevant and necessary to the program. The data will be shared with and secured by authorized personnel who have a need to know the information for the purpose of performing their duties associated with the purpose of the collection. The individual will be notified of the purpose, use and possible effects of the collection of his or her personal information. The collecting agent will identify, evaluate and comply with all applicable Federal privacy laws and regulations and it's own privacy policies. The collecting agent will ensure that all personnel handling personal data will receive the proper training on the laws, regulations and policies governing privacy. Privacy policies will be communicated to the public and respond to public concerns or complaints about privacy.

NOTE: The specific methods for protection of data will vary somewhat between different organizations and will resemble the following description of data protection techniques.

Upon receipt of biometric data, the test organization will place the data on a server that is dedicated for the test. This server will be located in an office secured with a cipher lock that is also dedicated to the test projects. Only selected members involved in the test projects will have the combination to the lock. The server itself will have a lock that prevents any unauthorized person from opening the server and removing a hard drive. The key for the server will be kept in a locked file cabinet in another office. The test server will not be remotely accessible, for example through the Internet.

The server operating system will have a lock feature. A user will not be able to access the computer unless he/she first unlocks the computer by supplying a user name and password. The server will automatically lock if it is not used for more than 5 minutes. Users will be required to lock the computer manually when they are not using the system. In addition, the computers/server must have a password-protected screensaver set.

For the test, an SQL-based server database will exist on the server, with a defined list of users who have access to it. Only certain TSA and test organization personnel who have authorization to access and manipulate data will be on the list for the test database. Another level of security can be placed on any individual database table (optional). This would be used if there were tables that only a subset of authorized personnel was permitted to see.

4. TEST REQUIREMENTS

4.1 Planning

The activities described in this section will be performed to ensure that access control device evaluations are efficient, expedient, unbiased, and reliable.

4.1.1 Test Type

The testing described in this document is known as controlled <u>Scenario</u> testing. The following descriptions are provided for perspective. Fundamentally, there are three types of biometric tests: Technology, Scenario, and Operational:

a.   Technology Testing - Designed to evaluate one or more biometric algorithms for enrollment and matching performance. Technology test planning is contingent on the type of data an examiner wishes to generate. Testing of all algorithms is carried out on a standardized corpus. Nonetheless, performance against this corpus will depend on both the environment and the population in which it was collected. This factor will often be used to create a test corpus that is neither too difficult nor too easy for the algorithms to be tested. Although example data may be distributed for developmental or tuning purposes prior to the test, the actual testing needs to be done on data that has not previously been seen by algorithm developers. Testing is carried out using offline processing of the data. Because the corpus is fixed, the results of technology tests are repeatable.

b.   Scenario Testing - Carried out in an environment that models a real-world target application of interest. Each tested system will have its own acquisition sensor and 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 using the same policies. 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 and the variables associated with crew selection can be carefully controlled.

c.   Operational Testing - Typically designed to measure or predict the performance of a fielded system. Operational systems to be evaluated may have already been fielded or may be fielded for the purpose of validation through performance testing. Operational test planning is directed by the type of performance information a test organization wishes to collect and is constrained by elements of the operational environment that cannot be altered for testing.

For TSA's core test of biometric devices, the Controlled Environment Scenario Test configuration (see b. above) will be used, reducing the number of variables and resulting in improved test repeatability and increased reliability for product performance comparisons.

4.1.2   Test Objectives

Test objectives are to quantify the performance of a biometric component of an ACS, at a specified operating point, in a controlled environment scenario that is not modality-specific or biased.

4.1.3   Inputs to and Outputs from the Test Process

Volume 1, Chapter 1 of this guidance package, provides biometric sub-system requirements for testing as input to the test process. Described within this document, TSA has provided input guidance as to the goals and objectives for test. In addition, manufacturers will be providing their biometric devices, processes, and documentation as test input.

For test output, the test facility will report to TSA test findings and substantiating data. Additional outputs will consist of detailed data summaries and a manufacturer out briefing where results and discussions will be available to the biometric device manufacturer. The TSA will then produce a QPL based upon test results.

4.1.4   Concept of Operations

The operation will use an accredited testing organization/facility to conduct controlled scenario performance testing of production biometric devices that are intended for access control to provide an unbiased accurate measure of device performance. Based on these test results and the quantitative performance requirements established by TSA, a QPL will be developed and maintained by TSA.

NOTE: For the initial QPL, the testing facilities will be used prior to completion of the accreditation process due to the urgency of completing the list.

TSA-authorized biometric device test facilities are required to maintain a continuous capability for testing and evaluating biometric subsystems and reporting the results to TSA. Using these results, TSA will update the QPL and make it available on a Web site (yet to be developed).

TSA will establish a biometric product application program to pre-qualify biometric sub-systems to be tested. The pre-qualification process requires that the biometric product manufacturer submit a qualification application, through the Web, to TSA. The qualification application requires that certain information be provided to TSA by the manufacturer, as detailed in section 3 of the Management Plan.

As a part of the pretest application process, manufacturers are required to provide device operating manuals and describe how they intend to train test facility administrators and operators. It is also the manufacturer's responsibility to ensure that adequate training will be provided to test facility staff prior to actual testing.

4.1.4.1   Device Administrator Operating Manual Requirements

In order to operate the manufacturer's biometric device, the minimum training topics that must be covered to instruct device administrators include:

a.   An overview of the principles and operation of the biometric device.
b.   Device installation procedures.
c.   Operator skills required for successful device operations.
d.   Device start-up procedures, normal operating procedures, human interface procedures, and shutdown procedures.
e.   Device error code and exception response activities.
f.   Device tear down procedures.

4.1.4.2   Operating Manual Requirements

Minimum training topics that must be covered to train device operators include:

a.   An overview of the principles and operation of the biometric device.
b.   Operator skills required for successful device operations.
c.   Device start-up procedures, normal operating procedures, human interface procedures, and shutdown procedures.
d.   Device error code and exception response activities.

4.1.4.3   Test Schedule Milestones

When the test pre-qualification phase has been completed, a test schedule will be developed to accommodate the availability of the manufacturer and facility resources.   The schedule milestones will include:

a.   Biometric device delivery to the test organization.
b.   Biometric device installation and integration with the facility test and evaluation network.
c.   Biometric device training of operators.
d.   A preliminary period of biometric device operation and debugging. It is the manufacture's responsibility to adjust their biometric sub-system for operational testing.
e.   Certification by the manufacturer that its biometric device is ready for test.
f.   Period for crew member habituation.
g.   Commencement of core testing with the biometric enrollment of the crew and the collection of enrollment data, time trials, and statistics.
h.   Continuation of core tests, including biometric verification testing of both genuine and imposter crew member biometric-identity pair submissions.   This work includes the determination of the associated FRR and FAR statistics for transactions.   Transaction time data will also be collected.
i.   Optional outdoor testing to obtain biometric verification data as described above.
j.   Analysis of the data and the assessment of qualification.
k.   Validation of test results and an out-briefing with the manufacturer.
l.   Results reported to TSA.
m.   Tear down and removal of manufacturer biometric devices.

4.2 Multi-Biometric Qualification

This section addresses TSA's position on the qualification and use of multiple biometric sub-systems in combination to qualify for the QPL for airports. "Multiple biometric sub-systems" means two otherwise independent biometric sub-systems, which, when used together, may be able to qualify, even if one or both of the sub-systems may not be able to qualify alone. This does not include production products that may exist that use multi-biometric techniques to improve their performance.

4.2.1 Analysis

When posed with the question, "Can combinations of two (or more) biometric devices be used together to constitute a qualified product?" TSA analysis determined that it would be inappropriate to reject this concept. For example, two relatively inexpensive biometric devices, combined together using sound fusion techniques, may provide an affordable solution that is fully capable of meeting all qualification requirements. Integration of these devices could be performed by systems integrators for solutions specific to an airport client. It would not be in the best interest of the government, airports, or the vendors to disallow such a qualification.

Allowing combinations of products complicates the pre-qualification and qualification performance testing aspects of this process. For a single product to pass the pre-qualification criteria, its performance must show promise of passing the performance criteria. However, determination of the expectation of the combination of two products is more difficult to evaluate.

4.2.2 Black Box Approach

For testing purposes, the combination of two products is treated as one entity. Testing plans, protocols, and evaluation processes are unaltered. To qualify, the combination must be time-efficient and achieve the transit time metric, which may be more difficult than for a single product. The determination of which products are combined is the responsibility of the vendors.

4.3 General Test Approach

This section defines the general approach and standard practices for the conduct of all biometric device qualification testing. Specific areas include configuration management practices, operational environment control, system calibration and threshold verification, test article selection, pretest activities, data collection, problem reporting, and posttest activities.

4.3.1 Configuration Management

Biometric sub-system configuration will be established during a configuration audit prior to the start of testing. At this time, quality assurance (QA) test team personnel will identify and record version and serial numbers of applicable hardware, software, and line replaceable units, including diagnostic and maintenance tools. Data collected during the configuration audit will be recorded on a Configuration Log Input Form (Appendix A).

System configuration will be strictly controlled throughout biometric device qualification testing. To aid in this control, QA seals will be placed in appropriate locations on each biometric device during the configuration audit. Should there be a need to make a change to the system configuration or access a sealed area due to equipment failure or maintenance, the Test Manager and the QA representative must be notified and the appropriate information recorded in the configuration log. The information recorded in the log must indicate the reason for accessing the area, details of any configuration changes made, the responsible individual, and the date and time. All entries into the configuration log must be approved by the Test Manager. If changes are made to the system configuration, the Test Manager reserves the right to perform regression testing to verify that system performance has not been affected.

4.3.2   Operational Environment

The primary objective of the core qualification test is to evaluate biometric device performance under controlled indoor operating conditions. A test environment will be created to ensure that there are no factors, such as external interference or emissions that will adversely affect the outcome of a test.

Optional outdoor testing may also be conducted under specified ranges of environmental conditions determined to be representative of outdoor conditions at airports.

Since the indoor test is the core test upon which the manufacturer's qualification will be based, the outdoor test is optional and mainly for informational purposes. A manufacturer whose biometric device qualifies indoors will not lose the qualification based on the results of subsequent outdoor test results for the same device. The manufacturer may choose to provide identical or different (but functionally identical) devices for these tests. For example, the manufacturer might provide Device A for the core indoor test and then test Device A again for the optional outdoor test. The manufacturer may also choose to modify Device A for the outdoors or provide a separate Device B for optional testing outdoors. For example, the manufacturer may provide an environmental housing or even an enclosed booth to house the device. Enrollment will only be performed on the core test enrollment station (i.e., if an outdoor device, B, is offered for optional testing outdoors, it must be compatible with enrollment with device A).

The measurements of outdoor device performance encompass both performance and operability issues. Performance issues include failure rate metrics. Operability issues cover the effects of environmental factors on the availability and reliability of the biometric devices as well as the individual end user interaction with the biometric identification device. The following subsections describe the three representative environmental categories upon which outdoor testing will be based. These conditions are not meant to duplicate or replicate all possible environmental conditions, but rather are indicative of how well the biometric devices will perform in these specific outdoor conditions.

4.3.2.1   Outdoor Hot/Wet

Representative of tropical areas of the United States, optional outdoor tests will take place under hot, humid, and wet conditions. These conditions will be provided through actual location

testing or through simulated conditions within an environmental chamber. Typical test characteristics are provided in Table 1.

Table 1. Test Characteristics – Outdoor Hot/Wet

Condition	Tested Value
Temperature	Above 80 degrees F
Humidity	Above 60%
Precipitation	Falling rain for 40 to 60% of the test trials
Wind	0 to 40 miles per hour

4.3.2.2   Outdoor Hot/Dry

Representative of desert-like areas of the United States, optional outdoor tests will take place under hot, dry conditions. These conditions will be provided through actual location testing or through simulated conditions within an environmental chamber. Typical test characteristics are provided in Table 2.

Table 2. Test Characteristics – Outdoor Hot/Dry

Condition	Tested Value
Temperature	Above 80 degrees F
Humidity	Below 60%
Precipitation	Blowing sand for 40 to 60% of the test trials
Wind	0 to 40 miles per hour

4.3.2.3   Outdoor Cold/Dry

Representative of arctic areas of the United States, optional outdoor tests will take place under cold and dry conditions. These conditions will be provided through actual location testing or through simulated conditions within an environmental chamber. Typical test characteristics are provided in Table 3.

Table 3. Test Characteristics – Outdoor Cold/Dry

Condition	Tested Value
Temperature	Below 40 degrees F
Humidity	Below 40%
Precipitation	Not specified
Wind	0 to 40 miles per hour

Table 4 identifies particular modalities and associated specific environmental factors. (The specific modalities listed are those most frequently considered with respect to biometric devices for airport access control.)

Table 4. Modality Specific Environmental Factors

Modality	Airport Indoor Environment	Airport Outdoor Environment
Fingerprint	-Temperature -Lighting: non-directional ambient -Humidity -Vibration	Airport indoor environmental factors plus: Lighting: direct sunlight (natural vs. simulated) Condensing humidity Elemental exposure, including clouds and other typical elements
Hand Geometry	-Temperature -Lighting: non-directional ambient	Airport indoor environmental factors plus: Lighting: direct sunlight (natural vs. simulated) Elemental exposure, including clouds and other typical elements
Facial	-Lighting: non-directional ambient -Background composition	All airport indoor environmental factors plus: Lighting: direct sunlight (natural vs. simulated) Elemental exposure, including clouds and other typical elements
Iris	-Lighting: non-directional ambient -Vibration	All airport indoor environmental factors plus: Lighting: direct sunlight (natural vs. simulated) Elemental exposure, including clouds and other typical elements
Voice	-Ambient noise	All airport indoor environmental factors plus: Elemental exposure, including typical elements, especially wind
Signature	-Lighting: non-directional ambient -Vibration	All airport indoor environmental factors plus: Lighting: direct sunlight (natural vs. simulated) Elemental exposure, including typical elements
Others as specified by the manufacturer, e.g., magnetic inductance, bio-impedance	-Device-specific TBD	Device-specific TBD

4.3.3 Device Operability Verification

Device operability verification will be conducted periodically during qualification testing. These tasks will be performed by the test team according to manufacturer procedures at the start of every test period and at manufacturer recommended time intervals thereafter to assure that the biometric sub-system is operating within manufacturer performance parameters.

4.3.4 Test Crew Selection

The test facility manager will assemble a crew of human test subjects to carry out the qualification testing. The demographics of the crew will be controlled in terms of gender, age, and work category, and are intended to be representative of airport employee populations. Controlling these factors will allow for more defensible test results across various crew populations, avoiding accusations of bias due to disproportionate demographic characteristics.

4.3.4.1   Crew Size

The determination of the crew size depends on several interrelated statistical measures. To determine the crew size, TSA employed the PRESS (Program for Rate Estimation and Statistical Summaries) tool, which helps researchers analyze data collected on biometric authentication devices. It was created at St. Lawrence University, through funding from the Center for Identification Technology Research. The results of this effort have provided an optimum crew size of 200 individuals for enrollment (accounting for over 10% attrition) and a target of at least 180 for revisit verification testing. This result is based on 15 verification transactions by each crew member.

TSA Crew sizes will be 250 individuals for enrollment, to account for potential attrition in terms of number of revisit individuals, and of the possible variation in the number of revisits (therefore transactions) per person.

4.3.4.2   Crew Demographics

4.3.4.2.1   Age Distribution of Crew

Age distribution of crew shall adhere to the ranges of values shown in Table 5.

Table 5. Age Distribution

Age Distribution (In Any Size Evaluation)		
Less than 30	30 to 50	Over 50
20 - 35%	25 - 45%	25 - 45%

4.3.4.2.2   Gender Distribution of Crew

Gender distribution of crew shall adhere to the ranges of values shown in Table 6.

Table 6. Gender Distribution

Gender Distribution	
Male	Female
40 - 60%	40 - 60%

4.4.4.2.3 Work Category Distribution of Crew

To represent the demographics of airport employees, work categories of crew shall adhere to the ranges of values shown in Table 7.

Table 7. Labor Distribution

Labor Distribution	
Office Worker	Manual Laborer
40 - 70%	30 - 60%

(NOTE: These values may be adjusted based on information received from AAAE in the future)

4.3.5   Pretest Activities

Pretest activities will include a configuration audit, a Test Readiness Review (TRR) with manufacturer participation, and a pretest briefing, which will be conducted prior to the start of each test period with participation from the TSA test team only.

4.3.5.1   Pretest Briefing

A pretest briefing will be conducted by the Test Manager prior to each test period and qualification test category. The pretest briefing will be attended by all test team members. During the pretest briefing the Test Manager will:

a.   Identify test team members and assign specific responsibilities.
b.   Review system configuration.
c.   Review the specific biometric device test procedures.
d.   Review the results of relevant tests.
e.   Identify and review any existing or expected problems.
f.   Provide all necessary test documentation and associated forms.
g.   Review test equipment configuration.

Minutes of the pretest briefing will be recorded by a designated member of the test team and validated by the QA personnel. The minutes will provide enough information to completely and accurately document the meeting.

4.3.5.2   Configuration Audit

Following successful system installation and checkout, but prior to the Test Readiness Review (TRR), there will be a system configuration audit. The audit will be performed after an operational system configuration has been established by the manufacturer representative. This configuration will represent the system baseline at the start of qualification testing.

The configuration audit will be performed by QA personnel with the assistance of a manufacturer representative. The primary goal of the audit is to identify and record system hardware, firmware, and software configuration accurately. The Configuration Log (Appendix A) will be used to document all applicable hardware and software versions and serial numbers. This log will be created and maintained by QA personnel throughout qualification testing.

At the conclusion of the configuration audit, QA personnel will place QA seals at the appropriate locations on the biometric device to maintain configuration control throughout the test. In addition, the manufacturer representative will sign a system readiness form documenting approval of system configuration and preparedness for starting qualification testing.

4.3.5.3   Test Readiness Review

A TRR will be held after completion of biometric device installation, checkout, and test team training. This review will be conducted by the test team manager and will be attended by all

personnel involved with qualification test conduct. The TRR will be used to verify system and test team readiness for conducting qualification testing. During the TRR, the test team manager will:

a. Verify (by inspection) that the biometric device meets all safety requirements.
b. Verify completion of configuration audit.
c. Review established system and test equipment configurations.
d. Verify completion of test team training.
e. Identify and review any changes to the biometric device test plan or procedure.
f. Review the biometric device qualification test schedule.
g. Review test crew characteristics.

Minutes of the TRR will be recorded by a designated member of the test team and validated by QA personnel. The minutes will provide enough information to completely and accurately document the review.

4.3.6   Data Collection

During core testing, both quantitative and qualitative data will be collected and recorded in a manner that is specific to the test organization infrastructure and that achieves TSA biometric device test requirements and objectives.

The quantitative enrollment error rate will be recorded automatically (if possible) and the data will be entered into the test-organization-information system.

For verification, the quantitative capture of biometric sub-system decisions (accept/reject only) will be accomplished and used to determine the associated FAR and FRR values for transaction level (up to three attempts) only. In addition, the intervals between the beginning of each verification transaction and the resultant decision for each transaction for all crew members will be recorded.

Qualitatively, crew reactions to device use will be surveyed and manually entered for use in debriefing the biometric device manufacturer.

Complete, accurate, and reliable collection of data is an integral part of the biometric device test. To facilitate this, test data collection will be automated to the maximum extent possible. For any required manual data recording, the Test Manager will assign test team members with specific data collection responsibilities prior to the execution of each test category. Data collection assignments will be made at the pretest briefing. Designated members will be provided with necessary data collection forms and/or equipment and will be responsible for recording data as required in the general biometric device test procedure.

The automated data collection system and the test team will collect data as defined in the general biometric device test procedure. The data will include, at a minimum:

a. Test description.
b. Test date(s) and time(s).
c. Crew member identifier.

d.   Device indications (if any).
e.   Timeline data for transaction time analysis.
f.   Device operational or failure data (if any).

To facilitate the correlation of biometric device response to test crew member, a bar code reader (or similar automated, highly accurate device) will be used to read each test crew member's identifier before he or she interacts with the device.

At the conclusion of each test session, all data collection forms and additional media will be validated and signed by QA personnel. All data will be sensitive and stored in accordance with the TSA privacy guidance.

4.3.7   Problem Reporting and Tracking

Any test anomaly or equipment problem that occurs during biometric device qualification testing will be documented. Specific details of the event will be recorded by the test experimenter and validated by QA personnel immediately following the occurrence. The information must be recorded on the Test Observation Log Input Form (Appendix B) and include exact details of the event, equipment serial numbers, biometric device hardware and software version numbers, time to repair, name of individual who observed the event, any known effects on test outcome, and times and dates of all significant maintenance and repair actions

A further review of all logged anomalies will determine if a qualification problem report needs to be written. A qualification problem report will be written if the event involves a functional problem with the biometric device or could affect the results of a test. Each problem will be assigned a unique number and will be tracked throughout qualification testing. Priority levels will be used to document the severity of the problem. These priorities are identified as:

a.   Type I - Qualification Critical. Affects the performance of a critical operational function of the biometric device or results in a degradation of performance below acceptable levels.
b.   Type II - Test Critical. Does not affect the performance of a critical function of the biometric device, but has an unsatisfactory effect on the test.
c.   Type III – Non-Critical. Involves a non-critical operational function or a non-operational system function.

Qualification testing will be terminated if the system fails and cannot be repaired by the manufacturer within three (3) working days, unless additional time is approved by the Test Director. Components that cannot be repaired may be replaced only when accompanied by a manufacturer statement that the replacement unit configuration exactly matches the original unit, and with the approval of the Test Director. At the conclusion of each qualification test, all qualification problem reports will be compiled by the test team and included in the final test report.

4.3.8 Posttest Briefing

There will be a posttest briefing at the conclusion of each test period and test category. All test team members will attend the posttest briefing. The Test Manager will summarize the test activities and relevant issues. During the posttest briefing the Test Manager will review, as necessary:

a.   Deviations from the planned test procedures.
b.   Test anomalies.
c.   Configuration management issues.
d.   Equipment failures.
e.   Upcoming test schedule.

Minutes of the posttest briefing will be recorded by a designated member of the test team and validated by the QA personnel. The minutes will provide enough information to completely and accurately document the meeting.

4.3.9 Data Reduction and Analysis

The test team will perform all data reduction and analysis (DR&A) upon completion of qualification testing. The DR&A methods used are defined in the general test procedure. Identical analysis will be performed for each biometric device tested to provide consistent, unbiased results. Specific biometric sub-system performance parameters that will be calculated include, but are not limited to Transaction time for verification (TT_V), FTE, and the FRR and FAR for transactions (multiple attempts) at the biometric match operational threshold set by the manufacturer.

4.4 Inspection

Prior to testing, an Evaluation Program Elements Checklist will be completed to ensure proper installation and normal operation of all, equipment being evaluated, test equipment, and equipment interfaces.

It is anticipated that each manufacturer will support the installation of its devices in the test organization's facility in close cooperation with the test organization. The manufacturer will be required to certify that the installation is functional. The manufacturer must also provide specific configuration and settings data at the completion of setup and written instructions to the test staff, should any be necessary. Manufacturer personnel are not expected to be present during the actual testing period (unless contacted by the Test Director).

4.4.1 Physical Layout of Test Environment

The experimenter shall record the physical layout of the test environment, including but not limited to the following:

a.   Dimensional area dedicated to scenario test execution.
b.   Presence of natural and artificial lighting.
c.   Positioning of biometric acquisition devices.
d.   Relative location of each biometric device in the test environment.

4.4.2   Specifications

The experimenter shall record the following elements of the biometric system:

a.   Acquisition device: Manufacturer, model, version, and firmware, as applicable.
b.   If the acquisition device's core acquisition components are integrated within a third-party device: manufacturer, model, version, and firmware of the core acquisition components.
c.   Biometric algorithms: Version and revision.
d.   If the scenario test incorporates a biometric software application, such as a demonstration application or logical access interface: Provider, title, version, and build of the software application.
e.   Systems tested on or through PCs, PDAs, or other computing devices: Processing power, memory, manufacturer, and model of computing device.

4.4.3   Architecture

The experimenter shall record the following elements for the biometric sub-system and the facility infrastructure:

a.   Biometric data acquisition, processing, and storage architecture.
b.   Data flow between biometric device and test organization's facility equipment components.
c.   Test management application: Design and functions of any application into which the test system is integrated for test management.
d.   Data analysis application: Design and functions of any application used to analyze performance results.
e.   Schematics: Acquisition devices, workstations, server components, and layout of test components.

4.4.4   Implementation

The experimenter shall record system implementation information corresponding to the method of biometric and platform system acquisition and the level of manufacturer involvement in system implementation.

4.5   Performance Measures

4.5.1   Core Test and Options

The core test consists of transaction level error rate testing under controlled conditions, and determination of FTE and verification transaction time. Options include other conditions, FTA, transaction time for identification (1: N), and enrollment quality threshold.

4.5.2   Core Test Graded Performance Metrics

This section describes the core test measurements at a high level. For each production biometric device test, core tests (including enrollment and verification tests) will be conducted after the

device has been certified for operation and the crew has been trained. Three (3) core TSA test metrics will be gathered. Table 8 defines the 3 core test metrics. The first column lists the index number of each metric. The second column identifies the name of each core test metric and the origin of the data (enrollment, transactions, or attempts). The third column lists each explicit measurement symbolically. Last, the fourth column lists the role of the metric.

Table 8. Core Test Metrics

Core Test Metric Index	Core Test Metric Name	Core Test Metric Symbol	Metric Role in Core Testing
1	Transaction Error Rates	FRR , FAR	Reported, graded
2	Multi-Attempt Failure to Enroll (FTE)Rate	FTE	Reported, graded
3	Transaction Time (Verification)	TT_V	Reported, graded

For the TSA core qualification performance test, transaction error rate values will be determined at the threshold setting established by the manufacturer. Here, FRR represents the proportion of verification transactions where truthful claims of identity are incorrectly denied. Likewise, FAR represents the proportion of verification transactions where wrongful claims of identity are incorrectly confirmed. In addition, a Transaction is defined as the result of up to three verification attempts by an individual crew member.

TSA established a single maximum FRR - FAR pair, below which a particular device must perform. A specific device test result is then reported as qualified or not, based on the statistical analysis shown in Appendix A of Volume 1, Chapter 1. In order to pass at these levels, devices will be required to show that measured test results for both error rates are significantly less than the qualification criteria error rate. (This analysis approach is necessary to account for the inherent non-repeatability in human-based testing, and to provide a level of assurance that a re-test of a device will result in the same pass/fail outcome.)

Metric 2, FTE, addresses the percentage of the population of crew members who cannot generate a usable template for the biometric device under test.

Metric 3, transaction time (TT_V), addresses the time interval from the claim of identity (card swipe or bar code) of a first verification attempt to the availability of the corresponding transaction result.

4.5.3   Test Options

Some devices (based on manufacturer request) may be subjected to additional testing beyond the core test. This depends on the method of operation of the device and the range of operating environments for which the device is deemed suitable. The topics considered optional are:

a.   Transaction times (identification mode) measurement.
b.   Enrollment quality threshold effects.
c.   Failure to acquire measurement.
d.   Other environmental conditions.

4.6   Operator-Crew Member Interaction

Experimenters shall determine and report operator-crew member interaction required and permitted, as follows:

a.   Whether the operator is to provide specific guidance above that provided by the system during enrollment or matching instructions.
b.   The amount of information given to the crew member regarding the evaluation.
c.   The amount of feedback given to the crew member during the evaluation.

4.7   Habituation

The end users are the airport employee population (target population), which is characterized as highly habituated. The operational usage of these biometric devices will often be a several times a day occurrence for a large segment of the population. Therefore, the test shall be focused on approximating (to the extent possible) the highly habituated end user. The use of biometric product-supplied feedback mechanisms should contribute to the habituation of the crew.

4.8   Enrollment and Matching

4.8.1   Enrollment

The successful enrollment of a crew member typically includes an immediate verification that the candidate enrollment template can be successfully matched. This may take place prior to template storage. The time separation between candidate enrollment template generation and the enrollment verification shall be as little as possible or based on the manufacturer's directions. In essence, it is immediate.

The template is generated by the process of enrollment as specified by the manufacturer of each device. The test organization will acquire the enrollment templates, store them, and make them available for use during verification testing.

4.8.2   Verification and Imposter Testing

In order to generate data for calculation of FRR and FAR, verification and imposter testing must be performed.

4.8.2.1   Same Day

The minimum time between the enrollment and same day verification shall be one hour. Multiple same day verification trials can be performed (proposed to be five trials), with no additional elapsed time between trials. (This may facilitate some aspects of emulation of habituation [see Section 4.7].)

4.8.2.2   Revisit

The core test revisits will take place three times within six weeks of enrollment. Ideally, the spacing of these revisits will result in one revisit every two weeks. During each revisit session, each crew member should conduct at least five genuine verification transactions and five imposter transactions. This will provide a total of 15 genuine transactions (for computation of FRR) and 15 imposter transactions (for computation of FAR) for crew members successfully completing all three revisits. Data for crew members with fewer than three revisits will also be included in the overall performance calculation.

4.9   Levels of Effort and Decision Policies

The experimenter shall report enrollment and verification levels of effort and decision policies.

The minimum and maximum number of placements, attempts, and sequences required or permitted to enroll may be somewhat dependant on the device under test. A device may allow enrollment after one attempt, or may require multiple attempts and sequences. Unless otherwise dictated, the following shall apply:

a.   Three attempts shall be allowed for each enrollment sequence.
b.   Two enrollment sequences shall be allowed (if unable to enroll on the first sequence).
c.   Three attempts shall be allowed for each verification transaction.

The minimum and maximum duration permitted or required to enroll within a given enrollment presentation, attempt or sequence shall be defined and reported. A biometric device may terminate an enrollment transaction after a fixed duration. This may be due to the inability to acquire sufficiently distinctive data or the inability to sense any biometric data input whatsoever. It is not feasible to allow a biometric device to attempt to acquire data indefinitely; therefore, for devices that do not timeout, a time of 30 seconds shall be established as the default timeout.

The maximum number or duration of presentations, attempts, and sequences during enrollment are referred to as enrollment presentation limits, enrollment attempt limits, and enrollment sequence limits, respectively.

4.10 Errors and Exception Cases

For a given interaction of a crew member with the device under test, errors or exception cases may occur, including:

a.   Biometric device provides the operator with a functional error code - The operator shall react to the error code as mandated by the manufacturer's manuals. The time associated with reacting to the error code shall be included as part of the crew interaction time interval. If the device error is not corrected within 10 minutes, then the specific device with the error shall be removed from service and, as appropriate, the entire test enrollment or subsequent verification sequence restarted from the beginning with a substitute device of the same production make and model.

b.   During enrollment, a crew member is not successful in obtaining an acceptable enrollment result – Two sequences of three repeated attempts at enrollment shall be made. If enrollment is not possible, this result shall be recorded, the specific individual crew member removed for core revisit verification test purposes, and the crew subsequently adjusted to maintain the validity required of core test statistics.

c.   During the core revisit verification test, the standard test protocol of up to three repeated attempts at verification is established. Any errors resulting from verification will be recorded and used in qualifying the biometric devices.

4.11   Reporting Performance Results

Reporting will be in accordance with established requirements and conveyed in a basic structure.

4.11.1 Reporting Requirements

All reporting requirements shall be documented in a test report. General reporting requirements are identified in the international standards on performance testing and reporting (Section 2).

4.11.2 Report Structure

The final test report shall be in accordance with the outline in Appendix C of this document.

4.12   Conformance

Conformance issues are covered in the Standards Chapter (Volume 1, Chapter 3) of the Guidance Package.

4.13   Qualification Criteria

The primary objective of biometric device qualification testing is to evaluate sub-system performance against the mandatory qualification requirements defined in the criteria, which establish the minimum performance requirements necessary to achieve TSA qualification. Table 8 contains the metrics and criteria for verification.   The following paragraphs discuss the approach to be taken for the evaluation of biometric device performance against the mandatory criteria.

4.13.1 Verification Rates

The objectives of verification rate testing are to determine if the biometric device can verify the identity of genuine attempts and deny access to imposter attempts, as defined in the criteria. To achieve TSA qualification, the biometric device must achieve a measured genuine transaction rejection rate and a measured imposter transaction acceptance rate significantly below the qualification value as specified in Appendix A of Chapter 1 of Volume 1 of this Guidance Package.

4.13.2 Failure to Enroll Rate

The objective of FTE testing is to verify that the biometric sub-system can operate, under realistic operating conditions, with an FTE rate that is less than or equal to the maximum rate specified in the criteria. The FTE performance of every biometric device will be evaluated with the full compliment of crew members selected for the test.

4.13.3 Transaction Time

TSA established that the biometric device must process individual identity verification decisions at or below the maximum verification time specified in the criteria. (In addition, for biometric devices that operate in a one-to-many or identification mode at all times, then the identification decision time must be at or below the maximum verification time specified in the criteria). The objective of transit time testing is to measure, under simulated operating conditions, the verification transaction time of the biometric device (not to include the subsequent actions of the ACS). To accurately measure this time, the test team will process the full set of genuine verification transaction for each crew member. Transaction time metrics will then be measured.

4.14 Operational Considerations

In addition to the core test requirements, the test team will evaluate other operational characteristics of the biometric device as identified in the criteria. The results of these evaluations will not influence system qualification, but will serve as inputs to the aviation industry's decisions on the purchase, deployment, and use of the equipment. The results will also provide information for the individual airport authority to use in evaluating the operational impact of biometric device deployment. Table 9 lists individual operational considerations and the method of evaluation.

Table 9. Biometric Device Operational Considerations

ID Number*	Operational Consideration	Method
T-3.9	Evaluation of the physical characteristics such as unit weight, size, and/or cost	Inspection, Analysis
T-3.2 O-2.1.1	Evaluation of system reliability and availability	Analysis
O-2.2.3	Evaluation of training required with respect to system operability, calibration, and maintenance	Analysis
O-2.1.4 O-2.2.2 O-2.2.7 O-2.2.8	Evaluation of systems operational usability and adaptability	Inspection, Analysis

*The ID Number points to a specific portion of the technical (T-paragraph number) or operational requirements (O-paragraph number). See Volume 1, Chapters 1 and 2.

The following paragraphs provide a brief description of operational characteristics and the approach to be taken to evaluate them during qualification testing.

4.14.1 Physical Characteristics

Although TSA has not defined any precise physical constraints to be placed on a biometric device, smaller and more flexible devices (in terms of mounting) are more practical for use in a variety of airport situations and, thus, are more desirable. Accordingly, the test team will evaluate and record the relevant physical characteristics of the biometric device during qualification testing.

4.14.2 System Failure Data

The biometric device criterion specifically defines sub-system requirements relating to availability. No specific testing will be conducted to evaluate these factors; however, the test team will collect data relating to the day-to-day system reliability, including data associated with failures and durability of equipment during qualification testing. Additionally, manufacturer supplied data and data collected in the test observation log, the system configuration log, and the qualification problem reports will be compiled. A complete record of the system's failure data will be included in the qualification test report.

4.14.3 Training

Devices that are easily operated and maintained will be more acceptable than devices that require extensive specialized training for operation, calibration, and maintenance. As part of this evaluation, the test team will consider the complexity of the manufacturer-provided training for operation, calibration, and maintenance of the system.

4.14.4 Operational Usability and Adaptability

Devices that are adaptable to a wide variety of user types and airport operating conditions will be more acceptable to potential users and system owners. In particular, the test team will observe the devices' ability to adapt to different individuals in the test crew and environmental conditions.

5. ORGANIZATIONAL ROLES AND RESPONSIBILITIES

5.1 Transportation Security Administration

The following roles will be assigned to TSA, test facility, and support contractor test team personnel: TSA Test Director, Test Manager, test engineers, and QA personnel. The responsibilities of these roles are defined as follows:

a. TSA Test Director (TSA)
   1. Schedule all required equipment and resources.
   2. Review and approve the specific biometric device test procedure.
   3. Schedule and oversee all test activities.
   4. Review and approve the test report, including recommendations concerning biometric device qualification.
   5. Attend manufacturer posttest briefings.

b. Test Manager/experimenter (test facility)
   1. Ensure the biometric device is properly installed and operational prior to testing.
   2. Ensure the biometric device meets all safety requirements prior to test conduct.
   3. Review specific biometric device test procedures.
   4. Conduct pretest and posttest briefings.
   5. Coordinate activities of all test personnel during test conduct.
   6. Ensure compliance with test procedures.
   7. Supervise collection and reduction of test data.
   8. Approve system configuration changes.
   9. Review test report.

c. QA personnel
   1. Review specific biometric device test procedures.
   2. Verify crew demographics.

3. Verify device installation (dimensions of positioning, etc.).

4. Conduct system configuration audit.

5. Provide biometric device, test article, and test equipment configuration control during test conduct.

6. Review documentation of daily test activities.

7. Ensure compliance with test procedures.

8. Validate collected data.

5.2 Manufacturer

The manufacturer shall provide the personnel necessary to support the test team prior to and during qualification testing. This shall include, but is not limited to, test team personnel training, system installation and checkout, system calibration and maintenance, and general technical support. Support during qualification testing will only be at the request of the Test Manager. In general, manufacturer personnel will not be present during test conduct.

6. DOCUMENTATION REQUIREMENTS AND CONTROL

The test will be executed according to the guidelines established in this plan. Effective documentation and control of all events must occur during the test process to ensure compliance with stated objectives. This section provides a brief description of the documents that will be used during test.

The following paragraphs identify the documentation required to execute the test program including the privacy plan, general and specific biometric device test procedures, and the biometric device qualification test report.

6.1 Biometric Device Qualification Test Report

The "Biometric Device Qualification Test Report" (see Appendix C for outline) will contain a detailed analysis of the qualification test results, an operational evaluation of the system, and a summary of problems encountered during testing. The report will contain all of the information necessary to evaluate the system against the criteria and provide information concerning its operational performance. It will be prepared by the test team and approved by the Test Director.

6.2 Test Control

Extensive control of test activities and documentation of results is required throughout all phases of qualification testing. To accomplish this, test control documentation will be utilized. This documentation will include a configuration log, test briefing minutes, test data, qualification problem reports, and a biometric device test observation log.

6.2.1 Configuration Log

The Configuration Log Input Form (Appendix A) will be used to document and control biometric device configuration throughout qualification testing. The log will contain biometric device configuration data from the configuration audit and document any system baseline changes that occur during testing. Entries into the log will be performed by the test team and validated by QA personnel.

6.2.2 Test Briefing Minutes

The minutes of test briefings will provide enough information to completely and accurately document pretest and posttest meetings. The minutes will be compiled for each biometric device and will be used as a reference to document the daily test activities. These meeting minutes will be assembled by the test team and will be included in the qualification test report.

6.2.3 Test Data

Test data will be collected throughout qualification testing and will be retained for subsequent analysis. Proper recording of this data is the responsibility of the Test Manager and will be validated by QA personnel. Any biometric device proprietary information obtained during test will be used for qualification, test, and analysis purposes only. The TSA test team will not disclose proprietary information to anyone who has not entered into a nondisclosure agreement with the manufacturer.

6.2.4 Qualification Problem Reports

All entries into the test observation log will be reviewed daily to determine if a qualification problem report needs to be written. In general, a qualification problem report will be written if the observation is related to equipment failure or if it may affect test results. The problem reports will be written by the Test Manager, assigned a unique number, and will be closely tracked throughout testing. All problem reports will be addressed in the qualification test report. This will include a description of the problem, disposition, and the results of any retests performed, if applicable.

6.2.5 Test Observation Log

A test observation log will be compiled during testing to document all test anomalies and equipment failures. Specific details will be recorded on the Test Observation Log Input Form (Appendix B). All entries will be recorded by the Test Manager (or operator) and validated by QA personnel immediately following the occurrence. The log will be an attachment to the qualification test report.

6.3 Data Distribution Plan

Data reported in the test reports will be submitted to TSA only. TSA will control its distribution and will make the QPL and supporting information available based on TSA policy.

7. TSA TRAINING/FAMILIARIZATION

The manufacturer will train the test team prior to qualification testing. The level of training will be sufficient to enable the test team to independently operate the equipment during qualification testing and provide training to the test crew. In addition, the manufacturer will familiarize the TSA test team with the design and functionality of the biometric device to enable them to perform the technical tasks necessary to execute qualification testing with minimal manufacturer support. *At the conclusion of this training, the manufacturer representative will sign a training completion form. This will document that the manufacturer has completed test team training and is confident with the ability of the test team to operate the biometric device to the degree necessary for qualification testing. (note – latter section may be subject to change in the future)*

8. SCHEDULING

The Test Manager will be responsible for scheduling all biometric device test events. This includes scheduling document preparation, briefings, test conduct, and data analysis activities.

9. VERIFICATION METHODS

The methods used for verification of a requirement or evaluation of a characteristic will be inspection, analysis, demonstration, and test. Testing will be used wherever possible for verification of all requirements at the device or sub-system level. These terms are defined below:

a. Inspection - Verification by visual examination of the item, review of descriptive documentation, and comparison of the appropriate characteristics with a predetermined or referenced standard to determine conformance to requirements without the use of special laboratory equipment or procedures.

b. Analysis - Verification by technical/mathematical evaluation or simulation using mathematical representation (e.g., mathematical models, algorithms, equations), charts, graphs, circuit diagrams, data reduction/recording, and representative data to prove that an item meets specified requirements. Representative data may include data collected from previous or other equipment and system verifications.

c. Demonstration - Verification by operation of the item in performing its functions under a set of conditions. The item may be instrumented and quantitative performance may be monitored and recorded. A determination that the demonstration is satisfactory will be indicated; this may be based upon satisfactory limits of performance.

d. Test - Verification through systematic exercising of the item under appropriate conditions, with instrumentation and collection, analysis, and evaluation of quantitative data for predetermined performance characteristics. Acceptability of the item is determined by the comparison of the data with pre-established quantitative requirements and occurrences.

10. TEST EQUIPMENT AND CONSUMABLES

Table 10 will be used to indicate the equipment that to be used by the TSA test team during the test (as the details of that equipment selection become available).

Table 10. Biometric Device Qualification Test Equipment

Item No.	Quantity	Equipment Description	Model No.
1	1	Computer system - laptop PC	TBD
2	TBD	Bar code scanner - TBD	TBD
3	TBD	Bar code reader - TBD	TBD
4	TBD	TBD	TBD
5	TBD	TBD	TBD
6	TBD	TBD	TBD
7	TBD	TBD	TBD
8	TBD	TBD	TBD
9	TBD	TBD	TBD
10	TBD	TBD	TBD
11	TBD	TBD	TBD

Table 11 will be used to list the consumables that will be required to execute the test.

Table 11. Biometric Device Test Consumables

Item No.	Quantity	Description	Model No.
1	TBD	QA seals	TBD
2	TBD	TBD	TBD
3	TBD	TBD	TBD
4	TBD	TBD	TBD

NOTE: The items and equipment listed in Tables 10 and 11 will be provided by the test facility, except where otherwise noted.

11. GLOSSARY

ADMINISTRATOR.   Individual employed by the test organization who oversees and administers the operations and conduct of procedures with crew members on the actual system.

ATTEMPT. Submission of one or a sequence of biometric samples to the system.

CREW. Set of test subjects gathered for a test. Crew members may be volunteers who are compensated for their test participation

CREW MEMBER. Person presenting a biometric sample to the system.

END USER. The airport or air carrier employee who will ultimately present his/her biometric sample to a biometric ACS to gain access to secure areas of airports.

EXPERIMENTER. Test organization employee who defines, designs, and analyzes the test.

FAILURE TO ACQUIRE RATE. Proportion of verification or identification attempts for which the system is unable to capture or locate an image or signal of sufficient quality.

FAILURE TO ENROLL RATE.   Proportion of the crew for whom the system is unable to complete the enrollment process.

FALSE ACCEPT RATE.   Proportion of verification transactions with wrongful claims of identity that are incorrectly confirmed.

FALSE REJECT RATE. Proportion of verification transactions with truthful claims of identity that are incorrectly denied. Note that in this context, this measure is inclusive of both failures to acquire as well as false non-matches.

HABITUATION.   Familiarity with the workings of a biometric system and/or application, particularly in the area of presentation and acquisition device interaction.

IDENTIFICATION. Application in which a search of the enrolled database is performed and zero, one, or more record pointers (identifiers) are returned.

OFFLINE TESTING. Execution of enrollment and matching separately from image or signal submission.

ONLINE TESTING. Execution of enrollment and matching at the time of image or signal submission.

OPERATOR.   Individual employed by the test organization whose function is to conduct procedures with crew members on the actual system.

SAMPLE.   A biometric measure presented by the crew member and captured by the data collection subsystem as an image or signal (e.g., fingerprint, face, iris images).

SCENARIO TEST. A test in which the end-to-end system performance is determined in a prototype or simulated application.

TECHNOLOGY EVALUATION. An offline evaluation of one or more algorithms for the same biometric modality that utilizes a pre-existing or especially collected corpus of samples.

TEMPLATE. User's stored reference measure based on features extracted from enrollment samples.

TEST ORGANIZATION. Functional entity under whose auspices the test is conducted (i.e., the independent test organization that will be chosen for this test). The test organization is the employer of the experimenter(s) and the test operator(s).

TRANSACTION. A transaction (for test purposes) consists of up to three verification attempts by an individual crewmember.

VERIFICATION. Application in which the crew member makes a positive claim to an identity, features derived from the submitted sample biometric measure are compared to the enrolled template for the claimed identity, and an accept or reject decision regarding the identity claim is returned.

APPENDIX A - CONFIGURATION LOG INPUT FORM

Configuration Log Input Form

	ITEM NAME	ITEM PART #	ITEM SERIAL #	ITEM REV. LEVEL
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				

Configuration Changes

Enter the corresponding information for each change made to the biometric device configuration:

	DATE OF CHANGE	REASON FOR CHANGE	COMMENTS
	/ /		
	/ /		
	/ /		
	/ /		
	/ /		
	/ /		
	/ /		

APPENDIX B - TEST OBERVATION LOG INPUT FORM

Test Observation Log Input Form

Biometric Device Model: _____

Test Title/Name: _____

Test Date: ____/____/____   **Observer Name:** _____

Observations/Test Events (indicate crew ID and time of observation): _____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

This page intentionally left blank.

APPENDIX C - BIOMETRIC DEVICE QUALIFICATION TEST REPORT

Biometric Device Qualification Test Report

The Biometric Device Qualification Test Report will contain the following:

a.   Executive Summary
b.   System Description/Configuration
c.   Test Purpose
d.   Test Objectives
e.   Reference Documents
f.   Test Date and Location
g.   Manufacturer Information
h.   Test Team Members
i.   Test Results Summary
j.   Detailed Test Results
k.   Data Collection Techniques
l.   Data Analysis Techniques
m.   Procedural Deviations
n.   Problems Encountered
o.   Regression Test Requirements
p.   Conclusions and Recommendations
q.   Attachments: Test Observation Log, System Configuration Log, Test Briefing

VOLUME 3 – PLAN FOR BIOMETRIC QUALIFIED PRODUCTS LIST (QPL)

CHAPTER 3

BUSINESS MODEL
For
Biometric Sub-System

30 September 2005

Volume 3, Chapter 3 - Business Model for QPL

1.0   Introduction

The purpose of this Business Model Plan is to outline the method of financing the TSA biometric qualification program. This plan is divided into the following two (2) sections:

"Initial Business Model "

"Sustained Business Model "

This plan is specific to biometric sub-systems and addresses all non-Governmental activities necessary to establish and maintain an evaluation process that supports developing, maintaining and managing a viable TSA Biometric Qualified Product List (QPL).

2.0 Initial Business Model

In the initial phase of testing for the QPL, TSA will identify testing organizations and will support the preparation of these facilities for the identified qualification testing. The manufacturer will pay for all direct testing costs, as well as its biometric device(s) and/or sub-system(s), all test facility personnel training performed by the manufacturer, equipment shipping charges to and from the testing facility, any required sub-system modification, and adapter fabrication (if necessary).

3.0   Sustained Business Model

The method for financing the long-term continuous process of testing new and derivative products will be developed by the industry. TSA will only fund the internal activities necessary to perform the role of Test Director and will maintain the QPL. All testing costs are expected to be covered by the manufacturers on a fee for service basis.

VOLUME 3 – PLAN FOR BIOMETRIC QUALIFIED PRODUCTS LIST (QPL)

CHAPTER 4

NOTIONAL SCHEDULE
For
INITIAL QPL

30 September 2005

Volume 3, Chapter 4 - Notional Schedule for Initial QPL

OVERVIEW

Following the publication of the TSA Guidance Package, about 2 months will be devoted to familiarization with the guidance, particularly the Application for Qualification process by the manufacturers. The TSA review of applications is expected to begin in the following month. Laboratory Performance testing is expected to be done in batches of pre-qualified products, beginning sometime in the first half of calendar 2006. TSA expects that a list of qualified products will be published after the evaluation of each batch, and the complete Initial Qualified Product List may be completed as early as Spring 2006.