Comparative Biometric Testing

Official Test Plan

Version 2.1

International·Biometric·Group

Research Consulting Integration

International Biometric Group
One Battery Park Plaza
New York, NY 10004
212-809-9491

Table of Contents

Table of Figures

1. Executive Summary

Test Overview

International Biometric Group's Comparative Biometric Testing evaluates the ability of biometric systems to enroll and verify individuals within logical and physical access test scenarios. Results from Comparative Biometric Testing facilitate deployment, partnership, and product development decisions in applications such as network and IT security, e-commerce, retail and point of sale, access control, and card-based ID systems.

The performance data collected, evaluated, and reported for biometric systems includes false match rates (FMR), failure to enroll rates (FTE), and false non-match rates (FNMR). To evaluate systems' susceptibility to false non-matching over time, test subjects are verified in a return visit approximately six weeks later.

Comparative Biometric Testing also assesses FMR and FNMR at three security thresholds – high security, medium security, and low security. If vendors do not provide adjustable thresholds, systems are tested at a single threshold of the vendor's choosing.

240 non-acclimated test subjects recruited from the general populace comprise the test population. The testing is based on real-time enrollment and verification of subjects as opposed to offline comparison of static or recorded biometric samples. This methodology provides results reflective of (1) feature extraction and matching algorithm robustness and (2) device ergonomics, system usability, and ease of sample submission in a real-world environment.

By virtue of the scenario-based nature of IBG testing, error rates may be higher than are generally claimed in the biometric industry. This is less a reflection on the potential effectiveness of biometrics in logical and physical access applications than a reflection on the discrepancy between theoretical versus real-world test efforts.

Primary and Secondary Visits

IBG's Comparative Biometric Testing is broken into a Primary Visit and a Secondary Visit for each test subject. The two visits are separated by approximately six weeks.

Test Process: Primary Visit

On the subject's initial visit to IBG's testing facilities, test operators gather demographic data, including age, sex, race, height, weight, and occupation. The subject is assigned a unique user ID. For each biometric system, the subject attempts to fraudulently match against two previously enrolled "target" subjects. The subject then attempts to enroll in each system. Upon successful enrollment, the subject attempts to match as himself. Test operators accompany and direct subjects throughout the testing in order to provide scripted instructions, collect data, record subject comments, and to address any anomalies.

To the degree possible, the number of “false” match attempts, enrollment attempts, and “true” match attempts permitted are standardized across different types of biometric technologies and devices in order to derive comparative accuracy results for non-like systems. In addition, the test order is designed such that in a round with N systems, each system is tested an equivalent number of times in the first position, second position, and so forth until the Nth position. This reduces the likelihood of a system’s test data being skewed due its being testing first or last for a disproportionate percentage of users.

In addition to the standard FMR, FTE, and FNMR test processes, Visit 1 incorporates an “additional effort” test of a system’s ability to enroll users originally unable to enroll in a given system. The subject is (1) given expanded enrollment instructions and (2) prompted to enroll, if possible, a different set of biometric data. For example, a subject may be prompted to re-attempt enrollment through an alternate fingerprint or through an alternate passphrase. This data is compiled separately from standard FTE data.

Test Process: Secondary Visit

International Biometric Group retests the Primary Visit enrollees approximately six weeks after their initial enrollment and verification testing. The Secondary Visit determines the ability of systems to verify users when a substantial time period is introduced between enrollment and verification.

Secondary Visit testing consists of true verification, meaning that subjects are asked to verify against their previous enrollment. There is no false verification testing. The same procedures used for true verification testing in the Primary Visit testing are repeated during the Secondary Visit. On systems with adjustable thresholds, subjects initially attempt verification at high security; if a system falsely rejects a subject, the test is repeated at the medium threshold. If a system falsely rejects a subject at the medium threshold, the subject attempts verification at the low threshold.

After true verification testing, subjects are asked to fill out a market research survey and questionnaire.

The procedures for the Secondary Visit true verification testing are identical to the true verification testing performed in the Primary Visit.

Test Deliverables

After the primary visits are completed, each vendor tested will receive a high-level report with its own technology's accuracy data from the first visit, including FMR, FTE, and FNMR data. Each vendor will have the opportunity to respond in writing to the primary visit results, and those written comments will be included in the Final Report.

Also after the primary visits are completed, sponsors will receive a preliminary report with accuracy data collected for all of the vendors.

After the completion of the secondary visits, each vendor will be provided with its own technology's accuracy data from the second visit, including FMR, FTE, and FNMR data. Each vendor will again have the opportunity to respond in writing to these results, and those written comments will be included in the Final Report.

Each paying participant in the testing (i.e., sponsors and purchasers) will receive a Final Report. Vendors who have not paid to participate in the testing will not receive the Final Report, but they are welcome to purchase the Final Report if they wish. The Final Report will include substantial data and detailed analysis related to system performance, usability, user perception, and notable data trends.

About International Biometric Group

IBG is an independent biometric consulting and integration firm. IBG is vendor-independent and technology-neutral. IBG is not affiliated with any university, government agency, or biometric vendor.

2. Test Philosophy

2.1. Introduction

International Biometric Group's Comparative Biometric Testing evaluates the ability of biometric systems to enroll and verify individuals under controlled, real-world operating conditions. The data collected, evaluated, and reported for biometric systems includes (but is not limited to) false match rates (FMR), failure to enroll rates (FTE), and false non-match rates (FNMR). To evaluate systems' susceptibility to false non-matching over time, the testing includes subject verification over the course of two visits spread approximately six weeks apart.

The primary purpose of Comparative Biometric Testing is to help public and private sector institutions determine the degree to which commercially available biometric systems are suitable for deployment in logical access and physical access applications. Independent data related to matching accuracy and enrollment rates under real-world enrollment and matching conditions – such as those encountered in an office, workplace, or home – has traditionally been lacking in the biometric industry. Such data, however, is an essential component of making informed decisions on deployment, technology acquisition, and product development.

2.2. Test Principles

Three basic principles are followed to ensure the accuracy, applicability, and integrity of Comparative Biometric Testing.

- Emphasis on COTS (Current off-the-shelf) solutions

Comparative Biometric Testing focuses primarily on commercially available biometric systems, as opposed to systems whose functionality has been modified – through design, development, or integration – for this test effort. This ensures that testing is reflective of the capabilities of state-of-the-art technologies as made available to deployers, end users, and systems integrators.

- Emphasis on scenario testing as opposed to utilization of static or recorded data

Comparative Biometric Testing evaluates the core biometric functionality of commercially available systems – sample acquisition, feature extraction, and matching capabilities – hand-in-hand with device ergonomics, system usability, and ease of sample submission. This scenario-driven approach ensures that results are indicative of the full biometric system's capabilities as opposed to being solely indicative of the matching or extraction algorithms. Close control of test conditions ensures that environmental factors do not impact test results.

- Normalization of parameters for defining false matches, failures to enroll, and false non-matches

One of the major challenges in scenario testing is defining the points at which false matching, failure to enroll, and false non-matching are judged to have occurred. Comparative Biometric Testing normalizes the points at which enrollment and matching error events are defined for different biometric systems according to ”reasonable effort, reasonable risk” criteria. The normalization of enrollment and matching error event ensures that error rates can be compared across biometric systems with dissimilar enrollment and matching processes, and to ensure that systems are neither penalized nor rewarded for their particular enrollment and verification processes. Please refer to Section 6.2, *Defining False Match, Failure to Enroll and False Non-Match Events*, for a full discussion of this issue.

3. Test Participation and System Selection

3.1. Test Participation

IBG testing is conducted to determine the degree to which commercially available biometric systems are suitable for deployment in logical access and physical access applications. IBG makes test results available for purchase, and for qualified organizations who sponsor the testing, provides a means for companies to nominate a specific system to be tested.

Test Sponsors. Test Sponsors represent the interests of the commercial and government markets. Test Sponsors provide IBG with general input and feedback on the interests of the marketplace in comparative testing, and are allowed to nominate one system per Test round. Biometric vendors are not permitted as Test Sponsors.

Test Pre-Purchasers. Test Pre-purchasers are commercial or government institutions that commit to purchasing test results prior to the beginning of a given Round. Test Pre-Purchasers are allowed to nominate one system per Test round. Biometric vendors are allowed to pre-purchase test results and to nominate one system per Test round; and they may nominate their own system for testing, so long as it meets IBG test criteria.

Test Purchasers. Test purchasers are commercial or government institutions who purchase test results once a Round has begun or subsequent to a Round's completion. Biometric vendors are allowed to purchase Test results.

Test Sponsors	Test Pre-Purchasers	Test Purchasers
• Provide general input and feedback on industry interests in comparative testing • Allowed to nominate 1 system per Test round • Biometric vendors are not permitted as Test sponsors	• Commit to purchasing test results prior to beginning of a given Round • Allowed to nominate 1 system per Test round • Biometric vendors are allowed to pre-purchase test results and to nominate 1 system per Test round, including their own technology	• Purchase test results once a Round begins or subsequent to a Round's completion • Any organization is allowed to purchase Test results • Do not nominate systems

Figure 1: Categories of Test Participation

3.2. System Selection

Comparative Biometric Testing focuses primarily on commercially available biometric systems, as opposed to systems whose functionality has been modified – through design, development, or integration – for this test effort. This ensures that testing is reflective of the capabilities of state-of-the-art technologies as made available to deployers, end users, and systems integrators. IBG reviews system nominations with Test Sponsors and Test Pre-Purchasers to resolve any questions regarding the suitability of a nominated system for testing. A system must be capable of acquiring “live” biometric data, generating an enrollment template, associating this enrollment with a unique identifier, executing match attempts against this template, and indicating the results of match attempts.

Final system selection, including decisions regarding the suitability of a particular system for testing, is the sole responsibility of IBG.

3.3. Availability of Test Results

After the primary visits are completed, each vendor tested will receive a report with its own technology’s accuracy data from the first visit, including FMR, FTE, and FNMR data. Each vendor will have the opportunity to respond in writing to the primary visit results, and those written comments will be included in the Final Report.

Also after the primary visits are completed, sponsors will receive a preliminary report with accuracy data collected for all of the vendors.

After the completion of the secondary visits, each vendor will be provided with its own technology’s accuracy data from the second visit, including FMR, FTE, and FNMR data. Each vendor will again have the opportunity to respond in writing to these results, and those written comments will be included in the Final Report.

Each paying participant in the testing (i.e., sponsors and purchasers) will receive a Final Report. Vendors who have not paid to participate in the testing will not receive the Final Report, but they are welcome to purchase the Final Report if they wish. The Final Report will include substantial data and detailed analysis related to system performance, usability, user perception, and notable data trends.

International Biometric Group permits tested vendors who have purchased the Final Report to publish a limited set of test data under strict release terms. This data is limited to a single FMR/FNMR pair for their system during the Primary Visit at one threshold. Only vendors who have purchased the Final Report may publish the data because they have the opportunity to read the full report and to understand their results in the context of the other systems. Vendors must complete a release (see Appendix D) and receive written approval from IBG prior to releasing any data.

All other test data is held strictly confidential and may not be shared, disclosed, or distributed without International Biometric Group’s express prior written permission.

4. Test Facilities and Testing Environment

4.1. Test Facilities

Comparative Biometric Testing takes place at IBG facilities in New York City.

4.2. Testing Environment

The test laboratory consists of dedicated workstations for peripheral devices, tables for standalone systems, and assigned spaces for systems that require distance between test subjects and acquisition devices (such as certain facial-scan systems). This facilitates meaningful and consistent data collection for logical and physical access systems.

Care is taken to ensure that systems are tested in a fashion consistent with their intended use in logical or physical access systems. Depending on the technology tested, users may be standing or seated, although test subjects are not allowed discretion in the manner of interacting with systems.

To ensure that external factors such as temperature, lighting conditions, and background noise do not impact system performance, the testing environment in IBG's test laboratory is closely controlled. At the beginning of each test session, temperature and humidity are measured and any necessary adjustments are made to ensure consistent operating conditions.

5. Test Center Personnel

5.1. Test Schedulers

Test schedulers are responsible for scheduling and confirmation of initial and subsequent test visits. Test schedulers also prepare data sheets prior to subject arrival.

5.2. Test Examiners

Skilled test examiners are a critical element of Comparative Biometric Testing. Test examiners are responsible for the following:

- Accompanying and directing test subjects during their interaction with test systems.
- Noting temperature and humidity measurements in the test area at the beginning and end of each testing day.
- Providing scripted test instructions and ensuring compliance with these instructions
- Briefly demonstrating for subjects the manner of interaction with test systems
- Providing additional instructions when warranted according to test protocols
- Collecting test data including incidents of false matching, failure to enroll, and false non-matching; number of verification attempts at each security level; and number of placements or submissions necessary to enroll and verify
- Adjusting security thresholds during verification attempts
- Entering subject ID numbers for false match attempts, enrollment, and verification attempts
- Monitoring operation of test systems
- Conducting exit surveys to collect subject feedback regarding ease of use, intrusiveness, and privacy impact
- Noting any relevant comments provided by subjects during testing

IBG staff are highly familiar with biometric system operations and serve as test examiners. This ensures consistency of data collection throughout the test process. In order to accurately track subject interaction with systems, test examiners accompany a single subject, and are not responsible for instructing multiple subjects simultaneously.

5.3. Data Entry Staff

Subsequent to subject testing, data sheets are provided to data entry staff for logging, insertion into spreadsheets, and reconciliation. Data entry staff are responsible for the following:

- Manual entry of test data into preformatted spreadsheets

- Ensuring consistency within data sheets, for example, crosschecking the recorded number of verification attempts at each security level versus match results
- Resolving any discrepancies or anomalies in data sheets through interaction with test examiners

6. Test Subject Management

6.1. Overview

Because the test scenario incorporates two separate visits, managing the test subjects is a critical issue. The most important factors are: ensuring that all the data is gathered correctly, associating test subject IDs with the correct individuals, maintaining a constant flow of individuals, and maintaining a good retention rate.

6.2. Subjects' Data Records

Each subject will have several data sheets active at any given time for each test system:

- An enrollment form
- A verification form for each visit
- A checklist

The checklist is used to monitor the subject's progress for each system. All forms are filed according the subject ID; the subject's name does not appear on any forms.

6.3. The Subject ID List

The Subject ID list is maintain by Test Schedulers, and maps the subjects' names and contact details to their test IDs. This information is kept strictly separate from the data sheets collected during testing.

6.4. Maintaining the Test Population Size

The testing will have an initial Test Subject population of 240 individuals. In an ideal world, the test population would remain stable from the first visit to the second visit. In practice, however, not all Test Subjects will return for the second visit. Test Subjects are given modest co-payments upon successful completion of each visit. While this type of incentive can help to maintain the test population and ease recruitment – IBG ensures a minimum 80% retention rate from the first visit to the second visit.

7. System Acquisition, Configuration, and Installation

7.1. Acquisition of Biometric Systems

After final system selection, IBG contacts vendors to inform them of their nomination. Vendors unfamiliar with IBG’s Comparative Biometric Testing are provided with information on IBG’s testing, test principles, and test objectives. This ensures that vendors can make informed decisions on participation in IBG testing. Vendors are not required to participate in IBG testing, and may decline to provide a system if nominated. In the case that a vendor whose system has been nominated does not wish to participate, the nominating organization is notified to identify a replacement system selection. As a condition of testing, vendors are required to sign a release and a confidentiality agreement.

IBG provides vendors with test milestone dates and the test plan, and establishes a primary point of contact through whom issues are resolved relating to system operations and settings.

In the event that a selected vendor has more than one system version appropriate for logical and physical access applications, the vendor is asked to provide their "most robust and representative system model version" whose core technology is suitable for logical and physical access applications. Based on IBG’s experience with biometric devices and technology, each system is evaluated to ensure its suitability for testing.

7.2. Configuration of Test PCs

For systems tested as peripheral devices, IBG provides PCs on which the biometric hardware and software will be installed. All PCs are similarly configured in terms of version of operating system, display resolution, and RAM. The default OS is Windows 2000, although alternative operating systems can be installed if necessary. IBG reserves the right to substitute PCs with equivalent hardware specifications.

If a vendor's biometric system cannot operate on the PCs provided for testing, vendors may provide a test PC. The specifications of all test PCs are included in the final report.

7.3. Installation and Testing of Biometric Systems

The vendor must provide all software and peripheral equipment (including scanners, cables, etc.) necessary for the system to function. Once the systems are in IBG's possession, we note the hardware and software model numbers, serial numbers and version numbers.

Vendors are allowed (but not required) to install and configure their systems onsite at IBG's test facility. Subsequent to system installation and prior to test initiation, IBG reviews the systems to ensure that they operate and function properly. In the case of any malfunctions, anomalies, or system instability, vendors are contacted and asked to either provide direction on correcting malfunctions or to visit the test facility for troubleshooting. Any malfunctions or system instability encountered during testing are addressed on a case-by-case basis to determine whether vendor involvement is warranted.

The date when all the biometric systems are configured and functioning properly is known as the Acquisition Date. Upon the Acquisition Date, the vendors are not allowed to update, modify or alter their systems for the remainder of the Test, except for the resolution of malfunctions as stated above.

7.4. Threshold Settings

Many biometric systems have verification threshold settings that can be adjusted to meet deployer requirements for security and convenience. In order to maximize the amount of relevant test data collected, IBG requests that each vendor provide three verification threshold settings: *high security*, *medium security,* and *low security*.

- *High security* is intended to indicate a system's performance when configured to be most resistant to false matching while still providing reasonable resistance to false non-matching.

- *Medium security* is intended to indicate a system's performance when configured to attain the strongest balance between false matching and false non-matching.

- *Low security* is intended to indicate a system's performance when configured to be most resistant to false non-matching while still providing reasonable resistance to false matching.

Vendors are allowed to custom-configure these thresholds or to select pre-existing security levels which best reflect the aforementioned thresholds. Vendors are not required to provide multiple threshold settings, and may opt to utilize a single setting if they so choose.

8. Test Protocols

8.1. Overview

International Biometric Group's Comparative Biometric Testing evaluates the ability of biometric systems to enroll and verify individuals within logical and physical access test scenarios. The data collected, evaluated, and reported for biometric systems includes (but is not limited to) false match rates (FMR), failure to enroll rates (FTE), and false non-match rates (FNMR). To evaluate systems' susceptibility to false non-matching over time, the testing includes subject verification over two visits spread across six weeks.

The testing assesses FMR and FNMR at three (3) security thresholds – high security, medium security, and low security. If vendors do not provide adjustable thresholds, systems are tested at a single threshold of the vendor's choosing.

240 non-acclimated test subjects recruited from the general population comprise the test population. The testing is based on real-time enrollment and verification of subjects as opposed to offline comparison of static or recorded biometric samples. This methodology provides results reflective of (1) feature extraction and matching algorithm robustness and (2) device ergonomics, system usability, and ease of sample submission.

Testing is divided into a Primary Visit and a Secondary Visit. Test data collected during Visit One includes FMR, FTE, and FNMR. Test data collected during Visit Two includes FNMR.

Test instructors accompany and direct subjects throughout the testing in order to provide scripted instructions, manually collect data, record test subject comments, and to address any anomalies.

8.2. Test Subject Visits

During a Test Subject's Primary Visit, he performs false match testing, enrollment testing, and false non-match testing in each biometric system.

During a Test Subject's Secondary Visit, he performs false non-match testing in those same systems from the 1st visit in which he or she successfully enrolled. The first visit lasts approximately 1 hour, and the second visit lasts about one half hour.

8.2.1. Primary Visit: Initial Data Collection and Forms

On the test subject's initial visit to IBG's testing facilities, greeting staff gather test subject demographic data. The test subject is assigned a unique subject ID and introduced to a test instructor. The test instructor reads a brief, scripted overview of the test effort to the test subjects. Forms used and issued in Initial Data Collection are as follows:

- **Agreements to Participate.** Agreements to Participate establish the conditions of participation in Comparative Biometric Testing.

- **Subject Data Forms.** Subject Data Forms collect Test Subjects' data such as age, sex, race, height, weight, and occupation.

- **Test Scripts.** Test Scripts are narratives used by Test Instructors to guide test subjects through the various test components. Scripts incorporate placement advice that examiners may read to test subjects when necessary.

- **Test Data Sheets.** Test Data Sheets are used to collect test data such as match attempts, placements required to enroll, false matches at a given security level, and so forth.

  The order in which subjects interact with each system within a given Round is indicated on the Test Data Sheet. The Test Order is arranged such that in a round with N systems, each system is tested an equivalent number of times in the first position, second position, and so forth until the Nth position. This reduces the likelihood of a system's test data being skewed due its being testing first or last for a disproportionate percentage of users.

  The Data Sheet also lists two target ID numbers corresponding to two previously enrolled subjects against whom false match attempts will occur for a newly arrived test subject.

8.2.2. Primary Visit: False Match Testing

The test instructor briefly describes the manner of interacting with the first test system and demonstrates the method of providing biometric data (e.g. placing a fingerprint on a scanner). These instructions and demonstrations are scripted.

The test instructor reads scripted instructions on the process of false match testing in the first test system, indicating the number of false match attempts allowed. The test instructor enters the first target ID against which the test subject is to attempt to falsely match. The test subject attempts to fraudulently match three times against the first target subject at "low" security by providing specific biometric samples (e.g. right index fingerprints, spoken passphrases, or facial images) as per test instructions.

If on the first match attempt the test instructor determines that the test subject has submitted biometric samples in an egregiously incorrect fashion (such as placing only the tip of the finger on a scanner or failing to speak properly into a microphone), the first false match attempt is waived, instructions are provided to ensure proper sample submission, and the sequence begins again.

If a false match occurs on any of the three attempts, the test instructor adjusts the security level to “medium.” The test subject attempts to fraudulently match three times against the first target subject at medium security. If a false match occurs on any of the three attempts, the test instructor adjusts the security level to “high.” The test subject attempts to fraudulently match three times against the first target subject at high security.

After cycling through false match tests against the first target subject, the test subject attempts to falsely match against the second target subject. The protocols for the second test subject are identical to those of the first.

Data recorded by the test instructor during Primary Visit False Match Testing is as follows:

- Number of placements and attempts to match at each security threshold against each target subject
- Number of successful and unsuccessful false match attempts against each target subject
- (If applicable) match scores associated with each false match attempt
- Incidence of egregiously incorrect biometric sample submission
- Unsolicited comments provided by the test subject

8.2.3. Primary Visit: Enrollment

The test subject proceeds to attempt enrollment in the first test system. The test instructor reads scripted instructions on the process of enrollment to the test subject, indicating the number of placements, passphrases, or samples required to enroll. The test instructor establishes a new user with the test subject’s ID, and fills any other fields required to initiate an enrollment sequence with generic information.

The subject is allowed two “enrollment sequences” in which to enroll successfully in the first system by providing specific biometric samples (e.g. right index fingerprints, spoken passphrases, or facial images) as per test instructions. If the subject is unable to enroll on the first attempt, the test instructor may need to reenter test subject data prior to the second enrollment attempt.

If on the first enrollment attempt the test instructor determines that the test subject has submitted biometric samples in an egregiously incorrect fashion (such as placing only the tip of the finger on a scanner or failing to speak properly into a microphone), the first false match attempt is waived, instructions are provided to ensure proper sample submission, and the sequence begins again.

If the user is unable to enroll after two attempts, the test instructor initiates an “Additional Effort” enrollment sequence designed to measure a system’s failure to enroll rate when test subjects are provided with additional guidance on enrollment. The subject is given scripted, expanded enrollment instructions, which may involve demonstrations of interaction with acquisition devices. If possible, test subjects are prompted to enroll using a different biometric sample. For example, a subject may be prompted to re-attempt enrollment through an alternate fingerprint or through an alternate passphrase. “Additional Effort” enrollment data is compiled separately from primary failure to enroll data.

Test subjects unable to enroll during either the primary or “Additional Effort” enrollment sequences are escorted to the next test system and do not attempt true match attempts, as there is no enrollment data against which to attempt true matching.

Data recorded by the test instructor during Primary Visit Enrollment Testing is as follows:

- Number of sample submissions required to enroll during primary enrollment testing
- Number of attempts required to enroll during primary enrollment testing
- (If applicable) number of sample submissions required to enroll during “Additional Effort” enrollment testing
- (If applicable) number of attempts required to enroll during “Additional Effort” enrollment testing
- Incidence of egregiously incorrect biometric sample submission
- Unsolicited comments provided by the test subject

8.2.4. Primary Visit: True Match Testing

Enrolled test subjects proceed to attempt to match against their enrollment. The test instructor reads scripted instructions on the process of true match testing in the first test system, indicating the number of true match attempts allowed. The test instructor enters the test subject’s ID. The test subject attempts to match three times against his or her enrollment at “high” security by providing specific biometric samples (e.g. right index fingerprints, spoken passphrases, or facial images) as per test instructions.

If on the first match attempt the test instructor determines that the test subject has submitted biometric samples in an egregiously incorrect fashion (such as placing only the tip of the finger on a scanner or failing to speak properly into a microphone), the first true match attempt is waived, instructions are provided to ensure proper sample submission, and the sequence begins again.

If the test subject is unable to match within three attempts, the test instructor adjusts the security level to “medium.” The test subject attempts to match three times at medium security. If the test subject is unable to match within three attempts, the test instructor adjusts the security level to “low.” The test subject attempts to match three times at low security.

Data recorded by the test instructor during Primary Visit True Match Testing is as follows:

- Number of sample submissions required to match at each security threshold
- Number of successful and unsuccessful match attempts
- (If applicable) match scores resulting from each match attempt
- Incidence of egregiously incorrect biometric sample submission
- Unsolicited comments provided by the test subject

8.2.5. Primary Visit: Additional False Match Testing for Finger-Scan Systems

These tests are designed to measure finger-scan systems' false match rates for same-subject alternate fingerprints

In order to maximize the amount of data collected during False Match Testing, an additional series of tests are conducted for finger-scan systems. Test subjects able to enroll in a given finger-scan system attempt to match their middle fingerprint against their enrolled index fingerprint from the same hand. The test subject attempts to falsely match three times against his or her enrolled fingerprint at "low" security.

If a false match occurs on any of the three attempts, the test instructor adjusts the security level to "medium." The test subject attempts to fraudulently match three times against his or her enrolled fingerprint at medium security. If a false match occurs on any of the three attempts, the test instructor adjusts the security level to "high." The test subject attempts to fraudulently match three times against his or her enrolled fingerprint at high security.

Data recorded by the test instructor during Primary Visit False Match Alternate Fingerprint Testing is as follows:

- Number of placements and attempts to match at each security threshold
- Number of successful and unsuccessful match attempts
- (If applicable) match scores resulting from each match attempt
- Incidence of egregiously incorrect biometric sample submission
- Unsolicited comments provided by the test subject

8.2.6. Primary Visit: Conclusion

Once a test subject has executed all applicable tests for each test system, the Primary Visit is complete.

For Rounds in which the biometric disciplines tested utilize readily acquired identifiable biometric data (finger-scan, facial-scan, and voice-scan), the test subject also provides identifiable biometric data to be stored in a database for systems analysis.

8.3. Secondary Visit: True Match Attempts over Time

These tests are designed to measure systems' false non-match rates over time.

Approximately six weeks days subsequent to the Primary Visit testing test subjects return for further testing in which the subject attempts to match against his or her existing enrollments in all systems in which he or she enrolled during the Primary Visit. This ensures the collection of substantial FNMR data over time.

The test protocol for the Secondary Visit is identical to the Primary Visit True Match testing. The test subject attempts to match three times against his or her enrollment at high security by providing specific biometric samples (e.g. right index fingerprints, spoken passphrases, or facial images) as per test instructions.

If on the first match attempt the test instructor determines that the test subject has submitted biometric samples in an egregiously incorrect fashion (such as placing only the tip of the finger on a scanner or failing to speak properly into a microphone), the first true match attempt is waived, instructions are provided to ensure proper sample submission, and the sequence begins again.

If the test subject is unable to match within three attempts, the test instructor adjusts the security level to medium. The test subject attempts to match three times at medium security. If the test subject is unable to match within three attempts, the test instructor adjusts the security level to low. The test subject attempts to match three times at low security.

Data recorded by the test instructor during the Secondary Visit is as follows:

- Number of sample submissions required to match at each security threshold
- Number of successful and unsuccessful match attempts
- (If applicable) match scores resulting from each match attempt
- Incidence of egregiously incorrect biometric sample submission
- Unsolicited comments provided by the test subject

After the Secondary Visit True Match Attempts, an exit survey is conducted wherein users are asked to rate systems based on their impressions of the systems' ease of use, intrusiveness, and impact on privacy. These terms are briefly defined prior to collection of this exit survey data to ensure that users have a basic understanding of what is meant by terms such as intrusiveness and privacy impact. The exit survey is reproduced in Appendix G.

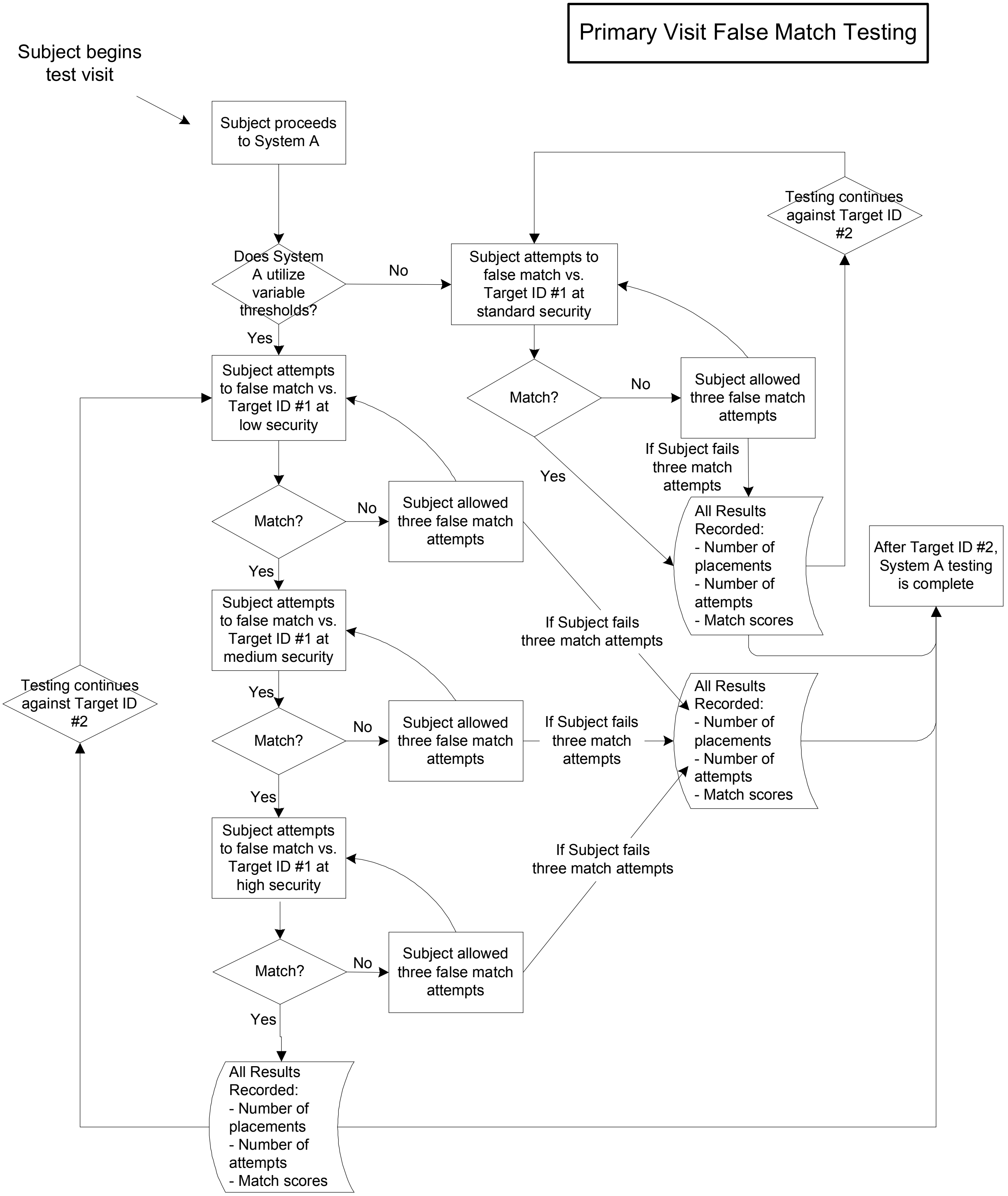
Primary Visit False Match Testing
Subject begins test visit
Subject proceeds to System A
Does System A utilize variable thresholds?
No
Yes
Subject attempts to false match vs. Target ID #1 at standard security
Match?
No
Subject allowed three false match attempts
Yes
If Subject fails three match attempts
All Results Recorded: - Number of placements - Number of attempts - Match scores
Testing continues against Target ID #2
After Target ID #2, System A testing is complete
Subject attempts to false match vs. Target ID #1 at low security
Match?
No
Subject allowed three false match attempts
Yes
Subject attempts to false match vs. Target ID #1 at medium security
Yes
Match?
No
Subject allowed three false match attempts
If Subject fails three match attempts
If Subject fails three match attempts
All Results Recorded: - Number of placements - Number of attempts - Match scores
Yes
Subject attempts to false match vs. Target ID #1 at high security
Match?
No
Subject allowed three false match attempts
If Subject fails three match attempts
Yes
All Results Recorded: - Number of placements - Number of attempts - Match scores
Testing continues against Target ID #2

Figure 2: Primary Visit False Match Testing

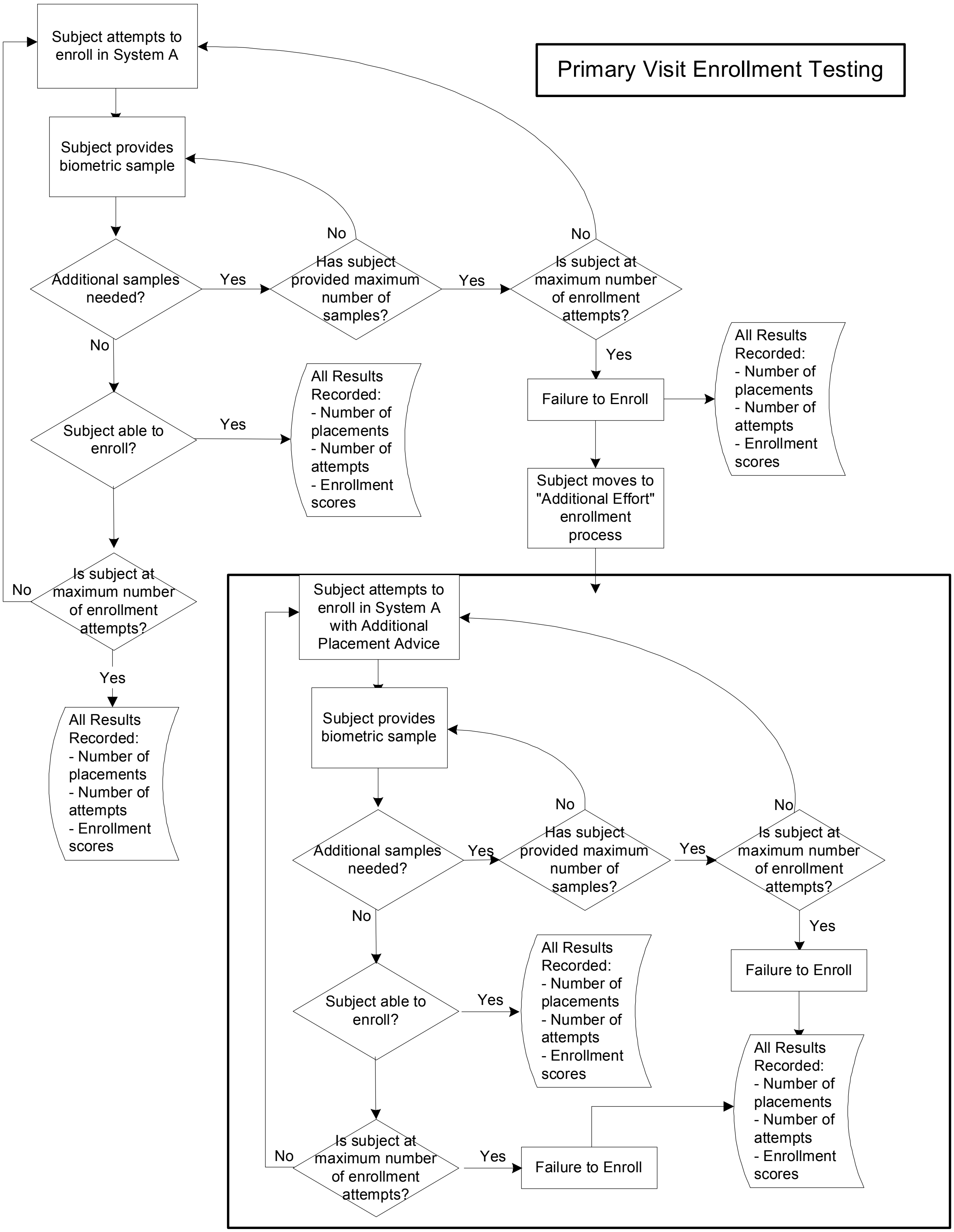
Primary Visit Enrollment Testing
Subject attempts to enroll in System A
Subject provides biometric sample
Additional samples needed?
Yes
No
Has subject provided maximum number of samples?
No
Yes
Is subject at maximum number of enrollment attempts?
No
Yes
Failure to Enroll
All Results Recorded:
- Number of placements
- Number of attempts
- Enrollment scores
Subject moves to "Additional Effort" enrollment process
Subject able to enroll?
Yes
All Results Recorded:
- Number of placements
- Number of attempts
- Enrollment scores
Is subject at maximum number of enrollment attempts?
No
Yes
All Results Recorded:
- Number of placements
- Number of attempts
- Enrollment scores
Subject attempts to enroll in System A with Additional Placement Advice
Subject provides biometric sample
Additional samples needed?
Yes
No
Has subject provided maximum number of samples?
No
Yes
Is subject at maximum number of enrollment attempts?
No
Yes
Failure to Enroll
All Results Recorded:
- Number of placements
- Number of attempts
- Enrollment scores
Subject able to enroll?
Yes
All Results Recorded:
- Number of placements
- Number of attempts
- Enrollment scores
Is subject at maximum number of enrollment attempts?
No
Yes
Failure to Enroll

Figure 3: Primary Visit Enrollment Testing

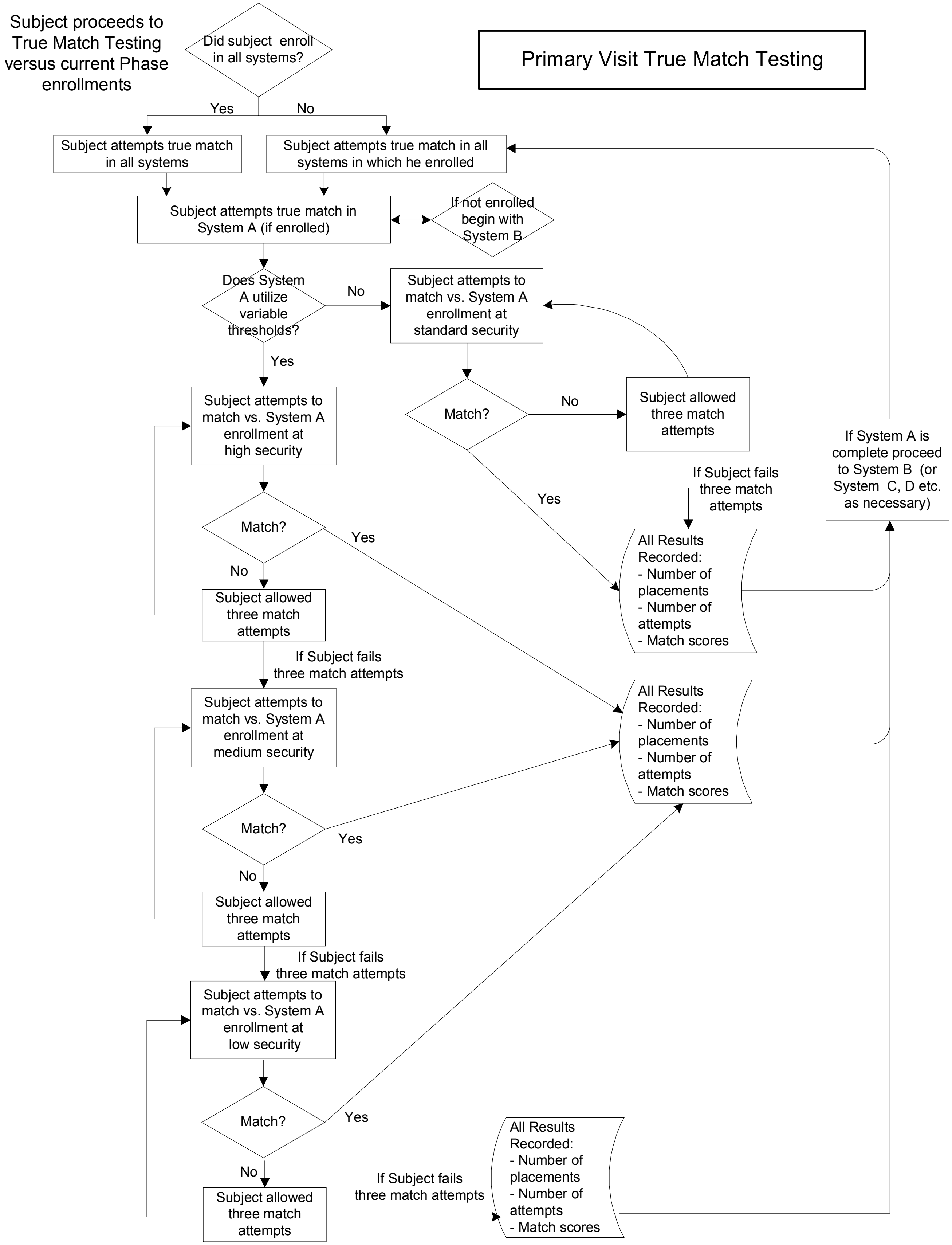
Subject proceeds to True Match Testing versus current Phase enrollments
Did subject enroll in all systems?
Primary Visit True Match Testing
Yes
No
Subject attempts true match in all systems
Subject attempts true match in all systems in which he enrolled
Subject attempts true match in System A (if enrolled)
If not enrolled begin with System B
Does System A utilize variable thresholds?
No
Subject attempts to match vs. System A enrollment at standard security
Yes
Subject attempts to match vs. System A enrollment at high security
Match?
No
Subject allowed three match attempts
If Subject fails three match attempts
Yes
If System A is complete proceed to System B (or System C, D etc. as necessary)
Match?
Yes
No
Subject allowed three match attempts
If Subject fails three match attempts
All Results Recorded:
- Number of placements
- Number of attempts
- Match scores
Subject attempts to match vs. System A enrollment at medium security
All Results Recorded:
- Number of placements
- Number of attempts
- Match scores
Match?
Yes
No
Subject allowed three match attempts
If Subject fails three match attempts
Subject attempts to match vs. System A enrollment at low security
Match?
Yes
No
Subject allowed three match attempts
If Subject fails three match attempts
All Results Recorded:
- Number of placements
- Number of attempts
- Match scores

Figure 4: Primary Visit True Match Testing

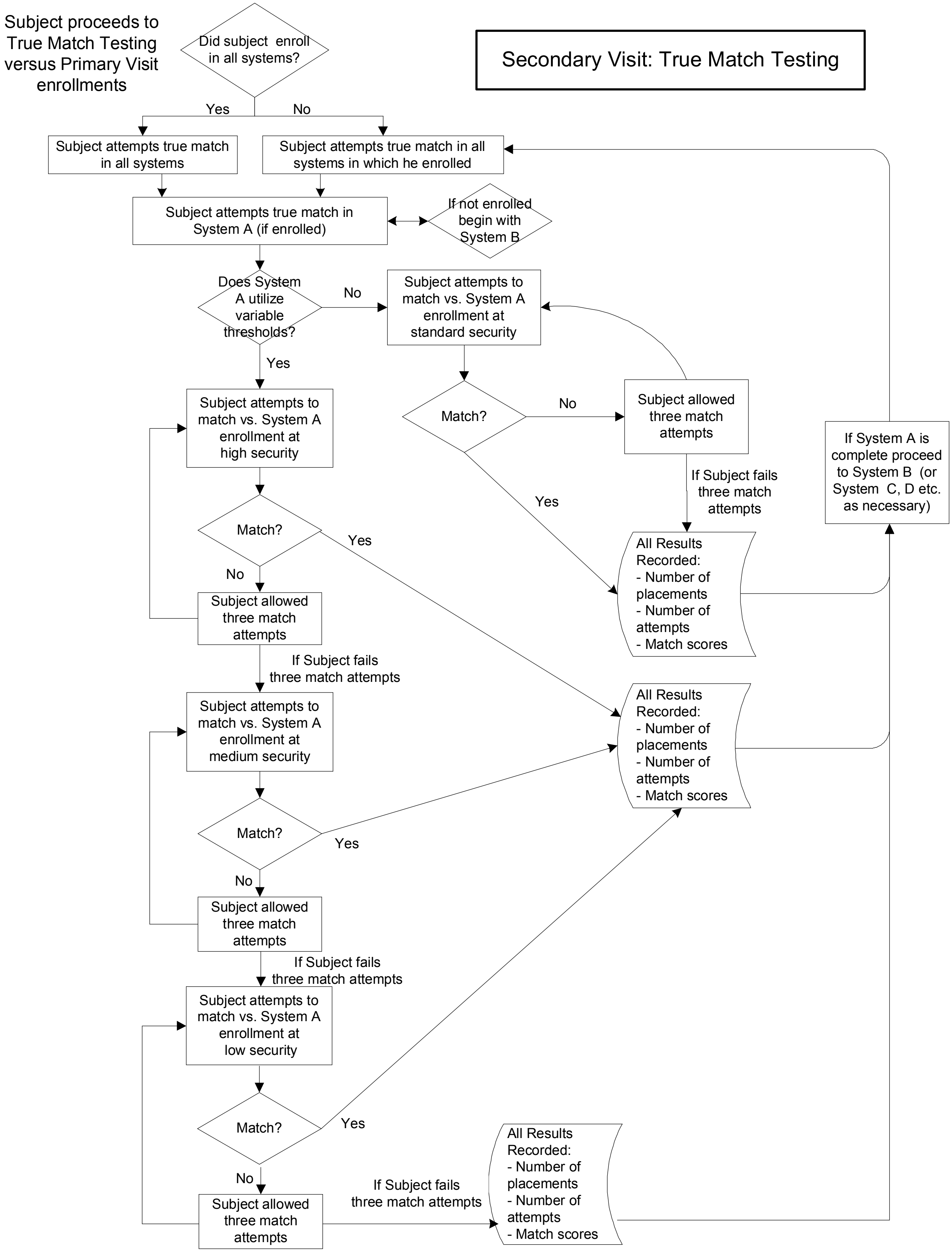
Subject proceeds to True Match Testing versus Primary Visit enrollments
Did subject enroll in all systems?
Secondary Visit: True Match Testing
Yes
No
Subject attempts true match in all systems
Subject attempts true match in all systems in which he enrolled
Subject attempts true match in System A (if enrolled)
If not enrolled begin with System B
Does System A utilize variable thresholds?
No
Subject attempts to match vs. System A enrollment at standard security
Yes
Match?
No
Subject allowed three match attempts
Subject attempts to match vs. System A enrollment at high security
If Subject fails three match attempts
Yes
If System A is complete proceed to System B (or System C, D etc. as necessary)
Match?
Yes
No
All Results Recorded: - Number of placements - Number of attempts - Match scores
Subject allowed three match attempts
If Subject fails three match attempts
Subject attempts to match vs. System A enrollment at medium security
All Results Recorded: - Number of placements - Number of attempts - Match scores
Match?
Yes
No
Subject allowed three match attempts
If Subject fails three match attempts
Subject attempts to match vs. System A enrollment at low security
Match?
Yes
No
If Subject fails three match attempts
Subject allowed three match attempts
All Results Recorded: - Number of placements - Number of attempts - Match scores

Figure 5: Secondary Visit True Match Testing

8.4. Defining False Match, Failure to Enroll, and False Non-Match Events

Defining the point at which a subject can reasonably be judged to have false matched, failed to enroll, or false non-matched is one of the biggest challenges in biometric scenario testing. Within Comparative Biometric Testing, the number of false match attempts, enrollment attempts, and true match attempts permitted before declaring a false match, failure to enroll, or false non-match are normalized to the degree possible across technologies and devices. The normalization of enrollment and matching error events allows comparative accuracy results to be generated for biometric systems with dissimilar enrollment and matching processes.

8.4.1. False Match Events

Background. In most logical and physical access applications, there is a limit to the amount of number of placement attempts an individual is permitted in order to match successfully. Comparative Biometric Testing establishes normalized parameters on placements, time, and/or verification sequences permitted to successfully match in test systems. Ability to successfully match as an imposter against a target subject’s enrollment within normalized parameters is recorded as a false match.

Biometric systems vary widely in the point at which they disallow further match attempts subsequent to failure to match against enrolled data. Systems may allow only one match attempt before reverting to a backup or lockout mode, or may allow multiple attempts to match successfully. Other systems may terminate a matching sequence after a certain period of time if the user does not match successfully. On the other hand, certain systems may not define a point at which further match attempts are disallowed, instead cycling through an indefinite match loop.

Determining the point at which a false match occurs is complicated by the fact that a subject might provide a biometric sample of insufficiently high quality to generate a match template. A subject may place a finger on a scanner but not generate a match template, such that no match attempt occurs. In this case, the system will not have rendered a “no match” decision, although a placement will have occurred. A further complication is the fact that a subject might hold his or her finger on a scanner for several seconds, such that a series of match attempts takes place.

False Match Protocols. For most systems involved in Comparative Biometric Testing, false match protocols are defined such that the subject is allowed one false match sequence to match against a target subject’s enrollment data. A false match sequence is defined as three placements or sample provisions (e.g. spoken passphrases) or, for systems such as certain facial-scan technologies which acquire and attempt to match a continuous stream of images, a single time-limited matching cycle. In failure to acquire situations wherein a placement does not result in the generation of a match template, placements are terminated after two seconds of the subject’s active provision of the biometric sample (for example within two seconds of a finger coming into full contact with a scanner).

Successfully matching against a target subject’s enrollment data at any point during a false match sequence is recorded as a false match; conversely, inability to match against a target subject’s enrollment data at any point during a false match sequence is recorded as a true non-match. For example, matching on any of three placements or sample provisions, or on any match attempts executed through acquisition of a continuous data stream, is recorded as a false match. Exceptions to this protocol include (1) systems with match processes whose length is such that allowing three placements would be inconsistent with the requirements of most logical or physical access implementations and (2) continuous data stream systems which do not “time out”, or halt match attempts, within a reasonable amount of time. In such systems, fewer than three placements may be permitted or a specific amount of time may be allotted (typically 10 seconds) for false match attempts.

Normalization of False Matching. Comparative Biometric Testing normalizes the points at which false matching error events are defined for dissimilar biometric systems according to ”reasonable effort, reasonable risk” criteria. Considerable effort is put forth to avoid either penalizing or rewarding those systems with comparatively lengthy or abbreviated matching processes. In most cases, subjects are allowed three placements or sample submissions to match against a target subject’s enrollment data.

Typical System	System's Matching Parameters	Normalization of FMR
Facial-scan System 1	• Three match attempts permitted before matching sequence terminated • Match attempt requires acquisition of an acceptable sample (facial image) • Facial images acquired through video snapshots • Match attempt times out if an acceptable facial image is not acquired within five seconds	A false match is recorded if a match occurs on any of three facial image acquisitions; acquisition without template generation is recorded as a match attempt; 'time out' due to failure to acquire an acceptable image is recorded as a false match attempt
Facial-scan System 2	• One matching cycle permitted before matching sequence terminated • Match attempt requires acquisition of an acceptable sample (facial image) • Matching cycle defined as the continuous attempted acquisition and matching of facial images for 10 seconds through a video camera	A false match is recorded if a match occurs within one matching cycle
Finger-scan System 1	• One verification attempt permitted before verification sequence terminated • Verification attempt requires acquisition of an acceptable sample (fingerprint image)	A false match is recorded if a match occurs on any of three sample acquisitions; acquisition without template generation is recorded as a match attempt; 'time out' due to failure to acquire an acceptable image is recorded as a false match attempt
Finger-scan System 2	• No limit on verification attempts permitted • Verification attempt requires acquisition of an acceptable sample (fingerprint image)	A false match is recorded if a match occurs on any of three sample acquisitions; acquisition without template generation is recorded as a match attempt; 'time out' due to failure to acquire an acceptable image is recorded as a false match attempt

Figure 6: Typical Normalization Scenarios for False Match Events

8.4.2. Failure to Enroll Events

Background. In most logical and physical access applications, there is a limit to the amount of time and effort an individual can dedicate to enrolling in a biometric system. If, for example, a number of individuals are scheduled to enroll at a given time and location, and enrollment is more time-consuming than had been anticipated, then enrollment backlogs may occur. To account for institutions' interest in minimizing the time and effort necessary to enroll in biometric systems, Comparative Biometric Testing establishes normalized limits on placements, time, and/or enrollment sequences permitted to enroll in test systems.

Defining the point at which a failure to enroll occurs is complicated by the fact that in nearly all biometric systems a successful enrollment requires acquisition of multiple acceptable biometric samples. For example, finger-scan systems often require that three fingerprint acceptable biometric samples be acquired to enroll a user. This practice reduces a system's susceptibility to false non-matching attributable to variations in biometric sample presentation. Some systems may require five acceptable biometric samples to enroll, others may require one.

In addition, biometric systems vary widely in the point at which they determine that a failure to enroll has occurred. Systems may allow five sample submissions to acquire three acceptable samples, or may allow four sample submissions to acquire two acceptable samples. System may preempt an enrollment sequence after a certain period of time; in fact, certain systems may not define a point at which a failure to enroll occurs at all, instead cycling through an indefinite enrollment loop.

Failure to Acquire versus Failure to Enroll. A user may be unable to enroll in a biometric system for two reasons:

- Inability to provide biometric samples from which features can be extracted and templates generated. This is classified in the biometric industry as a *failure to acquire*, and is reflective of insufficiently distinctive biometric data.

- Inability to provide biometric samples from which features can be extracted and templates generated. This is classified in the biometric industry as a *failure to enroll*, and is reflective of insufficiently consistent biometric data.

As the purpose of scenario testing is to indicate the accuracy and utility of a biometric system in a reasonable recreation of a real-world operating environment, no distinction is made between failure to acquire and failure to enroll in Comparative Biometric Testing. From a deployment perspective, what is germane is the percentage of individuals who need to be authenticated through alternate means; whether this is attributable to inability to provide distinctive biometric data or inability to provide consistent biometric data is a secondary consideration.

Enrollment Protocols. For most systems involved in Comparative Biometric Testing, failure to enroll protocols are defined such that subjects are allowed two "enrollment sequences". An enrollment sequence is defined as a subject's attempting to provide (or a system's attempting to acquire) no more than a predetermined number of samples for the purpose of enrollment.

For example, in a finger-scan system in which three acceptable samples are required to enroll, an enrollment sequence may be defined as five fingerprint placements. If three acceptable samples are not acquired by the fifth placement, that particular enrollment sequence is a failed attempt, and the user is given a second opportunity to enroll consisting of five additional placements. If the user cannot provide three acceptable samples during this second enrollment sequence, he or she is a failure to enroll. Note that the limiting factor is placements, not acquisitions –

a user may place his or her finger on a platen five times (or speak five passphrases) without the system acquiring any biometric samples. This would constitute a failed enrollment sequence, as discussed in *Failure to Acquire versus Failure to Enroll*.

The exception to this protocol is for systems with enrollment processes whose duration is such that allowing two full enrollment attempts would be inconsistent with the requirements of most logical or physical access implementations. In such systems, inability to enroll after one enrollment sequence may qualify as a failure to enroll.

Normalization of Failure to Enroll. Comparative Biometric Testing normalizes the points at which enrollment error events are defined for dissimilar biometric systems according to ”reasonable effort, reasonable risk” criteria. Considerable effort is put forth to avoid either penalizing or rewarding those systems with comparatively lengthy or abbreviated enrollment processes. In most cases, subjects are allowed two placements or sample submissions beyond the minimum required for enrollment. For example, users would be allowed three placements per enrollment sequence in a system that requires one acceptable sample; users would be allowed five placements in a system that requires three acceptable samples.

Typical System	System's Enrollment Requirements	Normalization of FTE
Facial-scan System 1	• Four acceptable samples required to enroll • Sample consists of a facial image • Facial images are continuously acquired for 20 seconds through a video camera	A failure to enroll is recorded subsequent to one (1) 20-second enrollment sequence in which fewer than four acceptable samples are acquired
Facial-scan System 2	• One acceptable sample required to enroll • Sample consists of a facial image • Facial images acquired through video snapshots acquired for a period of five seconds	A failure to enroll is recorded subsequent to two (2) 5-second enrollment sequences in which no acceptable samples are acquired
Finger-scan System 1	• One acceptable sample required to enroll • Sample consists of a fingerprint image	A failure to enroll is recorded subsequent to two (2) three-placement enrollment sequences in which no acceptable samples are acquired
Finger-scan System 2	• Three acceptable samples required to enroll • Sample consists of a fingerprint image	A failure to enroll is recorded subsequent to two (2) five-placement enrollment sequences in which fewer than three acceptable samples are acquired
Voice-scan System	• Five acceptable samples required to enroll • Sample consists of a spoken passphrase	A failure to enroll is recorded subsequent to two (2) five-passphrase enrollment sequences in which fewer than three acceptable samples are acquired

Figure 7: Typical Normalization Scenarios for Failure to Enroll Events

8.4.3. False Non-Match Events

Background. In most logical and physical access applications, there is a limit to the amount of number of placement attempts an individual is permitted in order to match successfully. Comparative Biometric Testing establishes normalized parameters on placements, time, and/or verification sequences permitted to successfully match in test systems. Inability to successfully match against one's own enrollment data within normalized parameters is recorded as a false non-match.

Biometric systems vary widely in the point at which they disallow further match attempts subsequent to failure to match against enrolled data. Systems may allow only one match attempt before reverting to a backup or lockout mode, or may allow multiple attempts to match successfully. Other systems may terminate a matching sequence after a certain period of time if the user does not match successfully. On the other hand, certain systems may not define a point at which further match attempts are disallowed, instead cycling through an indefinite match loop.

Determining the point at which a false non-match occurs is complicated by the fact that a subject might provide a biometric sample of insufficiently high quality to generate a match template. A subject may place a finger on a scanner but not generate a match template, such that no match attempt occurs. In this case, the system will not have rendered a “no match” decision, although a placement will have occurred. A further complication is the fact that a subject might hold his or her finger on a scanner for several seconds, such that a series of match attempts takes place.

False Non-Match Protocols. For most systems involved in Comparative Biometric Testing, false non-match protocols are defined such that the subject is allowed one true match sequence to match against his or her enrollment data. A true match sequence is defined as three placements or sample provisions (e.g. spoken passphrases) or, for systems such as certain facial-scan technologies which acquire and attempt to match a continuous stream of images, a single time-limited matching cycle. In failure to acquire situations wherein a placement does not result in the generation of a match template, placements are terminated after two seconds of the subject’s active provision of the biometric sample (for example within two seconds of a finger coming into full contact with a scanner).

Inability to match against one’s own enrollment data for the entirety of a true match sequence is recorded as a false non-match; conversely, a successful match against one’s own enrollment data at any point during a true match sequence is recorded as a true match. For example, failure to match on each of three placements or sample provisions, or on all match attempts executed through acquisition of a continuous data stream, is recorded as a false non-match. Exceptions to this protocol include (1) systems with match processes whose length is such that allowing three placements would be inconsistent with the requirements of most logical or physical access implementations and (2) continuous data stream systems which do not “time out”, or halt match attempts, within a reasonable amount of time. In such systems, inability to match within fewer than three placements or within a given amount of time (typically 10 seconds) may qualify as a false non-match.

Normalization of False Non-Matching. Comparative Biometric Testing normalizes the points at which false non-matching error events are defined for dissimilar biometric systems according to ”reasonable effort, reasonable risk” criteria. Considerable effort is put forth to avoid either penalizing or rewarding those systems with comparatively lengthy or abbreviated matching processes. In most cases, subjects are allowed three placements or sample submissions to match against their enrolled data.

Typical System	System's Matching Parameters	Normalization of FNMR
Facial-scan System 1	• Three match attempts permitted before matching sequence terminated • Match attempt requires acquisition of an acceptable sample (facial image) • Facial images acquired through video snapshots • Match attempt times out if an acceptable facial image is not acquired within five seconds	A false non-match is recorded subsequent to failure to match after acquisition and attempted matching of three facial images *or* after three match attempts time out due to failure to acquire an acceptable image
Facial-scan System 2	• One matching cycle permitted before matching sequence terminated • Match attempt requires acquisition of an acceptable sample (facial image) • Matching cycle defined as the continuous attempted acquisition and matching of facial images for 10 seconds through a video camera	A false non-match is recorded subsequent to one 10-second matching cycle in which subject fails to match, whether due to failure to acquire or failed match attempts
Finger-scan System 1	• One verification attempt permitted before verification sequence terminated • Verification attempt requires acquisition of an acceptable sample (fingerprint image)	A false non-match is recorded subsequent to three placements in which subject fails to match, regardless of whether a match template was created
Finger-scan System 2	• No limit on verification attempts permitted • Verification attempt requires acquisition of an acceptable sample (fingerprint image)	A false non-match is recorded subsequent to three placements in which subject fails to match, regardless of whether a match template was created

Figure 8: Typical Normalization Scenarios for False Non-Match Events

Appendix A: Adherence to Best Practices for Biometric Testing

IBG's Comparative Biometric Testing adheres in nearly all respects to *Best Practices in Testing and Reporting Performance of Biometric Devices* Version 1.0[1], a reference document published by the UK Biometric Working Group (UK BWG). Comparative Biometric Testing predates the publication of this document by approximately one year.

IBG testing diverges mildly from certain recommended practices of the aforementioned document in the following respects:

- Paragraph 18 of the UK BWG document states the following:

  "…we define (a) the false match rate and (b) the false non-match rate, to be the error rates of the matching algorithm from a single attempt-template comparison…"

  While mindful of the UK BWG approach, Comparative Biometric Testing defines these error rates subsequent to a normalized number of attempts or attempt sequence. Since most logical and physical access applications allow a specific number of placements or a certain duration of interaction to grant access, IBG has found that defining error rates according to this normalized standard provides a truer reflection of performance in a real-world environment.

- While mindful of the UK BWG's primary focus on Receiver Operator Characteristic (ROC) curves, Comparative Biometric Testing views Failure to Enroll errors as a critical indicator of overall system performance, and as such places this data on a par with False Match Rate and False Non-Match Rate in overall results analysis.

- Paragraph 44 of the UK BWG document states the following:

  "For scenario evaluations, test data must be separated in time from enrollment by an interval commensurate with "template ageing" of the target system..."

  Due to its focus on scenario-based performance, Comparative Biometric Testing defines a roughly consistent period of time between enrollment and subsequent true match attempts regardless of technology. That is, Visit 2 testing occurs at the same time for finger-scan, facial-scan, iris-scan, etc., although the "healing time" for these characteristics may vary. In IBG's experience, it is rare that the healing time of a biometric characteristic strongly informs deployment decisions.

- Paragraph 47 of the UK BWG document states the following:

[1] www.cesg.gov.uk/technology/biometrics

"In both technical and scenario evaluations, the collection [of test data] *must ensure that presentation and channel effects are either: 1) uniform across all volunteers; or 2) randomly varying across volunteers. If the effects are held uniform across volunteers, then the same presentation and channel controls in place during enrollment must be in place for the collection of the test data…"*

Comparative Biometric Testing incorporates specific protocols for collection of test data during enrollment and during subsequent true match testing. However, in most cases, the amount of submission advice and direction given to biometric system users is greater during system enrollment than during system usage. Comparative Biometric Testing incorporates more elaborate scripted submission guidance during enrollment than during subsequent true match testing (though true match testing does incorporate standard submission guidance). This may result in a slightly increased likelihood that, during true match testing, presentation effects will inform overall system performance.

- Paragraph 48 of the UK BWG document states the following:

  "Not every member of the test population will be able to test in the system. The "failure to acquire" rate measures the percentage of the population unable to give a usable sample to the system as determined by either the experimenter or the quality control module."

  Comparative Biometric Testing does not generally distinguish between Failure to Acquire and algorithm-based matching errors when calculating error rates. From a deployer's perspective, Failure to Acquire and matching errors are difficult to separate in a meaningful fashion; in many logical and physical access systems acquisition and template generation functions are inseparable. At various point in Comparative Biometric Testing, a system's failure to acquire usable biometric sample(s) on a given submission or placement attempt may inform that system's failure to enroll rate, its false match rate, and its false non-match rate.

- Paragraph 50 of the UK BWG document states the following:

  "Volunteers should not be told whether the current comparison is genuine or impostor to avoid even unconscious changes in presentation."

  While mindful of the UK BWG approach, Comparative Biometric Testing does inform test subjects of the type of match attempts (true and false) being executed. Placement advice and protocols are identical in each case. The decision to inform test subjects of the type of test being executed reflects real-world system operations, where individuals will normally be aware of whether they are executing a true match or false match attempt.

Appendix B: Biometric Technologies and Systems Tested

The following vendors' systems have been tested in prior Comparative Biometric Testing Rounds.

Round One	Round Two	Round Three
Finger-scan	**Finger-scan**	**Finger-scan**
• *American Biometric Company*	• *Advanced Precision Technology*	• *AcSys Biometrics*
• *DigitalPersona*	• *American Biometric Company*	• *BES*
• *Identicator*	• *AuthenTec*	• *Identix*
• *Identix*	• *DigitalPersona*	• *Precise Biometrics*
• *Mytec*	• *Ethentica*	• *SAGEM MORPHO*
• *Sony*	• *Precise Biometrics*	• *SecuGen*
• *ST Microelectronics*	**Facial-scan**	• *Sony*
• *Veridicom*	• *Visionics*	**Facial-scan**
Facial-scan	**Voice-scan**	• *Viisage*
• *Miros*	• *Nuance*	**Voice-scan**
• *Visionics*	**Signature-scan**	• *T-NETIX*
	• *Cyber-SIGN*	**Iris-scan**
	Keystroke-scan	• *Iridian*
	• *Net Nanny – BioPassword*	

Figure 9: Vendors' Systems Tested in Prior Rounds

Appendix C: Vendor Testing Form

Vendors whose systems are selected for Comparative Biometric Testing are required to remit the following document.

IBG plans to include Company’s product as part of its Comparative Biometric Testing. Please specify the appropriate model/version of Company’s product that will be evaluated:

Model __________________________ Version __________________________________

Please specify three threshold settings for 1:1 VERIFICATION. If there is only one security threshold available for your technology, check here ___ and leave lines below blank.

High Security Threshold: _______

Medium Security Threshold: _______

Low Security Threshold: _______

If your system has an ENROLLMENT threshold that can be set, please specify preferred setting:____

IBG acknowledges that, except as otherwise expressly stated, you do not make any representations or warranties, either express or implied, including without limitation any representations or warranties as to merchantability or fitness for a particular purpose, respecting the biometric devices and/or software. Both parties agree to release, waive, discharge and covenant not to sue the other party or its officers, agents or employees for any liability, claim and/or cause of action arising out of or related to any loss, damage or injury that occurs as a result of the Study. You warrant that IBG has the right to evaluate the system (hardware and software) that you will be providing. **Company must keep all data and results pertaining IBG’s Comparative Biometric Testing confidential unless IBG provides prior written permission to release data.**

For testing, Company must provide (2) scanners in addition to all software and peripheral equipment (cables, etc.) necessary for the system to function. The equipment that is submitted for testing must be capable of enrolling and verifying 300 subjects of various demographic backgrounds.

All hardware, software, and documentation must be received no later than (*Acquisition Date*).

All materials should be shipped to:

International Biometric Group
Comparative Test Study – Round Four
One Battery Park Plaza
New York, NY 10004

X________________________________

Company:

Name:

Title:

Date:

REQUIREMENTS FOR VENDOR SYSTEMS

IBG's Comparative Biometric Testing is designed to measure the effectiveness of biometric solutions for logical and physical access applications. To participate, vendors are asked to supply a system that fulfils the following criteria:

- The system must be able to perform 1:1 matching, with each subject being allocated a unique identifier or PIN.
- The system must be able to support a database of at least 300 test subjects.
- The system should be a commercially available, not specially built, system.

Each system will be inspected to ensure to the extent possible that it is representative of a system currently available in the marketplace. In the event that a selected vendor has more than one system appropriate for testing, the vendors are asked to provide their "most robust representative system".

TESTING ENVIRONMENT

For testing, IBG provides PCs on which the biometric hardware and software will be installed. The PCs have similar configurations, with at least a Pentium III processor and 128MB RAM running Windows 2000 (an alternative OS can be substituted as required). The PCs have a combination of parallel, serial, and USB ports available. IBG reserves the right to substitute PCs with equivalent hardware specifications. The vendor must provide all software and peripheral equipment (including scanners, cables, etc.) necessary for the system to function. If a vendor's biometric system cannot run on the PCs specified above, vendors may provide a PC. The specifications of any PCs provided by vendors are included in the final report.

THRESHOLD SETTINGS

Many biometric systems have verification threshold settings that can be adjusted to meet requirements for security and user convenience. Comparative Testing is designed to ascertain both false acceptance and false rejection rates, as specific applications may emphasize one rate over another for particular types of transactions. IBG allows each vendor to select three different verification threshold settings: "low security", "medium security" and "high security", with "high" being the setting least susceptible to false acceptances. Vendors are not required to utilize multiple threshold settings – vendors can opt to utilize a single setting if they so choose.

INSTALLATION AND TESTING

IBG configures and tests each system to ensure that it functions properly. We allow the vendors to correct any malfunctions before testing. Any malfunctions or other issues encountered during testing are addressed on a case-by-case basis to determine whether vendor involvement is warranted. These issues are documented during testing to resolve any potential impact on performance.
The date when all the biometric systems are configured and functioning properly is known as the Acquisition Date. Prior to the Acquisition Date, vendors may come on site to inspect the system and premises. Subsequent to the Acquisition Date, the vendors are not allowed to update, modify or alter their systems for the remainder of the Test, except for the resolution of malfunctions as stated above.

Appendix D: Confidentiality and Disclosure Form

Vendors who purchase the Final Report and seek to publish limited data according to IBG's strict guidelines are required to remit the following document.

This information contained in IBG's Comparative Biometric Testing ("Test") is covered under relevant evaluation and/or confidentiality agreements. This information is confidential and subject to non-disclosure provisions. IBG maintains all proprietary rights, including without limitation, trade secrets and copyrights related to the Test and all the results. **You may not copy, disclose or reproduce any part of the Test of the results in any form or by any means without prior written approval of IBG.**

Provided that you adhere to the terms contained herein and that you receive **prior written approval** from IBG, you may publicly disclose exactly two (2) rates ("Rates") relating to your product's performance as follows:

The Rates shall be a Primary Visit overall False Match Rate (FMR) and the corresponding False Non-Match Rate (FNMR) at one (1) threshold setting during the initial visit. You may not disclose any other data relating to your system's performance nor may you disclose any data at all relating to other vendors' performances.

With any disclosure, either written or verbal, you agree to state that the rates are from International Biometric Group's Comparative Biometric Test – Round Four. In all printed disclosures, the following paragraph must be prominently included:

"These performance metrics are derived from Round Four of International Biometric Group's Comparative Biometric Testing conducted in 2002. Visit www.biometricgroup.com for details on testing methodology and information on obtaining complete results."

1. Product Tested: ____________________

2. Threshold (circle one, if applicable): Low Medium High

3. False Match Rate for Visit 1: _________

4. False Non-Match Rate for Visit 1:_________

Vendor: ______________________________

Name & Title: ______________________________

Signature: ______________________________ Date: _________

The above information may not be disclosed until this form is executed by IBG below:

X _________________________ Date: ____________

Samir Nanavati, Partner
International Biometric Group

Appendix E: Test Scripts

The following scripts are representative of the material used to introduce Test Subjects to Comparative Biometric Testing and to guide Test Subjects through specific system processes.

Test Introduction

Today we are going to test biometric technologies. You are going to attempt to match against a previously enrolled person in each system, and then attempt to enroll and verify on each system. We will be testing finger-scan systems that measure unique aspects of your finger, facial-scan systems that measure unique aspects of your face, an iris-scan system that measures unique aspects of your eyes, and a voice-scan system that measures unique aspects of your voice.

Finger-Scan System: Enrollment and Match Testing

A. Introduction. This is a finger-scan device. It measures unique aspects of your finger. To use the device, press your [dominant] index finger flat on the platen like this [demonstrate], and remove it when I prompt you. Try to position your finger so that the center of your fingerprint is in the center of the platen.

B. False Match Test. We are now going to attempt to match against two other peoples' enrollments. We will try three times against each enrollment using your [dominant] index finger.

C. Enrollment Test. We are now going to enroll in the system. Place your index finger on the platen when I prompt you and hold it there until I tell you to lift.

D. False Match Test: middle vs. index. We are now going to try to match against your enrollment using a different finger than the one you used to enroll. When I prompt you, place your [dominant] middle finger on the platen the same way as your index finger.

E. False Non-Match Test. We are now going to try to match against your enrollment to see if the system recognizes your finger. Place your [dominant] index finger on the platen when I prompt you.

F. Placement advice:

□ Move your finger up a little.
□ Move your finger down a little.
□ Move your finger left a little.
□ Move your finger right a little.
□ Press slightly harder.
□ Press slightly lighter.

Appendix F: Sample Test Forms

The following Sample Enrollment Form and Sample Verification Form are representative of the materials used to collect data during Comparative Biometric Testing.

Sample Enrollment Form

Subject ID	Date

Enrollment	
Enroll: Y N **#placements** __________	**Initial Enrollment Attempt** 1. *Instructions for enrollment with primary biometric*
Enroll: Y N **#placements** __________	**Additional Enrollment Attempt** 1. *If the system is unable to enroll the primary biometric, repeat enrollment process using the secondary biometric. Note that the additional enrollment attempt for this system uses the secondary biometric.*

Subject Checklist			
	Initials	**Date**	**Comments**
Enrolled			
Verification 1			
Verification 2			
Verification 3			
Verification 4			
Entered XLS			
Checked XLS			

Issues raised and resolutions (continue on separate page if necessary)

APPROVED:

Sample Verification Form

Subject ID	Date

False Match Testing – Target IDs

Initial Instructions for Test Examiners

1. Read script and demonstrate use of system
2. Read instructions for false match tests

Target ID #1____

Low *Match – No Match* **placements __**	**Medium** *Match – No Match* **placements __**	**High** *Match – No Match* **placements __**

Target ID #2____

Low *Match – No Match* **placements __**	**Medium** *Match – No Match* **placements __**	**High** *Match – No Match* **placements __**

False Match Testing – Primary Biometric vs. Secondary Biometric

Detailed Instructions for Test Examiners

1. Set security level to “lowest” using procedures previously outlined
2. Lock computer with control-alt-delete
3. Input User ID under username and click OK.
4. As per script, instruct subject to place right index finger on platen. If subject enrolled using left index finger, instruct subject to use right thumb
5. Allow subject to place right index finger a maximum of three times to verify.
6. If subject is incorrectly verified by system at security level “lowest”, change threshold to security level “normal” using procedure outlined above and repeat steps 2-5.
7. If subject is incorrectly verified by system at security level “normal,” change threshold to security level “highest” using procedure outlined above and repeat steps 2-5.

Low *Match – No Match* **placements __**	**Medium** *Match – No Match* **placements __**	**High** *Match – No Match* **placements __**

True Match Testing

Detailed Instructions for Test Examiners

1. Set security level to “highest” using procedures previously outlined
2. Lock computer with control-alt-delete
3. Input User ID into username field and click OK.
4. As per script, instruct subject to place right thumb (or enrolled finger) on platen.
5. Allow subject to place thumb (or enrolled finger) a maximum of three times to verify.
6. If subject is incorrectly rejected by system at security level “highest”, change threshold to security level “normal” using procedures outlined above and repeat steps 2-5.
7. If subject is incorrectly verified by system at security level “normal,” change threshold to security level “lowest” using procedures outlined above and repeat steps 2-5.

High *Match – No Match* **placements __**	**Medium** *Match – No Match* **placements __**	**Low** *Match – No Match* **placements __**

Appendix G: Sample Exit Survey

The following pages include an example of the exit survey given to subjects at the end of the Secondary Visit.

QUESTIONNAIRE (Page 1) ID Number:

1) Compare each technology you used today to the traditional process of entering in a password to make a purchase online or to log on to a PC. Enter one number per box.

	Finger-Scan	Hand-Scan	Voice-Scan	Iris-Scan
1. Ease of Use 1=Much Easier 2=Easier 3=About the Same 4=More Difficult 5=Much More Difficult				
2. Impact on Privacy 1=Much More Privacy 2=Little More Privacy 3=No Change 4=Little Less Privacy 5=Much Less Privacy				
3. Security 1=Much More Secure 2=Somewhat More Secure 3=About the Same 4=Somewhat Less Secure 5=Much Less Secure				
4. Intrusiveness 1=Much Less Intrusive 2=Little Less Intrusive 3=No Change 4=Little More Intrusive 5=Much More Intrusive				

2) Rank the following to indicate your preference for making a purchase online (1 = most preferred, 5 = least preferred; **use each number only once**)
___ Finger Scan
___ Voice Scan
___ Iris Scan
___ Hand Scan
___ Traditional Password

3) Rank the following to indicate your preference for entering a secure facility (1 = most preferred, 5 = least preferred; **use each number only once**)
___ Finger Scan
___ Voice Scan
___ Iris Scan
___ Hand Scan
___ Traditional Badge or Card

4) Have you ever used a biometric before? (*Circle one*): **Yes -- No**
If so, please provide details:

5) How much would you be willing to spend to add a biometric to your PC or Door at home?
$_________

6) Is there anything you would like us to know about the technologies you used today?
Please use the back of this form.

QUESTIONNAIRE (Page 2) **ID Number:**

1. How would you feel using a biometric system instead of a signature when using a credit card?

1) very comfortable
2) somewhat comfortable
3) neither comfortable nor uncomfortable
4) somewhat uncomfortable
5) very uncomfortable

2. How would you feel using a biometric system instead of a PIN number when using an ATM?

1) very comfortable
2) somewhat comfortable
3) neither comfortable nor uncomfortable
4) somewhat uncomfortable
5) very uncomfortable

3. Would you be willing to use a biometric to confirm identity during air travel to board planes more quickly?

1) strongly in favor
2) moderately in favor
3) no opinion
4) moderately opposed
5) strongly opposed

4. Would you be willing to use a biometric to confirm identity when using a check for retail purchases?

1) strongly in favor
2) moderately in favor
3) no opinion
4) moderately opposed
5) strongly opposed

5. Would you be willing to use a biometric to confirm identity when opening locked doors or logging on to protected computers at work?

1) strongly in favor
2) moderately in favor
3) no opinion
4) moderately opposed
5) strongly opposed

QUESTIONNAIRE (Page 3) **ID Number:**

6. Would you be willing to use a biometric to confirm identity when voting?

1) strongly in favor
2) moderately in favor
3) no opinion
4) moderately opposed
5) strongly opposed

7. Would you be willing to provide a biometric to obtain or renew a driver's license?

1) strongly in favor
2) moderately in favor
3) no opinion
4) moderately opposed
5) strongly opposed

8. Are you in favor of or opposed to the use of a national ID card?

1) strongly in favor
2) moderately in favor
3) no opinion
4) moderately opposed
5) strongly opposed

9. Do you think biometrics are an effective tool in fighting identity fraud?

1) strongly in favor
2) moderately in favor
3) no opinion
4) moderately opposed
5) strongly opposed