

M1/03-0274

Project Proposal – Biometric Performance Testing and Reporting

1. Source of the Proposed Project

1.1. Title

“Biometric Performance Testing and Reporting”

1.2. Date Submitted

11 June 2003

1.3. Proposer

INCITS M1 Technical Committee

2. Process Description for the Proposed Project

2.1. Project Type

D - this is a standard development project.

2.2. Type of Document

The project is expected to result in a multi-part ANSI/INCITS standard that addresses the following areas at a minimum:

- a) Definitions, overall concepts,
- b) Technology testing and reporting,
- c) Scenario testing and reporting,
- d) Operational testing and reporting.

2.3. Definitions of Concepts and Special Terms

The following definitions are taken, in part, from the **Biometric Evaluation Methodology Supplement, Version 1.0, August 2002**.

Biometric Algorithm – A subcomponent of a Biometric System that may include the extraction and comparison of biometric data.

Biometric System – An automated system capable of capturing a **biometric sample** from an end **user**, extracting **biometric data** from the sample, comparing the data with one or more reference **templates**, deciding on how well they **match**, and indicating whether or not an **identification** or **verification** of identity has been achieved.

Biometric Performance Metric – a quantifiable assessment of the speed, accuracy or other characteristic of a Biometric Algorithm or System.

False Accept Rate (FAR) - The probability that a **biometric system** will incorrectly identify an individual, or will fail to reject an **impostor**. For a positive (verification) system, it can be estimated from:

$(\text{the number of false acceptances})/(\text{the number of impostor verification attempts})$.

False Match Rate (FMR) – The rate for incorrect positive matches by the matching algorithm for single **template comparison attempts**. For a **biometric system** that uses just one **attempt** to decide acceptance, **FMR** is the same as **FAR**. When multiple attempts are combined in some manner to decide acceptance, **FAR** is more meaningful at the system level than **FMR**.

False Non-Match Rate (FNMR) – The rate for incorrect negative matches by the matching algorithm for single **template comparison attempts**. For a **biometric system** that uses just one **attempt** to decide acceptance, **FNMR** is the same as **FRR**. When multiple attempts are combined in some manner to decide acceptance, **FRR** is more meaningful at the system level than **FNMR**.

False Reject Rate (FRR) - The probability that a **biometric system** will fail to identify a genuine **enrollee**. For a positive (verification) system, it can be estimated from:
 $(\text{the number of false rejects})/(\text{the number of enrollee verification attempts})$.

Failure To Acquire Rate (FTA) - The failure to acquire rate is the proportion of attempts for which a **biometric system** is unable to **capture** a sample of sufficient quality. When a **biometric system** allows multiple attempts, **FTA** measures **failure to capture** over these multiple attempts.

Failure To Enroll Rate (**FTE**) – The failure to enroll rate is the proportion of the user population for whom the **biometric system** is unable to generate reference **templates** of sufficient quality. It is the equivalent of **FTA** for the **enrollment** process, and depends on the procedures used in **enrollment** (which may differ from the procedures for later identification). It includes those who, for physical or behavioral reasons, are unable to present the required **biometric feature**.

2.4. Expected Relationship with Approved Reference Models, Architectures, etc.

None

2.5. Recommended INCITS Development Technical Committee
INCITS Technical Committee M1 - Biometrics

2.6. Anticipated Frequency and Duration of Meetings

It is anticipated that this project would require one-day meetings each quarter, with two additional one-day meetings within the first two quarters.

2.7. Target Date for Initial Public Review

It is estimated that the draft document would be ready for submission to INCITS for Milestone 4 processing in October 2003.

2.8. Estimated Useful Life of Standard

There is no known limitation on the useful life of this proposed standard.

3. Business Case for Developing the Proposed Standard

3.1. Description

The proposed standard would establish common procedures for testing and reporting the performance of biometric systems. In addition, the proposed standard would specify the reporting requirements that compliant declarations must meet in association with such reports.

3.2. Existing Practice and the Need for a Standard

Currently, there is no standardization in methods of evaluating biometric system performance. Each vendor develops unique test procedures and uses data sets of varying size, quality and origin to establish performance metrics that typically include False Match Rate, False Non-Match Rate and Failure To Enroll Rate. These variations make it impossible for customers and system designers to accurately assess the suitability of a given biometric system. They also make it impossible to design a system that combines multiple biometric systems to achieve customer-specified levels of performance.

Lack of standards in this area impedes the wide-scale adoption of biometric technologies in security and information system deployments. In the absence of standards, reporting of biometric system performance lacks rigor and disclosure. When customer experience varies significantly from their expectations, their confidence in the underlying technologies diminishes, as does their willingness to entrust the protection of human lives, important infrastructure or confidential information to systems that rely upon them.

By establishing a standard for measuring and reporting the performance of biometric systems, we will:

- Encourage the adoption of biometrics in applications where predictable performance is required.
- Provide a basis for objective comparison of biometric system performance based on compliant reports and disclosures.
- Allow customers and integrators to accurately assess system cost versus performance based on their particular needs.
- Increase the credibility of biometrics technologies within the customer community.
- Facilitate the development and deployment of large-scale systems based on biometric technologies.
- Provide a level playing field for providers who accurately report the performance of their biometric systems.

- Ensure that biometric system vendors can analyze new and existing products' performance in a cost-effective and statistically rigorous manner.

3.3. Implementation Impacts of the Proposed Standard

3.3.1. Development Costs

Technical editor labor is expected to total approximately four staff months.

3.3.2. Impact on Existing or Potential Markets

Though the federal government has conducted several pilot programs, the inability to accurately assess biometric system performance without costly testing under operational conditions has hampered the adoption of biometric technologies in real-world systems. It is expected that new markets, including many in the public sector, will likely emerge as a result of this standard.

3.3.3. Costs and Methods for Conformity Assessment

The cost and method of conformity assessment is not known at this time.

3.3.4. Return on Investment

There is no known data on which to make an estimate.

3.4. Legal Considerations

3.4.1. Patent Assertions

There are no known patents which apply to this proposal.

3.4.2. Dissemination of the Standard

Drafts of this standard will be distributed electronically. There may be distribution constraints as this document reaches different stages of development and processing within INCITS and ISO/IEC JTC1.

4. Related Standards Activities

4.1. Existing Standards

None.

4.2. Related Standards Activity

None.

4.3. Recommendations for Close Liaison

NIST/Biometrics Consortium Biometrics Working Group

ISO/IEC JTC1/SC27

Common Criteria Biometric Evaluation Methodology Working Group