AAMVA DECISION SUPPORT CONTRACT

BIOMETRIC TECHNOLOGY INFORMATION NEEDS

December 2003

Prepared by Fischer Consulting Inc

Copyright © 2003

EXECUTIVE SUMMARY

The American Association of Motor Vehicle Administrators (AAMVA) represents the officials of the jurisdictions in the United States and Canada who administer and enforce motor vehicle laws. After the terrorist attacks of September 11, 2001, AAMVA developed a strategy to enhance the issuance of secure identification credentials for driver licensing and photo identification purposes. One of the tasks resulting from this strategy was to develop a way to achieve the “one driver, one driver license, one driver license record” concept. That is, uniquely identify an individual such that (1) a holder will have no more than one driver license (DL)/identification (ID) card, (2) authorized users can verify that the holder of a DL/ID card is the individual to whom the card was issued, and (3) an individual has only one driver record, containing only information pertaining to that individual, and which “follows” the individual regardless of geographic location.

AAMVA commenced a biometric technology evaluation under the premise that biometrics may provide a solution to the one driver, one license, one record concept. Relevant evaluation criteria were identified and biometric technology performance data pertaining to the criteria was collected. Data sources included published tests, vendors and operational systems. After reviewing the available information, it became evident that there was insufficient data to predict and evaluate performance for solutions that would satisfy AAMVA's concept of operations.

This document identifies the information AAMVA requires to proceed with its investigation, placed in context by describing AAMVA's concept of operations foreseen for prospective solutions. Specific areas are noted in which currently available performance data fall short of AAMVA’s evaluation needs.

The intended audience of this document is organizations and academia in the biometric and related industries that may have an interest and the means to research the listed issues. Such organizations are encouraged to investigate and report on the identified information needs (or even components of these needs) that are applicable to their respective areas of expertise.

Inquiries about this document, or responses to the information needs, should be directed to AAMVA's Technology & Standards Department at 4301 Wilson Boulevard, Suite 400, Arlington, Virginia 22206, (703) 522.4200. Additional information about this project and others may be found AAMVA's web site at www.aamva.org.

Version 1.4 Copyright © 2003 Fischer Consulting Inc

TABLE OF CONTENTS

Copyright © 2003 Fischer Consulting Inc

1. BACKGROUND

The American Association of Motor Vehicle Administrators (AAMVA) is a voluntary, tax-exempt, nonprofit educational organization. AAMVA represents the officials of the jurisdictions in the United States and Canada who administer and enforce motor vehicle laws. Its members strive to develop model programs in motor vehicle administration, police traffic services and highway safety. The association serves as an information clearinghouse for these same disciplines, and acts as the international spokesperson for these interests. The association's programs encourage uniformity and reciprocity among the jurisdictions, and liaisons with other levels of government and the private sector. Its program development and research activities provide guidelines for more effective public service.

On October 24, 2001, AAMVA's Executive Committee passed a resolution creating a Special Task Force on Identification Security to develop a strategy on enhancing the issuance of secure identification credentials for driver licensing and identification card purposes, and to develop short- and long-term priorities and actions. The creation of the Special Task Force was in response to the tragedies of the September 11, 2001, terrorist attacks.

The Task Force submitted recommendations to the AAMVA Board of Directors at its January 2002 meeting and has since disbanded. The Uniform Identification (UID) Subcommittee developed a work plan based on the Task Force's recommendations. The UID Subcommittee has assigned tasks from the work plan to a number of Task Groups. The Unique Identifier Task Group (UID9) is tasked with developing a way to achieve the "one driver, one license, one driver record" concept, i.e. to uniquely identify an individual such that:

- A holder will have no more than one (1) driver license (DL)/identification (ID) card[1];
- Authorized users can verify that the holder of a DL/ID card is the individual to whom the card was issued; and
- An individual's driver record contains only information that pertains to that individual, and the individual has only one record that "follows" them regardless of geographic location.

The UID9 Task Group began with the premise that biometrics may provide a solution to this requirement. The Task Group must make a recommendation to the AAMVA Board on whether to implement biometrics as part of a comprehensive North American system, and if so, which biometric technology to use.

UID9 commenced with an investigation to determine the feasibility of implementing a biometric technology (or combination of biometric technologies) as part of a comprehensive North American system to assist in the unique identification of drivers. After carefully defining the system's objectives, the first round of evaluation indicated that some biometric technologies might provide a solution to the stated requirements. The biometric technologies focused upon were facial, fingerprint, and iris recognition. However, the supporting information was insufficient to determine if, within acceptable limits of uncertainty, these technologies (including any combination of these technologies) will work in a 300 million driver environment.

The purpose of this document is to put forth the information AAMVA requires to proceed with its investigation. AAMVA cannot consider the possible recommendation of one or more biometric technologies, to be used by all jurisdictions in the U.S. and Canada, without this information.

[1] In the remainder of this document, references to "drivers" include individuals who are not drivers but who hold or apply for an identification card in the same manner as a driver would hold or apply for a driver license.

Version 1.4 Copyright © 2003 Fischer Consulting Inc

This document is primarily intended for organizations and academia that are actively engaged in research and development activities in biometric technology and supporting infrastructure. These organizations will have the strongest interest in pursuing the answers to the stated information needs.

2. CONCEPT OF OPERATIONS

The concept of operations requires a 1:n search for every person added to the database, and a 1:1 comparison for every person already on the database prior to any transaction (in order to verify the person's identity). Searches are performed in a 300 million driver environment. It is unknown at this point whether the information will be contained in a central database or a distributed database where each individual jurisdiction maintains records for its cardholders. Users may have no, or only minimal, familiarity with biometric acquisition devices, as the majority of the driving population in the U.S. and Canada does not have experience with biometric acquisition (except of course for having photographs taken). A supervisor who has some training in the use of the biometric acquisition device will monitor biometric acquisition.

Applicants whose biometric data is new to the system (i.e. any person who has not already enrolled on the system since the implementation of a biometric, be they existing drivers or first time applicants) will provide biometric data and other biographic data[2] to be entered into a DL/ID information system. The biometric and biographic data will be separately compared to all existing records in the DL/ID information system. If neither the biometric data nor the biographic data register as pre-existing in the system, the DL/ID applicant is assumed to be new and legitimate. All subsequent transactions the applicant has with the DL/ID system will require a 1:1 biometric comparison of the applicant's existing record. A match of biometric or biographic data at enrollment (where the applicant is assumed to be new to the system) will trigger an exceptions process to determine the reason for the match. The match will either be refuted or confirmed, and the applicant will be denied or entered into the system as appropriate.

Not all matches are necessarily the result of a fraudulent enrollment attempt. The biometric information of an applicant who is new to the system may also be matched with an existing biometric record due to the following reasons:

- Technology related causes (e.g. the inability of a technology to distinguish between applicants with similar biometric data, system error, or operator error).
- User misunderstanding of application requirements (such as presenting him/herself as a new applicant instead of a transfer applicant).

Non-fraud related reasons for the biographic information of an applicant that is new to the system to match an existing biographic record include:

- Other individual with the same biographic data.
- Data entry error.
- Applicant is a victim of identity theft (i.e. a fraudulent enrollment was previously successfully performed by an impostor).

Applicants whose biometric data is not new to the system (i.e. DL/ID cardholders who have already provided biometric data on a previous occasion) should have data pre-existing in the system. When such DL/ID

[2] Biographic data as used here includes amongst others name, date of birth, DL/ID number and jurisdiction combination.

Version 1.4 Copyright © 2003 Fischer Consulting Inc

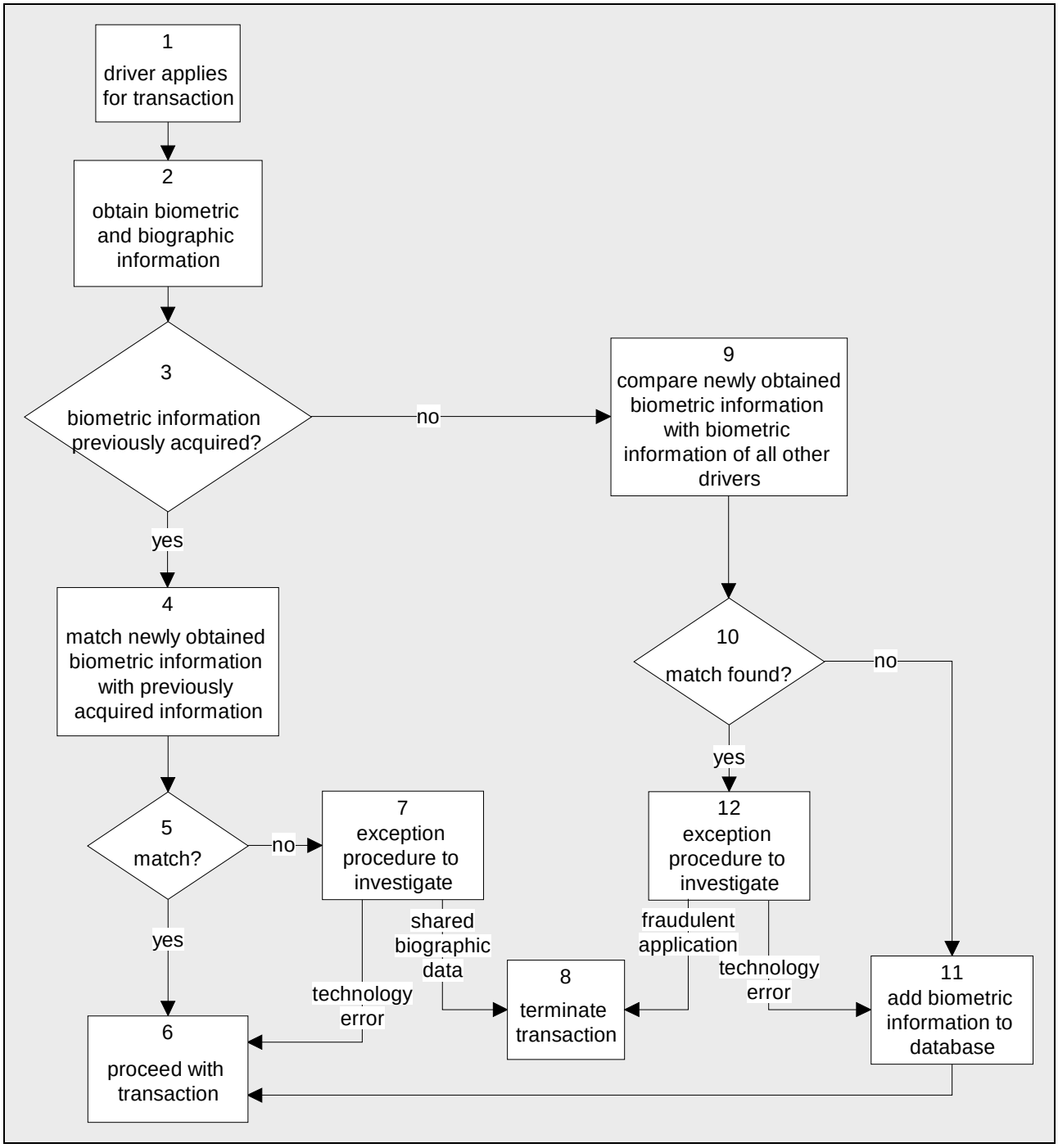
cardholders present themselves for a transaction, a 1:1 comparison of their biometric data will be performed to confirm the cardholder's identity. If the 1:1 comparison provides a positive confirmation of identity, the transaction is allowed to proceed. If the 1:1 comparison does not confirm the cardholder's identity, an exceptions process will be triggered to investigate the cause of non-confirmation. Non-fraudulent reasons for non-confirmation of a 1:1 match for applicants whose biometric data is not new to the system include:

- Technology related causes (e.g. the inability of a technology to match newly acquired biometric data with previously acquired biometric data of the same person).
- User / operator error (biometric data acquisition).
- Non-reported changes to biographic data used to make biometric record comparison (such as an unreported name change).

It is assumed that jurisdictions will continue the current practice of separately establishing DL/ID card validity periods. The impact on AAMVA's concept of operations is the span of time between “in person” customer transactions as opposed to transactions conducted by other means. The majority of the population is expected to only interact with the licensing agency when they first apply for a license, and when they must renew that license in person. The current validity periods range from 4 years to 12 years. However, many jurisdictions allow their drivers to renew their licenses over the Internet, via telephone, or by mail. Therefore, it may be even longer than 12 years between the times the driver submits their biometric. The time span will adversely impact the reliability of both 1:1 and 1:n matching – identity verification and the ability of the DL/ID system to prevent existing drivers from establishing multiple identities.

 Copyright © 2003 Fischer Consulting Inc

The diagram below (to be read with the accompanying notes) provides additional detail about the concept of operations.



The following notes apply to the numbered blocks as indicated:

1: At this point in the process, all applicants are treated in the same manner, regardless of the transaction. Transactions include license renewal, first time application for a license, change of address, etc. Applicants present their biometric information along with any other paperwork required for the specific transaction.

 Copyright © 2003 Fischer Consulting Inc

2: Regardless of whether a person is thought to have already been enrolled on the system, the first step is to obtain the driver's biometric information, and for the driver to submit his/her biographic information. Note that for some modalities (e.g. fingerprint), the extent of the biometric data acquired may differ depending on whether or not a person is thought to have already enrolled on the system.

3: The biographic information submitted by the driver is used to check if the driver's biometric information has been acquired previously. For new drivers, applying for their first license, the answer should be no. The answer should also be no for longtime drivers when they are first enrolled in the biometric system.

4: This is a verification process, i.e. verify if the driver is who he/she claims to be. This is performed by way of a 1:1 biometric comparison.

5: The system returns a "PROCEED / DO NOT PROCEED response," based on the 1:1 comparison. For each 1:1 comparison, the technology computes a "likeness" score. If the likeness score exceeds a predetermined threshold, a "PROCEED response" is given and the customer is allowed to continue with his/her transaction. A "DO NOT PROCEED response" indicates that the likeness score does not exceed the predetermined threshold, and an exceptions process is activated.

7: The exception procedure determines if the non-match was due to a biometric technology or data entry error, or due to more than one person using (or trying to use) the same biographic data, and may include a 1:n search. If the non-match was due to a technology or data entry error, the jurisdiction proceeds with the transaction. If the non-match was due to more than one person sharing (or trying to share) the same biographic data, the transaction is aborted. Administrative and investigative procedures are followed to determine the true owner of the biographic data.

8: The jurisdiction denies the transaction and may proceed with ID fraud enforcement or continue with an exception / appeal procedure. The terminated transaction is archived for future reference.

9: This is an identification process. The newly obtained biometric information is compared with the biometric information of every driver already in the database. That is, a check is performed to determine if the driver has previously obtained a driver license using different biographic data.

10: The system returns a "PROCEED / DO NOT PROCEED response," based on the 1:n comparison. During each 1:n search, the system searches for any records in the database for which the likeness score exceeds a predetermined threshold. If no records are found for which the likeness score exceeds the predetermined threshold, a "PROCEED response" is given and the customer is allowed to continue with his/her transaction. A "DO NOT PROCEED response" indicates that one or more records for which the likeness score exceeded the predetermined limit were found, and an exceptions process is activated.

11: Biometric information is added to the database after it has been determined that the person has not been previously enrolled.

12: The exception procedure determines if the match was due to a biometric technology error, or due to a fraudulent application (i.e. if the match was a true match or a false match). A false match means that the biometric technology wrongly identified the driver as another driver, in which case the jurisdiction proceeds to add the driver's biometric and biographic information to the database. A true match means that the driver has already enrolled on the system, in which case the jurisdiction aborts the transaction.

Version 1.4 Copyright © 2003 Fischer Consulting Inc

There are specific junctures in the concept of operations where the system may experience undetected failure:

Block 4 represents the point at which live biometric data is verified against a stored record on the database (1:1 match). At this point, a false match may occur as follows:

- Person A has successfully enrolled on the system. Person B presents him/herself to the system with the same biographic data used by person A, and the system falsely confirms that person B's biometric data and person A's biometric data belong to the same individual. This is known as a false match. If the biographic data really belongs to person A, person B thus succeeds in taking over the database record that identified person A up to that point. Alternatively, if the biographic data belongs to person B, the prior fraudulent enrollment of person A goes undetected.

Block 9 represents the point at which newly acquired biometric data is submitted for a database-wide search to ensure that the same individual did not previously enroll (1:n search). The following failures are possible:

- Person A is already enrolled in the database. Using a different set of biographic data, person A again applies for enrollment, and the system fails to recognize the similarity of the live biometric data to person A's stored biometric data (in Open Set Identification Performance Metrics (OSIPM) terminology, this is known as Potential Result 3 (PR3) – see Paragraph 4.2).
- Person A is already enrolled in the database. Using a different set of biographic data, person A again applies for enrollment, and the system wrongly indicates that person A's biometric information matches that of person B (PR 2 in OSIPM terminology).

Blocks 7 and 12 both represent the implementation of exception procedures that are activated when a database search results in a DO NOT PROCEED response and the customer transaction is flagged for investigation. Exception procedures are implemented to ascertain the reason for the DO NOT PROCEED response. Model exception procedures have not yet been developed for the jurisdictions and are not subject to AAMVA's research needs at this time. Although the procedures have not yet been written, it is theoretically possible that an error may occur each time an exception procedure is invoked – any exceptions process could potentially negate a correct database match (or non-match) result by mistake.

The following are also noted:

- It is expected that only a very small percentage of drivers for whom a 1:n search is performed, will already be on the database.
- The database is continually growing.
- The main purpose of the system is to prevent multiple licenses, i.e. to minimize the number of instances where an applicant (who is already in the database) is not matched against his/her existing record. False matches (i.e. instances where an applicant is wrongly matched with someone else's record) are undesirable as well, but can be processed by way of an exception procedure. Although resource intensive and detrimental to customer service, a false match does not compromise the integrity of the system.
- It is reasonable to assume that each time a customer presents his/her biometric for verification after initial enrollment, the most recently tendered biometric data will be added to the biometric data already stored on the DL/ID system. A policy for the use of new vs. previously acquired biometric data for 1:n search and 1:1 match purposes has not yet been established. The preferred option is to

 Copyright © 2003 Fischer Consulting Inc

use new data as primary source for search and match purposes (i.e. the reference data is regularly replaced), provided that the preceding identification can be performed within acceptable levels of confidence, and that the new data is acquired in the same manner as if the person is enrolling for the first time. An alternative option would be that the old data will remain the primary source for 1:n search and 1:1 match purposes, and that the new data is used to enhance search and match accuracy results. An alternative would be to use new data as primary source for search and match purposes (i.e., the reference data is regularly replaced when a person's biometric is acquired). It is reasonable to assume that the majority of customers will personally interact with a jurisdiction in a manner that requires biometric verification only once every several years due to the increasing convenience of performing many customer transactions via mail, telephone or Internet.

3. SHORTCOMINGS OF CURRENT DATA

After collecting information[3] on biometric technology performance from vendors, existing deployments and published tests, it became clear (as mentioned in Paragraph 1) that this information is insufficient for UID9's purposes. In particular:

- The environments represented by tests and deployments were considerably smaller than AAMVA's design environment of 300 million drivers – the largest fingerprint deployment (a criminal investigation implementation utilizing up to 10 prints per person) contained only 60 million records, with a few others containing over 10 million records. A small number of facial recognition deployments exceeded 1 million records, and the largest iris recognition deployment contained less than 500,000 records. AAMVA requires more information on the reliability of methods used to project large-scale performance from smaller tests and deployments in order to state with confidence that the issues related to a 300 million driver environment can be addressed.
- The concept of operations portrayed in the tests generally differed from the AAMVA concept of operations in the following respects:
    - The individuals in the probe database (i.e. the database containing biometric information representing new enrollees) were either all also represented in the gallery database (i.e. the database against which the biometric information in the probe database was compared), or a very large portion was also represented in the gallery database. In the AAMVA concept of operations, the opposite is true – only a very small portion of the drivers in the "probe" database is expected to be in the "gallery" database.
    - A "failure" was defined as a false match, and exception procedures were assumed to take care of false non-matches. In the AAMVA concept of operations, exactly the opposite is true – a false non-match results in a "failure" (allowing a person to obtain multiple identities), and a false match is handled by way of an exception procedure.
- Understandably, vendor performance projections and data are of greater utility in decision-making processes when validated by an independent 3rd party. In the absence of such validation, these

[3] The evaluation project was divided into two phases, with Phase I considering a set of objectives dealing with technology performance. This set of objectives essentially was a subset of the Phase II objectives. The information collection referred to here pertains to Phase I. The information requirements stated in Paragraph 4 however pertains to both Phase I and Phase II.

Version 1.4 Copyright © 2003 Fischer Consulting Inc

projections and data can reasonably be used only to confirm that a particular technology does not comply with the performance requirements.

- Information from existing deployments has limited application, due to the following reasons:
    - Differences in the concept of operations or environments of the existing deployments, and the AAMVA concept of operations and anticipated environment, may render comparisons invalid.
    - No existing deployment is of the same size/scope as the system contemplated by AAMVA. Neither is it anticipated that such a system will be deployed prior to the implementation of a driver license system in North America.

4. INFORMATION NEEDS

In its assessment of biometric technology for applicability to the issue of driver identification on a scale of 300 million drivers, AAMVA identified the enrollment and matching performance of the biometric modalities[4] as being key in their evaluation. In addition to this information, AAMVA has also identified additional data that will be needed for subsequent evaluation activities. The remainder of this paragraph describes these information needs.

Note that the broad scope of the information needs should not be misconstrued as an expectation that all information is to be provided by one organization. AAMVA would like to encourage organizations to respond to groups of information needs, individual information needs or even to components of an information need.

4.1. Compliance Requirements

In order for information to meaningfully contribute to AAMVA's evaluation activities, tests conducted to provide information need to be cognizant of the following:

- Test designs need to be consistent with AAMVA's concept of operations, as discussed in Paragraph 2 (above). Test results need to note how, if at all, the test environment differed from or did not reflect AAMVA's concept of operations, and how this may influence the applicability of the results to the AAMVA environment[5].
- Tests need to be managed (i.e. designed, monitored and audited) by an independent entity. That is, the entity performing the tests ideally should not be funded by or have any association with a particular biometric technology or biometric technology vendor that may cast doubt over the independence of the test results. Note that the entity managing (i.e. designing, monitoring and auditing) the tests may still have the actual tests performed by a vendor.

[4] A "biometric mode" (biometric modalities) generically refers to a type of biometric – such as fingerprint recognition, facial recognition, or iris recognition. Within each biometric mode, one may have different biometric technologies – such as template-based matching or pattern-based matching.

[5] This allows for either technology testing or scenario testing, or a combination of the two, as considered most appropriate by the testing entity to provide the stated information needs. Technology testing is understood to refer to offline testing of biometric data based on stored records, thus effectively not considering the influence of the interaction of drivers (in this case) with the system. Scenario testing on the other hand is understood to include live test subjects (drivers) in order to emulate the operational deployment environment.

 Copyright © 2003 Fischer Consulting Inc

- Test data need to be representative of a 1:300 million driver environment. It may be possible to extrapolate data from controlled tests using smaller database environments. In this case, confidence levels for the extent to which error rates for these smaller environments can be extrapolated to predict performance in substantially larger environments need to be noted.
- Because the ultimate database architecture is unknown at this point, the only requirement in this respect is that the architecture employed maintains the integrity of the system (i.e. ensuring that no subject may create more than one record on the system, thereby receiving multiple identity documents).
- Should it be found that the information provided in this document does not provide all the input relevant to the testing of a particular technology, AAMVA can be contacted to clarify the matter. Making assumptions without discussing such with AAMVA may result in test data that is not helpful to AAMVA's evaluation efforts.

4.2. Information Needs

In order to continue with its evaluation, AAMVA is in need of performance data and other information with respect to facial, fingerprint and iris biometric[6] modalities as listed below. A preference exists for the three modalities to be compared against each other with respect to each information need, rather than to evaluate modalities individually. However, results of individual modalities with respect to individual information needs will also be helpful to AAMVA's evaluation.

- Rates of failure to acquire biometric data (FTA), and failure to enroll biometric data (FTE), for statistically representative cross-sections of the U.S. and Canadian driving population. In addition, the influence of race, gender, age, and the influence of other aspects that may influence the rates for specific modalities (e.g. eye color, eyesight correction, medical issues, occupation (manual laborer or not)) are of particular interest.
- The user's ability to influence results of biometric acquisition and matching.
- Test results examining 1:n searching and 1:1 matching, separately. The results of 1:n searching must be expressed in terms of the OSIPM[7], which provide for the following:

  Potential Result 1 (PR1): Individual (already in database) correctly identified (correct result)

  Potential Result 2 (PR2): Individual **in database** identified as another individual (error result)

  Potential Result 3 (PR3): Individual **in database** not identified (error result)

  Potential Result 4 (PR4): Individual **not in database** identified as another individual (error result)

  Potential Result 5 (PR5): Individual (not in database) not found in database (correct result)

  The results of 1:1 matching can be expressed in terms of the False Match Rate (FMR) and False Non-Match Rate (FNMR).

[6] This does not preclude tests to be conducted in respect of other types of developing biometric technologies that may be able to provide a feasible solution to AAMVA's requirements.

[7] For a comprehensive discussion of Open Set Identification Performance Metrics, see the US Department of Defense report: **Face Recognition at a Chokepoint - Scenario Evaluation Results**, 14 November 2002, DoD Counterdrug Technology Development Program Office.

Copyright © 2003 Fischer Consulting Inc

- Transaction times for 1:1 matching and 1:n searching. "Transaction times" as used here refer to the time between submitting a query to the database and receiving the result. It does not include the time required to acquire the biometric. Acquisition time is understood to be dependent on (amongst others) the acquisition equipment used. Given that this is an area that is expected to see continued improvement, AAMVA is inclined to only evaluate acquisition time and acquisition accuracy during bid stage (i.e. at such time that bids for actual implementation are solicited). However, any data that can be provided on the performance of current generation acquisition equipment may prove to be helpful.
- The effects of template aging will be important to demonstrate if biometric technology is to be fully evaluated for implementation in a driver system. The time span within which customers will be presenting their biometric data for a subsequent transaction will generally be measured in years. Therefore, the temporal effects of biometric testing in ranges of 3 years, 5 years, 8 years, and 12+ years are applicable. AAMVA recommends the incorporation of longitudinal test data[8] to demonstrate the performance of template aging for both identification (1:300 million) and verification (1:1). Such longitudinal test data may be obtained from operational environments or from commissioned longitudinal biometric testing. If a testing organization asserts a shorter time span will provide substantially similar results, it will be helpful if such statements are justified and accompanied by a specific confidence level.
- The amount of operator training that will generally be required.
- The total cost of ownership for the implementation of a continent-wide system in the DMV environment, including implementation, operation, training, and maintenance. Given that all the parameters that determine the total cost of ownership have not been assigned values yet, this assessment would ideally result in a model that can be used again.
- Considerations for biometric matching for the enforcement of traffic laws (roadside enforcement). Such considerations include the portability of biometric capture devices, the suitability and security of using field-captured biometric data to perform 1:1 verification with records stored on the DL/ID system, and the suitability, security, and card storage technology required for on-card storage and matching. Weaknesses of available capture devices for use in field acquisition (operation under environmental extremes – heat, light, dampness, dust) are also important.
- A structured assessment of the security implications of a continent-wide biometric identity system. Note that this does not refer to biometric technology in general, but specifically to how the modalities under consideration differ in these respects.
- A structured assessment of the privacy implications of a continent-wide biometric identity system. Note that this does not refer to biometric technology in general, but specifically to how the modalities under consideration differ in these respects. The following are some of the aspects of privacy in which AAMVA is interested:
    - The dependence on images for the exchange of biometric data between different technologies of the same modality.

[8] Longitudinal testing refers to testing of the same subject(s) over a period of time, often over a number of years. In the current context, a subject would submit their biometric data in 2003, and re-submit their data in 2004, 2005, 2006…2015, etc. It should be noted that an actual longitudinal test of biometric technology will be difficult to structure, given the current rapid evolutionary cycle of biometric technology, including acquisition devices, matching algorithms, and database operational improvements.

 Copyright © 2003 Fischer Consulting Inc

  - The ease with which a person's biometric data can be obtained (from the person, e.g. via photography) without his/her knowledge. It may also be insightful to know how the actual situation (i.e. the ease with which a person's biometric can be obtained without his/her knowledge) compares to the perception among the public on this matter.

- The expertise required to interpret biometric search results, with specific reference to the amount of training involved.
- A model that can be used to estimate the number of multiple identities that can be expected for a given technology within the concept of operations as detailed in this document. One of the fundamental objectives of the project is to minimize the number of multiple identities on the database. Ideally, the model would be used during evaluation to estimate the number of multiple identities on a database given a number of input parameters or variables that define both the environment and the technology being evaluated. The model thus boils down to establishing the relationship between the number of multiple identities, and the variables that influence this number. Some of the variables that are thought to be involved are the FTER, OSIPM, FMR, FNMR, biometric template age, penalty applicable if an individual gets caught for a fraudulent transaction, and users' ability to influence biometric acquisition. The model thus requires knowledge of both the technical workings of a technology, and of the social dynamics that determine the number of fraudulent applications that can be expected. Depending on the causal relationships between the technical and social aspects, it may be possible to research these two areas separately.
- The level of standardization within different technologies. Aspects that AAMVA is interested in include:
  - The extent to which a modality is dependent on a particular technology for biometric acquisition.
  - The extent to which proprietary standards are required to interpret biometric data (for a particular modality).
  - The extent to which multiple vendors within a modality (or combination of modalities) may contribute to an effective continent-wide system.

Version 1.4 Copyright © 2003 Fischer Consulting Inc