Contents

Executive Summary ................................................... 3
Terms and Definitions ............................................... 4

Chapter 1 An Overview of Facial Recognition ...................... 6
1.1 Benefits of Using a Facial Recognition System ............. 6
1.2 Additional Benefits of Facial Recognition .................... 7

Chapter 2 Program Development and Enhancement ............. 10
2.1 Business Case Development .................................. 10
2.2 Project Planning ............................................... 11
2.3 Implementation ............................................... 11
2.4 Deployment .................................................. 12
2.5 Maintenance ................................................. 13

Chapter 3 Implementation and Operations ....................... 14
3.1 Legacy Cleanse or Scrub ..................................... 14
3.2 Staffing Considerations ...................................... 16
3.3 People and Processes ........................................ 16

Chapter 4 Technology ............................................... 21
4.1 Facial Recognition Technology .............................. 21
4.2 Standards .................................................. 22
4.3 Performance Metrics ........................................ 25
4.4 Image Capture ............................................... 27
4.5 Image Compression ......................................... 28
4.6 Search Engine Technology .................................. 28
4.7 Devices and Equipment ...................................... 30
4.8 Networks, Bandwidth, and Communication .................. 31
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Training</td>
<td>33</td>
</tr>
<tr>
<td>6</td>
<td>Privacy</td>
<td>37</td>
</tr>
<tr>
<td>7</td>
<td>Access and Sharing of Images</td>
<td>39</td>
</tr>
<tr>
<td>8</td>
<td>Stakeholders, Collaboration, and Outreach</td>
<td>44</td>
</tr>
<tr>
<td>9</td>
<td>Success Stories</td>
<td>48</td>
</tr>
<tr>
<td>Appendix A</td>
<td>Facial Recognition Survey Results</td>
<td>51</td>
</tr>
<tr>
<td>Appendix B</td>
<td>Model Legislation</td>
<td>53</td>
</tr>
<tr>
<td>Appendix C</td>
<td>Sample Memoranda of Understanding</td>
<td>55</td>
</tr>
<tr>
<td>Appendix D</td>
<td>Sample Application for Requesting a Facial Recognition Comparison</td>
<td>58</td>
</tr>
<tr>
<td>Appendix E</td>
<td>Working Group Roster</td>
<td>59</td>
</tr>
</tbody>
</table>
Identity fraud and identity theft are continuing problems, with estimated economic losses to consumers and businesses in the United States alone exceeding $24.7 billion annually.* Unfortunately, a portion of identity fraud and theft begins, or is continued, through the Department of Motor Vehicles (DMV) credential issuance process.

Facial recognition (FR) is a fraud prevention, fraud detection, business integrity, and risk mitigation tool used by the majority of U.S. and Canadian DMVs. FR software automates the process of photo image matching and is designed to determine whether the person shown in one photograph is likely to be the same person shown in another photograph. Consistent with the one person/one record principle, FR in the DMV enhances the integrity of the driver and non-driver identification registration processes to confirm that the person receiving the credential does not hold another DMV-issued credential in another name or with different personal identifying information (PII). Even in cases when a fraudster had previous success obtaining a fraudulent credential, FR improves the DMV’s ability to detect that fraud through image comparison analysis and investigation, often leading to arrest.

The importance of gaining stakeholder support for an FR program cannot be overemphasized. Strategic communication and outreach extolling the protective benefits of detecting and deterring DMV fraud also have an impact on protecting vulnerable populations; enhancing public safety; and identifying benefit fraud, identity theft, and other crimes. All of these result in creating a positive public impression and support.

This document was written for all DMVs, whether or not they currently employ an FR program. Jurisdictions with FR programs are encouraged to benchmark their practices against the recommended best practices contained herein and to make program changes where applicable and feasible to ensure their program is as strong as possible. For jurisdictions without a current FR program, this document can be used as a “blueprint” for building a strong program when enabling legislation is passed and funding necessary to implement an FR program is received. Toward that end, model legislation is contained in Appendix B. Appendix A contains an overview of a jurisdiction survey on the use of FR including a map that shows, at a glance, the jurisdictional adoption of FR.

After providing an overview of FR, this document provides recommended best practices in the areas of program development and enhancement, implementation and operations, technology, training, privacy, access and sharing of images, collaboration and outreach, and success stories.

Finally, it should be noted that the Facial Recognition Program Best Practices document and the Best Practices for the Deterrence and Detection of Fraud published in March 2015 are intended to complement each other, and both should be used to ensure fraud deterrence and detection practices are as robust as possible to prevent fraud from happening and to detect it when it does

* http://www.bjs.gov/content/pub/press/vit12pr.cfm

Executive Summary
**Terms and Definitions**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential</td>
<td>A driver’s license, identification card, permit, or other identity document issued by a DMV</td>
</tr>
<tr>
<td>Enroll</td>
<td>The initial process of collecting biometric data samples (photograph or facial image) from a person and subsequently storing the data in a reference template representing a user’s identity to be used for later comparison</td>
</tr>
<tr>
<td>Exception</td>
<td>Matching images found either during the scrub or during subsequent operations that are not fraudulent records</td>
</tr>
<tr>
<td>False positive</td>
<td>When one or more candidates are not matches with the probe. Examples include twins or people that look similar to the probe.</td>
</tr>
<tr>
<td>Feature extraction</td>
<td>Also referred to as template generation. This process identifies the points of interest (features) in the digital image that are relevant to the matching process. These features are then extracted, and a template record is generated.</td>
</tr>
<tr>
<td>Gallery</td>
<td>The array of photographs returned of potential matches when performing a one-to-many inquiry. Restricting or filtering (e.g., using age range, gender) the size of the searched image repository in identification applications may improve utilization of available adjudication staff but could exclude potential cases of fraud.</td>
</tr>
<tr>
<td>Identification</td>
<td>Also known as a one-to-many (or 1:N); a task in which the biometric system searches a database for a reference matching a submitted biometric sample, and if found, returns a corresponding identity. A biometric is collected and compared with all the references in a database. Identification is “closed set” if the person is known to exist in the database. In “open-set” identification, sometimes referred to as a “watchlist,” the person is not guaranteed to exist in the database. The system must determine whether the person is in the database and then return the identity.</td>
</tr>
<tr>
<td>Image processing</td>
<td>Could include image enhancement or checking the quality of the image against a predetermined standard</td>
</tr>
<tr>
<td>Leads</td>
<td>An automated list of possible candidate matches governed by a threshold within an image database</td>
</tr>
<tr>
<td>Lossy</td>
<td>Compression methods used in FR are called “lossy” because data is discarded or lost</td>
</tr>
</tbody>
</table>
Match score  Is termed as a genuine or authentic score if it indicates the similarity between two mate samples

Matching  The process of comparing a probe facial template with a previously stored template. The result of the matching process is a similarity score, which is then compared with the threshold value to determine a match or no-match decision.

One-to-record  One-to-one (or 1:1 match) against every image within a specific record

Personal identifying information  Any information about an individual, including any information that can be used to distinguish or trace an individual’s identity, such as name, Social Security number, date and place of birth, mother’s maiden name, biometric records, and any other information that is linked or linkable to an individual, such as medical, educational, or financial, and employment information

Scrub (cleanse, de-duplication)  The process of amending or removing data in a database that is incorrect, incomplete, improperly formatted, or duplicated as a result of fraud, clerical error, or some other cause

Threshold  The minimum degree of similarity between images to be considered a potential match

Triangle of recognition  An imaginary upside down triangle imposed over a face

Verification  Also known as a one-to-one (or 1:1 or one-to-record or 1:R search); a task in which the biometric system attempts to confirm an individual’s claimed identity by comparing a submitted sample with one or more previously enrolled templates
Facial recognition (FR) is a fraud prevention, fraud detection, business integrity, and risk mitigation tool used by the majority of U.S. and Canadian Departments of Motor Vehicles (DMVs). FR software automates the process of photo image matching and is designed to determine whether the person shown in one photograph is likely to be the same person shown in another photograph.

### 1.1 Benefits of Using a Facial Recognition System

Before jurisdictions considered FR technology, there was little evidence regarding the benefits of such a program. The National Institute of Standards and Technology (NIST) had just started its FR vendor tests. Illinois pioneered the use of FR for driver licensing applications beginning in 1999. In Canada, Alberta was the first province to implement FR in 2004.

A core responsibility of the DMV is to ensure that each driver’s license or ID card (DL/ID) applicant has only one identity on record. This is commonly referred to as the one person/one record principle. An FR program assists jurisdictions in ensuring that an individual has only one identity and is a proactive approach to identifying fraud before the issuance process is complete. FR systems are designed to combat identity fraud and identity theft.

#### Identity Fraud and Theft

Identity fraud occurs when someone uses a fictitious name backed by matching counterfeit breeder documents to obtain a genuine DL/ID or other document that contains false information. Identity theft occurs when someone uses the personal identifying information of another individual.

#### Internal Fraud

Depending on the FR system capabilities, some jurisdictions are able to track not only the individuals committing the fraud but also the office and operators who processed their transactions. If a DMV staff member or service provider is found to be involved in a disproportionately high volume of fraud cases, the FR system can be programmed to complete a mini-scrub of all of his or her transactions to determine whether there is a concern that requires further review.
**Clerical Errors**

A clerical error is the inadvertent creation of two records for the same person. FR helps identify when records of two different legitimate identities are overlaid or merged in error and instances when the wrong image is captured on an account. FR functionality can be used to track offices and operators who process a high number of errors.

### 1.2 Additional Benefits of Facial Recognition

Additional benefits include, but are not limited to, improving highway safety; reducing benefit fraud; and reducing financial fraud activities that target banks, retail stores, and insurance companies. FR helps communities recover after natural disasters. Moreover, FR provides invaluable assistance to law enforcement by helping to identify missing persons, most wanted persons, and other vulnerable populations. FR aids in solving serious crimes and detecting individuals avoiding government oversight (e.g., Sex Offender Registry requirements).

**Highway Safety**

The primary purpose of a DL is to clearly identify that an individual has met the requirements to drive legally and safely. The use of an FR system prevents individuals who lose their driving privileges from creating fictitious identities and obtaining a DL to continue driving without fear of detection by law enforcement.

To illustrate the correlation between individuals holding multiple records and highway safety, the New York DMV conducted a two-year study (January 2010–January 2012) to determine if drivers with multiple license records pose a serious traffic safety risk on New York’s roadways. Of the more than 12,300 cases involving drivers with multiple license records:

- 24% did not have a valid license.
- 67% had been involved in a crash compared with 43% of all New York State (NYS) licensed drivers.
- 10% had been convicted of impaired driving compared with 2% of all NYS licensed drivers.
- 27% had been convicted of a cell phone violation compared with 9% of all NYS licensed drivers.
- 49% had been convicted of unlicensed operation compared with 8% of all NYS licensed drivers.
- 57% had been convicted of a seat belt violation compared with 21% of all NYS licensed drivers.
- 34% had accumulated six or more points on their license records within an 18-month period at some point in time after November 18, 2004, compared with to 11% of all NYS licensed drivers.

The DMV’s FR program has provided an important tool for New York in identifying and addressing traffic safety–related issues. The success of New York’s program relies on the ongoing cooperation among the state’s traffic safety organizations, law enforcement agencies, and judicial system.

**Benefit or Financial Fraud**

A common example of benefit fraud is when a fraudster who obtains an ID card or DL in a fraudulent name now possesses a breeder document that may be used to secure genuinely issued credentials in a fraudulent identity. While gainfully employed in one job, the fraudster obtains employment at a second job and is now working for two employers simultaneously. If terminated from one job, possibly intentionally, the fraudster is then able to file for and obtain unemployment compensation under the false identity while continuing to work under the other identity. If a person is willing to create one false
identity, nothing prevents him or her from duplicating or expanding the scam.

Jurisdictions that use FR report that a significant percentage of DMV suspects have gone on to use their fraudulent identities to commit fraud against other entities, including government benefit providers. The New Jersey Motor Vehicle Commission (MVC) shares the results of its FR system findings with authorized stakeholders via AIRS, New Jersey’s “Aggregated Investigative Reporting Service.” This system was designed, constructed, and implemented to strategically target byproduct fraud. After detecting a fraudulent identity, the MVC FR team, in partnership with the lead law enforcement entity, posts information about fraudulent identities to the AIRS website. Twenty-three participating AIRS Users (federal, state, and county government benefit-conferring entities) systematically vet the AIRS case inventory and open a fraud investigation when warranted.

**Disaster Response**

Across Canada and the United States, FR has been used to assist medical examiner and coroner offices in identifying deceased persons. Use cases include identification of deceased individuals, homeless or lost individuals with memory challenges, and unconscious crash victims without identification documents.

Facial recognition greatly enhances the identification of victims of a disaster such as a tornado, which may be challenging if the nature of the event prevents individuals from obtaining a recognizable form of identification. Ensuring victims are known by a single identity helps in limiting the same person from receiving aid for the same condition several times or by multiple relief organizations, thereby helping distribute the aid and resources available across as many victims as possible.

Quick and efficient identification of emergency response staff is essential in managing and regulating access to disaster areas. FR technology may also be leveraged to expedite the rapid deployment of emergency response staff.

Advanced planning and registration of first responder staff anticipated to perform a role at an emergency is critical to obtain quick access to sites where their services are in immediate demand. Advanced planning should also account for quickly enabling reliable methods to register volunteers and other single-event responders that are connected with faith based or charitable organizations. Emergency planners may wish to explore remote registration methods or other procedures that allow these groups to register while en route so their services can be put to use as soon as possible when they arrive on scene.

**Assistance to Law Enforcement**

Law enforcement periodically leverages DMV FR systems, within the parameters set by legislation and DMV policies and procedures, to aid in criminal investigations, and other assistance activities.

The search of counterfeit document factories and labs frequently results in dozens, if not hundreds, of images of people who need to be identified. It is common for suspect images found on counterfeit identification to be run through a DMV image database. FR is an effective investigative tool for such purposes.

The Florida Department of Highway Safety and Motor Vehicles provides access to its FR database to law enforcement agencies in the state with which they have a Memoranda of Understanding (MOU). The Pinellas County Sheriff’s Office in Florida, a leader in bringing FR technology into mainstream law enforcement use, has equipped patrol vehicles with the equipment necessary to do on-the-spot FR verification and identification. In addition, the Florida Department of Corrections runs FR on every prisoner who enters the system and uploads mug shots to the Pinellas County Sheriff’s FR system. What follows are two success stories.
On February 6, 2013, a Bank of America in Pinellas County Florida was robbed by an unknown male suspect. Upon the arrival of a Pinellas County Sheriff’s Office Deputy, he reviewed surveillance footage that captured the suspect’s image. The deputy obtained a facial image of the suspect from the video footage while at the bank. He then submitted the image into the FACES (FR) database within his cruiser and immediately received three possible match images of the suspect. Officers were able to determine the suspect’s last known address and then meet with the suspect’s father, who confirmed the suspect’s identity within one hour of the robbery occurring.

In another example, in 2011, after a hockey game in which the home team was eliminated in the NHL Stanley Cup final, a large-scale riot broke out in downtown Vancouver British Columbia. Through social media, police were flooded with images of people taking part in the riot. DMV FR resources were available to police but only under court order. The police used FR to assist in identifying and locating suspects involved in person and property attacks during the riots.
In consideration of pursuing a facial recognition (FR) program, begin with the end in mind. For jurisdictions considering implementing an FR system, this chapter can be used as a blueprint to assist in development of an effective program. A program mission statement that concisely describes what the program is meant to accomplish and why must be written. The mission statement should be accompanied by a program charter that outlines the program business requirements and a statement of the intended use of FR, both internally and externally. The mission and charter should serve as guiding principles throughout program development and implementation, as well as ongoing maintenance.

2.1 Business Case Development

The first step in planning for a new project is to develop a business case that includes a feasibility study, legislative assessment, determination of fiscal needs and policy development, procurement, and outreach.

Legislative Considerations

As of the printing of this document, 47 of the 69 jurisdictions in North America have implemented some form of FR technology in their motor vehicle agencies (see Appendix A). FR has gained widespread acceptance. However, its use is not without opposition. Civil liberties groups and privacy advocates argue for limits on the use of FR (and in some cases, their prohibition). State and provincial legislators, if well-educated on the benefits of FR, will provide sound enabling legislation. Absent effective enabling legislation, courts are more likely to become involved and dictate how FR can or cannot be used. Privacy concerns are legitimate, but with proper legislation, public fears can be allayed and bad case law avoided.

To create sound legislation, a number of things need to be in place, not the least of which is a basic philosophy about how FR is to be used. To assist jurisdictions without current legislation and jurisdictions seeking to amend current legislation, the AAMVA has developed model legislation (see Appendix B). This model legislation is not intended to fit the exact needs of every jurisdiction. Rather, it is intended to provide a foundation of sound principles upon which jurisdictions may amend or insert additional language to meet their needs.

In considering legislation, jurisdictions should solicit input from key stakeholders and subject matter experts (SMEs), including law enforcement and prosecutors. If the intent is to allow images to be searched by or shared with law enforcement, legislation and policy should be aligned so the process is transparent and there are safeguards against abuse. Full disclosure is essential to counter the argument about the expectation of privacy in relation to the capture of an image for a DL/ID.

Budget Considerations

Completion of a cost–benefit analysis will provide the basis for funding justification and identify program benefits. Costs to be considered include, but are not limited, to:

- Business requirement and procurement development
- System acquisition
- Data conversion


Infrastructure (network, data storage, hosting, data recovery, or equipment)

Resource workload: staffing (implementation and ongoing)

Scrub of legacy records

Investigations, prosecution or administrative hearings: initial and ongoing

Information technology

Daily program management

Marketing and outreach

Public hearings and meetings

Training

Maintenance (licensing, additional storage, technology refresh, system upgrades)

Jurisdictions may wish to explore grant funding, increased fees, or other funding options to help fund the program.

**Procurement**

The most important task for the procurement team is to fully align procurement and FR program objectives. A close collaboration between the two will bring maximum value to the organization because it allows for procurement tools to be better used throughout the project’s lifecycle. The selected vendor must be able to meet the desired specifications and must be willing and able to successfully fulfill the terms and conditions of the procurement.

**Planning Stakeholder Outreach**

An outreach plan identifying stakeholders, methods of communication, and messaging should be developed. Including stakeholders early in the process will provide transparency and buy-in. It will also provide insight to stakeholder needs from the program. Chapter 8 provides details on outreach planning and execution.

### 2.2 Project Planning

A common understanding of the project’s objectives is required for key stakeholders. Discussion topics should include the scope of the project, desired outcome, necessary resources, timeline, and budget. The project lead must provide a clear vision of the project to the project team and key stakeholders. Responsibilities for each task should be clearly outlined so the project’s participants understand which person is responsible for which task and expected timeline for completion. The project’s roadmap should be broken into stages, each with measurable goals.

**Develop Requirements**

Business, functional, and technical requirements must be clearly identified and documented. The importance of developing comprehensive requirements is key to the success of deploying and operating an FR system that meets the jurisdiction’s objectives.

**Identify Risks**

All projects contain some form of risk. Jurisdictions should identify the risks and proactively develop mitigation plans to prevent their occurrence.

**Plan for Data Conversion**

Current data must be analyzed for record coherency, photo quality, and methods for extraction to enroll images into the FR system. The assessment of data conversion needs facilitates project scope estimates and influences decisions on screening and investigation processes.

### 2.3 Implementation

Although Implementation activities are defined in the project plan, careful execution of planned tasks is a key success factor in delivering and operationalizing an FR program. Implementation, sometimes referred to as project execution, typically defines the activities.
2.4 Deployment

When deploying an FR program, jurisdictions must determine the deployment option that best meets their needs.

Pilot Before Full System Deployment

Initial deployment of the FR system on a limited basis provides a jurisdiction with the opportunity to experience firsthand the impact that the system may have on its people and processes.

One pilot approach is a full deployment of the backend batch processing (1:N) while using the 1:1 process at time of enrollment in a limited number of branch offices. This enables the jurisdiction to identify the impact on customer service and issues of concern. For instance, the quality of the legacy images may impact the threshold used for the 1:1 process (see Chapter 3, Section 3.3 for more information on setting a threshold).

Another pilot approach is a full deployment of the 1:1 process at time of enrollment and a partial deployment of the backend processing (1:N). In this scenario, all images captured would be enrolled into the FR system with a portion of the images (e.g., Commercial Driver’s License) funneled through the 1:N process. This type of pilot approach delays obtaining the full benefit of FR and may increase the need for a follow-up scrub.

Full System Deployment

A full system deployment offers immediate program-wide benefits. The impact to employee workload and temporary decline in customer service will need to be evaluated against the immediate benefits. This approach eliminates the need for a follow-up scrub of images captured after full deployment, reducing future cost and workload.
2.5 Maintenance

The long-term continued use of an FR system depends on a purposeful maintenance plan.

Licensing and the need for additional storage as the image database increases in size are maintenance functions that should be reviewed on a regular basis. On a less frequent basis, technology refresh and system upgrade options should be considered.

FR technology is rapidly advancing, which may lead to a decision to take advantage of technology refreshes or upgrades, which may require reenrollment of images. Periodic upgrades provide the opportunity to increase the tools accessible to the analysts and take advantage of advances being made in the mathematical representations and matching processes software used in an FR system.

Depending on contract terms, maintenance may either be a required function of the vendor providing the FR system, or it may be managed by the jurisdiction’s IT staff. A jurisdiction should take maintenance and upgrade options into consideration when developing a maintenance plan and in determining an ongoing budget.
Jurisdictions are encouraged to follow the recommended best practices contained in this document related to the technical, operational, investigative, and prosecutorial processes as they relate to the use of FR technology. Understanding basic terms and concepts are important for understanding the materials herein. Two scenarios exist in conducting a biometric query: verification and identification. Verification (one-to-one/1:1 or one-to-record/1:R) is defined as a process in which the biometric sample is matched to a specific individual, showing that the person is who he or she claims to be. Identification (one-to-many or 1:N) is a type of search that compares the biometric sample with a database to determine if the reference already exists and to identify the sample.

### 3.1 Legacy Cleanse or Scrub

When implementing an FR system for the first time, a legacy photo cleanse, often referred to as a “scrub,” is the process of performing a 1:N identification for every image in the DMV database. The presence of legacy images provides the jurisdiction with the ability to immediately identify errors and fraudulent acts. When the legacy images are not enrolled in FR, the positive impact is delayed one or more DL renewal cycles. This process helps to both cleanse data errors in the historical data set and point toward suspicious activity for further analysis. If a jurisdiction lacks the resources necessary to complete a full scrub, the option to complete a partial scrub may be considered as an alternative (e.g., images captured since last issuance cycle).

A full image database scrub occurs as a batch process executed before delivery of the production solution and can typically be configured in two ways:

- A full 1:N (duplicate identity identification) and 1:1 (record verification) batch comparison of all images for all records contained within the database
- A full 1:N comparison of all images for all records contained within the database

Although not preferred, a partial database scrub also occurs as a batch process and can be configured in two ways:

- A 1:N comparison of only the most recent image for each record in the database (with the option to execute a verification for each record containing two or more images)
- A comparison on only images captured starting at a specified date

Although it is possible to stand up an FR system and use it from that day forward, it is strongly recommended and regarded as a best practice that a full scrub be performed; below are the pros and cons of a full versus a partial scrub.

<table>
<thead>
<tr>
<th>Scrub Type</th>
<th>Pro</th>
<th>Con</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full</td>
<td>A complete system cleanse of all images will ensure every image is compared and all results will be reported. This will enable complete system cleanup of all images and all errors corrected and all possible fraud cases identified for adjudication and action.</td>
<td>A complete system cleanse will be much more costly and there will be an even greater number of results that will need to be adjudicated, including matches for individuals that no longer reside in the jurisdiction. This adjudication will take more man-hours to complete as well as require more personnel to accomplish the adjudication process in a timely manner.</td>
</tr>
</tbody>
</table>

(continued)
Chapter 3: Implementation and Operations

The processes described below provide general guidelines for completing a scrub.

- Data assessment: Evaluate identity record data structure and assemble the plan, including the timing, deliverables, and owners for each of the tasks.
- Data design: Analyze the existing image database and demographic information to plan the data transfer into the FR system.
- Data transfer: Extract the data from the existing repository, move to the transfer media, and secure transfer to the FR system facilities.
- System assembly: Assemble, configure, and install software for the FR system.
- Enrollment: Create the FR database from the images and configuration of the results server using the demographic data.
- Identification search (scrub): Perform an FR identification search of each image against all other images.
- System-generated scrub results: Select highest probability matches for further investigation.

Regardless of type of cleanse conducted, the results may be reported in different ways depending on the system or vendor product used.

The following items should be considered when planning a scrub:

- The scrub should be completed immediately preceding the daily enrollment of drivers so there is no gap requiring an additional scrub at some point in the future.
- Jurisdictions that undertake a scrub of their image databases need to work closely with their vendors to set the threshold at which leads should be generated at the conclusion of the scrub.
- Jurisdictions may also wish to talk to others who have implemented an FR program to gather information and lessons learned on their experiences in handling scrub results.
- Selecting jurisdictions that have similar population numbers, renewal cycles, goals, and so on for the comparison will provide a basis for determining the workload that accompanies an FR system.

The New Jersey Motor Vehicle Commission conducted a legacy scrub of its 22 million image database over the course of a two-year period commencing in December of 2011 and concluding in March of 2014. The FR software ran 24/7 for 30 days and produced 1.2 million potential matches in need of examination and possible further analysis.

When the scrub is completed, the jurisdiction must analyze the scrub results. Potential matches must be reviewed to determine the presence of false positive, clerical error, or fraud, and appropriate action must be taken. Procedures must be developed or updated.
to address the errors and the analysis of cases to determine if other criminal activities have occurred along with the possible location(s) where the holder of the document may be located. These processes will assist in the cleanup of the image database.

In most cases, the following results will be identified but the vendor may use a specific word for these results. The following errors must be addressed to clean up the image system.

- False positive: Twins or people that look alike. This type of result requires no further action.
- Clerical error: Steps to take corrective action should be taken. The following are examples of clerical errors:
  - Duplicate error: Results show all images that have the same demographic information but different images.
  - Same image error: Results show that the images are the same but the demographic information is different.
- Fraud: Examples of fraud include a person intentionally using different identities; a person using multiple fictitious identities; multiple persons using the same identity; and a person using the identity of another, which would also constitute identity theft. Investigative action should be initiated in all of these instances.

3.3 People and Processes

Facial recognition technology incorporated into a credential issuing system works best when an organizational structure is established for the people and processes.

- Experienced analysts should be able to evaluate approximately 300 cases per day. An individual case may have two to 50 or more images to review.
- At a minimum, one investigative analyst is recommended for every 300 images reviewed by the analyst or comparison specialist.
- At a minimum, one investigator is recommended for every 300 images reviewed by the analyst or comparison specialist. See the AAMVA’s Best Practices for the Deterrence and Detection of Fraud for information on staffing a fraud unit.
- A multiple person review of the case is recommended when fraud is suspected. If a multiple person review is not possible, spot auditing should be completed.
- Staff who are responsible for reviewing potential cases should have other duties because burnout will occur if they are only reviewing matches.
- Individuals with analytical skills should be selected to review cases.
- Having individuals with a variety of ethnic backgrounds can be beneficial.
- Staff should be trained by the FR vendor and receive specialized FR training as outlined in Chapter 5.

Providing appropriate levels of access for system users based on their job responsibilities is a best practice for proper operation and security of an FR program.

3.2 Staffing Considerations

Factors to take into consideration in determining staffing to evaluate FR cases:

- To achieve optimal results, leads must be reviewed on a daily basis. Match analysis and investigation should include examination of criminal history and recent activity associated with the suspect and victim.
The credential issuance process that uses FR is best managed when a central issue method is incorporated. Central issuance allows for a more thorough vetting of the image captured before printing and issuing the DL document. (See the AAMVA’s DL/ID Standard and Secure Card Design Principles document.)

The following DL/ID issuance processes are recommended for central issuance programs:

- At the time of application, provided a full scrub was completed, perform a one-to-one FR comparison upon capture of new image to the most recently captured image for that record. If a partial scrub was completed, perform a one-to-record comparison. Display negative results to staff before approval or denial of the application.

- Enroll all new images captured for approved applications into the FR database.

- Complete a one-to-many comparison of newly enrolled images before production of the DL document.

- Complete review of cases on a daily basis, closing those that are false positive and taking corrective action on clerical errors, to ensure that credential production is not unduly delayed.

- Hold production of credential until analysis is completed. Forward matches related to fraud to investigations staff. Credential extensions may be required if the analysis or investigative process extends beyond the expiration date of the original document.

Best practices for over-the-counter programs include:

- Complete a full scrub of all images in the legacy system.

- For initial issuance, complete a one-to-many comparison of the newly enrolled images before production of DL document. If a potential match is identified, deny issuance and advise that the credential cannot be issued at this time.

- For renewal or duplicate applications, complete a one-to-one comparison at time of application, provided a full scrub was completed. If a partial scrub was completed, perform a one-to-record comparison. Deny issuance of the credential if images do not match.

- Complete a one-to-many comparison during an overnight batch. If a match is identified, cancel or suspend the credential as appropriate and refer the case to investigations.

**Exceptions Processing**

The term “exception” references matching images found either during the scrub or during subsequent operations that are not fraudulent images. They are images that cannot or were not processed as part of the scrub or daily operation. Examples of exceptions are undercover licenses for law enforcement; user test images; and images that cannot be enrolled because of a disfiguration, eye patch, and so on.

The procedure for processing exceptions must be identified before the implementation of any FR program. Jurisdictions need to establish policies and procedures on exceptions. An important step in the implementation process is to identify the images known in the current database that meet the set exception criteria for the jurisdiction before the initial scrub. This will eliminate images from being reported as fraudulent during the scrub. After the jurisdiction has identified images that meet the exception criteria,
the policy must be strictly followed to eliminate any errors during the adjudication process.

A benefit of having an exception policy in place before deployment is that after it has been implemented, operations will be enhanced by avoiding delays in customer processing. The plan will ensure that all images are reviewed for possible fraud and that appropriate action can be taken when fraud is identified.

There will be occasions when the FR system is unavailable. Credentials should not be issued until an FR comparison is completed. Jurisdictions must develop processes and procedures to handle such occurrences, whether central issuance or over the counter.

**What to Expect**

Jurisdictions need to understand that the vast majority of leads will not be fraud related. Some leads will be eliminated through the manual review process, others will be eliminated through the error correction process, and the remaining will be exceptions that require further investigation to determine if fraudulent activity has occurred.

Errors that may be identified through the use of FR are the linking of an image with the incorrect record; the erroneous creation of duplicate records for the same individual; failing to properly identify or protect an image captured for covert or undercover law enforcement purposes; and capturing an image that is flawed by lighting, pitch, yaw, roll, facial expression, or head or face coverings.

Evaluating the demographic information returned as part of the lead is an integral part of the review process. When the demographic information for two matching images also matches, this indicates that a duplicate record has been created erroneously.

In cases when the images returned as part of a one-to-record comparison do not match, the demographic information may or may not match (depending on the actions taken by the enrolling clerk), and the signature accompanying the images should be reviewed. If the signatures are two different names (e.g., John Smith and Jacob Smithson), this indicates there was no intention of fraud and that an image has been linked with the wrong record.

After the determination is made that the match is not a result of an error, each matching image should be compared side by side, looking for similar identifying features. If the analyst concludes that there is a likelihood of fraud, the matching image(s) should be individually run through the FR system for comparison within the image database. This provides the analyst with further evidence as to the origin of the suspect image(s) and provides another level of validation that the image(s) match. From here, the process of gathering information from the credential issuing process (i.e., proof of identification documents provided) and outside sources, such as criminal histories, will start the investigations process.

Jurisdictions should create error correction and investigative procedures and training for each type of error or suspected fraud that may occur.

**Setting a Threshold**

When developing an FR program, jurisdictions must determine the threshold at which potential matches should be generated. Different thresholds should be set for one-to-many and one-to-one comparisons.

The threshold directly impacts the number of cases received for manual review. Jurisdictions should balance the workload requirements with the potential fraud that may be identified.

The threshold is the minimum degree of similarity between images to be considered a potential match. If the similarity score falls below the threshold setting, there is a no-match decision. If the score is above the threshold setting, there is a match decision. The threshold is adjustable so that the FR system can be more or less strict, depending on the requirements of any given application.
Jurisdictions should be aware that lesser quality images that may be contained in their legacy database will still work in an FR comparison. However, adjustments may need to be made to thresholds to account for a difference in quality.

Statistics regarding the number of applicants processed, the number of cases, and the number of records of potential fraud should be recorded. Statistics should be reviewed annually to determine if the program’s goals and objectives are being met. Changes to thresholds may be necessary. The balance between the number of leads and the number of cases of fraud identified, based on a number of factors, will be different for each jurisdiction and may periodically change.

**Reporting and Trending**

Reporting must be a key component of a jurisdiction’s requirements development process because if left out of the definition and design phase, trying to implement after the fact can be expensive. Most FR products designed for DMV users already include several predefined reports. Additional reports may also be desired.

**Operational Reports**

The purpose of FR operational reports is to allow the jurisdiction to monitor operations and to ensure card requests are being processed appropriately. The operational reports defined for FR should provide answers to operational questions and measure key performance objectives. Examples include:

- **Enrollment Status Report and Pending Identification Report**: indicates whether all of the credential orders have been processed for a given date or whether there are delays without justification (stuck images)
- **Enrollment Error Report**: lists images unable to be enrolled, images that may be stuck, and where the delays are (used for troubleshooting)
- **Batch Enrollment Report**: indicates how many images failed enrollment and at what quality metric
- **“White List” and “White List Audit”**: jurisdictions can request a report that indicates whether the by-pass FR functionality is present for a particular record
- **Audit Report**: lists images processed by user

Additionally, some operational reports are designed for other teams in the organization so they can take action based on a final status in FR. For example, if an image fails enrollment, a letter needs to be sent to advise the applicant that his or her credential cannot be issued until he or she returns to an office for a photo retake.

The ability to retrieve a chronology of events (history) for any image request that enters FR and becomes a record is possible. It includes the history for any activity related to the record, such as any notes recorded, searches completed on the record, and so on.

**Analytical Reports**

Analytical reports are used strategically by management to make long-term decisions and manage staff activity. The details are generally irrelevant, but the aggregations (summaries) are important. The analytical reports defined for FR should provide measurements of key performance objectives. Examples include:

- **Disposition Report**: shows how many cases of fraud have been stopped
- **Central Issuance Management Report**: describes how long people are waiting to get a credential
- **Case Activity Report**: provides the number of images that have flowed through FR system, the number cleared by the system, the number cleared by each user, and the number that remain active
- **Pending Enrollment Report**: identifies how long images are waiting for enrollment in a central issuance environment
Pending Identification Report: indicates how long images are waiting for the 1:N process in a central issuance environment

Case Reports: provides a list of cases and statistics for each workflow type available (e.g., clerical error, criminal activity, research).

**Audit**

Audit responsibilities should be assigned to the entity charged with auditing the agency on an established audit schedule. Jurisdictions should ensure that proper policies, procedures, and controls are in place. Having these in place will avoid audit findings.
As with any processing-intensive and time-sensitive function, incorporating the right technology is critical to the success of the operation of an FR program. Careful planning will also improve the odds that technology costs are balanced against the return on the investment, as well as ensuring added capacity to meet growing demands can be easily and cost effectively performed.

4.1 Facial Recognition Technology

Humans often use faces to recognize individuals, and advancements in computing capability over the past few decades now enable similar recognitions programmatically. Early FR algorithms used simple geometric models, but the recognition process has now matured into a science of sophisticated mathematical representations and matching processes. Major advancements and initiatives in recent years have propelled FR technology into the spotlight. FR can be used for both verifications and identification (open set and closed set).

Facial recognition is a type of biometric software application that can identify a specific individual in a digital image by analyzing and comparing patterns. FR systems are commonly used for security purposes but are increasingly being used in a variety of other applications to include social media.

Facial recognition software is based on the ability to recognize a face and measure the various features of the face. Every face has numerous distinguishable features that enable electronic matching. The following are examples of such features:

- Distance between the eyes
- Length or width of the nose
- Depth of the eye sockets
- The shape of the cheekbones
- The length of the jaw line

These features are measured and create a numerical value that represents the characteristics of the facial structure, which can be efficiently evaluated by software to produce comparison results. Templates are one such method used by some FR systems to represent the characteristics of the facial structure. It is important to understand that FR systems rely on these measurements, and they cannot differentiate gender or race.

Facial recognition systems based on templates can quickly and accurately identify potential matches to the individual of interest when the conditions are favorable and controlled. In conditions when the subject’s face is partially obscured or in profile rather than facing forward or if the light is insufficient, match results are significantly less reliable. The technology is evolving quickly, and there are several emerging approaches, such as three-dimensional (3D) modeling, that may overcome some of the current limitations with the systems.

In May 2014, NIST published test results showing the comparative performance of one-to-many FR algorithms and contrasted this performance with
that that was measured in 2010\(^*\). The results are very relevant to duplicate detection applications such as those implemented by North American motor vehicle administrations.

The NIST report shows that for the four developers who submitted algorithms to NIST in 2010 and 2013, accuracy improved in all cases. In just three years, error rates were reduced from between 10% to 28% for these four algorithm developers. The NIST report also observes that face recognition error rates have declined significantly in the two decades since initial commercialization of the various technologies. Other notable findings from the NIST report include the following:

- As gallery population size grows, accuracy slowly degrades.
- Improvement of image quality is the largest contributing factor to recognition accuracy.
- The accuracy with which human reviewers can reliably adjudicate the most-similar faces returned in a large-population one-to-many search remains poorly quantified.

As with other biometrics, accuracy of FR implementations vary greatly across the industry. Absent other performance or economic parameters, users should prefer the most accurate algorithm.

Facial recognition use is not centric to governmental institutions or private corporations. There is extensive development and focus on smartphone applications for use in social media, gaming, and targeted marketing. For example, Facebook uses FR software to help automate user tagging in photographs.

### 4.2 Standards

Standardization is a vital portion of the advancement of the market and is necessary to avoid vendor lock-in. For FR, data interchange standards facilitate interchange of the biometric data themselves and enable interoperability of FR systems. For this type of standard, software exists to formally test conformance of images to the standards. However, it should be noted that several methods are used to represent the characteristics of a facial image; and as such, no standards exists for the numeric value used to represent the characteristics of the facial images that are produced by the proprietary face recognition algorithms supplied by various vendors. Therefore, the different methods used by FR systems to represent the facial structure are not interoperable and are not “future proof” with respect to evolving technology. Although open-source FR algorithms are available, their matching accuracy is far behind that of commercial FR products available today. Therefore, it is important to always retain the facial images in standards-conformant containers within the FR system. This will allow for the enrollment of historical images when updating or replacing an FR system in the future.

**Recommended Data Elements**

In addition to data interchange standards, standards defining the structure and format of data elements contained in a record should be adhered to when transmitting to another site or agency.

The assignment of a record’s unique identifier associated with each image is at the discretion of the jurisdiction and should be carefully considered during the development of the FR system. Two main factors should be considered. The first is limiting the identifiers to data currently captured during the credential issuance process to avoid an increase in workload at the driver testing stations. The second is to be as inclusive as possible to expand the capabilities associated with uploading images for purposes of investigation.

Additional record identifiers provide mechanisms for limiting the images searched. For instance, if an image of a woman is uploaded and no matching criteria is
The ANSI/INCITS (M1) 385-2004 and its related international standard ISO/IEC 19794-5:2011 Face Recognition Data Interchange Format are the face recognition standards and address detailed human examination of face images, human verification of identity, and automated face identification and verification.

ISO/IEC19794-5 has established a defined frontal image and is broken into subsections addressing full-frontal and token images. A full-frontal image is defined as an image within five degrees from center. A token image is defined by the location of the eyes. These standards leave other images, such as semi-profile, undefined but ensure that enrolled images will meet a quality standard needed for both automated FR and human inspection of face images. Work is underway at both the national and international levels to update the standards for 3D face data. These standards also facilitate the use of face information in applications that have limited storage (e.g., passports, visas, and DLs).

ANSI/NIST ITL 1-2011 Data Format for the Interchange of Fingerprint, Facial and Other Biometric Information is a standard that defines the format of records that form a transaction to transfer biometric information between sites or agencies. Type 10 image records contained in this standard are used to exchange image data from the face as well as images of scars, marks, and tattoos.

Other standards, such as ISO/IEC 19785 Common Biometric Exchange Formats Framework (CBEFF), deals specifically with the data elements used to describe the biometric data in a common way. The ISO/IEC 19784-1 BioAPI specification defines the Application Programming Interface and Service Provider Interface for a standard biometric technology application. National and international standards organizations continue to work on the progression of these standards.

<table>
<thead>
<tr>
<th>Data Elements</th>
<th>Mandatory</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential Number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unique Identifier</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credential Type (DL, ID, DPC, EDL)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSN/SIN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>First Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Middle Initial</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>City</td>
<td></td>
<td></td>
</tr>
<tr>
<td>State</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zip</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date of Birth</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Height</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weight</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Eye Color</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hair Color</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gender</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Race</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wearing Glasses</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Image Capture Date</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capture Operator</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capture Machine Name/Capture Station</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This chart provides a list of typical data elements of an image capture transaction.

selected, results for both men and women will likely be returned. However, if gender is a record identifier in the database, the user can limit the results to women, thereby increasing the opportunity for a potential match.

Much work is being done at both the national and international standard organization levels to facilitate the interoperability and data interchange formats, which will help facilitate technology improvement on a standard platform. A few of the key standards include:

* NIST Special Publication 500-290
The Organization of Scientific Area Committees (OSAC) Subcommittee on Facial Identification (SFI), formerly known as the Facial Identification Scientific Work Group (FSWIG), is involved in gathering and disseminating accurate information regarding the proper application of facial identification (FI) and FR methodologies and technologies. OSAC SFI delegates include scientists, practitioners, and managers from federal, state, local, and international agencies with criminal justice, intelligence, or homeland security responsibilities, to include representatives from the academic and research communities.

The mission of OSAC SFI is to develop consensus standards, guidelines, and best practices for the discipline of image-based comparisons of human features, primarily face, as well as to provide recommendations for research and development activities necessary to advance the state of the science in this field.

OSAC SFI seeks to leverage constituency group and stakeholder knowledge to produce guidelines, position statements, and address other issues including:

- Prioritized research and development needs, especially population studies and statistical validation
- Exchange of information and ideas
- Best practices
- Cognitive and system bias mitigation
- Ensuring conformance with regulatory reports
- Training to competency standards for experts and technicians
- Quality control and quality assurance standards
- Certification recommendations
- Proficiency testing recommendations
- Ethical issues
- Legal issues
- Source book creation
- Defining FI and FR use cases

OSAC SFI is working to ensure that standards related to FI and FR are consistent with those across the entire forensic community. Please visit the OSAC’s website for more information about OSAC (http://www.nist.gov/forensics/osac.cfm).

Limitations

It is important to have a contingency plan in place when an image fails to successfully enroll in an FR system. Poor quality image samples, user confusion, evasion or noncooperation, inadequate or excessive lighting, dirty cameras, thick-rimmed glasses, and excessive facial hair are some of the issues that present limitations in the use of the technology.

Performance Factors

System match performance is contingent on the following factors:

- Verification: Assuming good image quality, FR systems are highly accurate in matching a probe image against the image(s) associated with a single record (one-to-one verification task).

- Identification: FR systems are less accurate in attempts to identify individuals in which the system seeks to match an individual’s face with any possible image “on file” (one-to-many identification task). This type of search is likely to produce more than one match candidate that has a similarity score above the target threshold. Resolution of multiple match candidates must rely on human intervention for final adjudication.

* The OSAC Committee on Facial Identification (formerly known as FISWG). https://www.fiswg.org
Image quality: Sources of failure can be attributed to inconsistencies in pose, illumination, and expression. Other negative performance impacts can result from low camera resolution, optics distortion, or overcompression of the image. The more similar the environments of the images to be compared (background, lighting conditions, camera distance, size and orientation of the head), the better the FR system will perform.

Accuracy: If existing standards for images are met or exceeded, most of the current top-performing FR systems will deliver a relatively high level of accuracy for the identification task.

Time elapsed between captured images or aging: The less time that has elapsed between the images to be compared, the greater one can rely on the comparison results. The NIST testing has concluded that error rates increase with age from six years on—but not significantly. Also, the NIST has determined that some FR algorithms are better than others when comparing images of the same subject separated by age.

Consistent camera use: The more similar the optical characteristics of the camera used for the enrollment process and for obtaining the onsite image (light intensity, distortion, focal length, color balance), the more efficient the FR system will perform.

Gallery size: A gallery is the array of photographs returned of potential matches when performing a one-to-many inquiry. Restricting or filtering (e.g., using age range, gender, and so on) the size of the searched image repository in identification applications may improve utilization of available adjudication staff but could exclude potential cases of fraud.

The selection and composition of images that are used to develop the FR algorithms are crucial in shaping the eventual performance of the system.

4.3 Performance Metrics

Performance metrics commonly take the form of rates. For each metric, it is important to note that the measured or observed rate noted in any evaluation is distinct from the predicted or expected rate that occurs in deployed, fully operational biometric systems (predicted or expected performance rates may be gauged using measured or observed rates). Metrics are calculated from representative test data for a specific matching algorithm, and performance will vary based on demographics, sensor quality, lighting, and data format.

Common performance metrics include:

- Failure to enroll rate (FTE): The FTE rate is the proportion of enrollment transactions in which an image fails to successfully enroll. FTE can apply to overall enrollment or to the enrollment of specific biometric instances. Image sample quality and user–system interaction can influence FTE. Successful enrollment encompasses biometric detection and acquisition.

- False match rate: The false match rate is determined by the number of impostor comparisons that produce a score greater than or equal to the threshold divided by the number of impostor comparisons attempted.

- False non-match rate: The false non-match rate is determined by the number of genuine comparisons with similarity score less than the threshold divided by the number of genuine comparisons attempted.

- False-positive identification rate (FPIR) and selectivity: The FPIR is the proportion of identification transactions in which an imposter
subject is incorrectly matched by a biometric system. In many cases, this metric is derived from a system in which the genuine mated pair is not enrolled at all. Selectivity describes the expected number of false-positive identifications returned for a single transaction and may be greater than one. For example, a single transaction that returned five false matches would only count as a single false-positive identification but would be counted five times toward selectivity. Both metrics generally grow linearly with database size. A 10-fold increase in database size will lead to roughly a 10-fold increase in selectivity and a 10-fold increase in FPIR if FPIR is much smaller than 1.

- True-positive identification rate (TPIR), reliability, or hit rate: The TPIR, reliability, or hit rate describes the proportion of identification transactions in which a genuine subject is correctly matched by a biometric system. TPIR is generally close to the true match rate. However, as databases grow, the TPIR will increase slightly. This is because of rank-based search strategies that sometimes crowd out a genuine match if there are many potential imposter matches. In multipass configuration, the first and second passes are often rank limited even if the final pass is based on a threshold.

- False-negative identification rate (FNIR) and miss rate: Subtracting TPIR from 100% results in the FNIR or miss rate.

- Precision: Precision is the probability that a given match is genuine or the fraction of all matches that are genuine. Unlike the previous metrics, it depends on the prior probability that the subject submitted to a database is enrolled in it. It is often determined empirically by reviewing potential matches through other means. Precision generally does not change significantly as databases grow. A 10-fold increase in database size will usually yield 10 times as many false matches and 10 times as many true matches in the same ratio. Precision can be theoretically determined by calculating the total number of false matches and true matches expected from a given transaction. The number of false matches can be determined from the selectivity. The number of true matches is based on how many genuine records are expected to be enrolled per probe subject.

If subjects are uniformly and randomly selected from a population of fixed size, selectivity is the size of the database divided by the size of the population. For example, in a fixed population of 10 million residents, there is a 10% chance that any person would be contained in a 1 million person database and therefore 0.1 expected true comparisons. Multiplying 0.1 by the TPIR will yield the expected number of true matches.

For anti-fraud or de-duplication, however, the expected mated records are not searched. Any remaining mated records that exist are due to an automated or clerical filing error or due to fraud. This significantly reduces the expected number of true matches and affects the precision. Because of improvements in clerical processes and effectiveness of anti-fraud investigations, this number will tend to go down over the lifetime of a system. Results from several jurisdictions imply that roughly 0.1% to 1% of customers will have extra enrollments that result in true matches and that there are roughly three times as many true matches caused by clerical error as caused by fraud.

The nontechnical variables impacting precision are the size of the population that may ever be enrolled, the likelihood of clerical error, and the prevalence of fraud.
4.4 Image Capture

Good portrait images that support credential issuance also support FR. The AAMVA’s DL/ID Standards and Secure Design Principles provide guidance to DMVs for obtaining optimal portrait image capture, and it can be applied in other controlled environments where an organization captures still portrait images.

Pose: The portrait shall depict the face of the rightful cardholder in a full-face frontal pose with both eyes visible (i.e., captured perpendicular to an imaginary plane formed parallel to the front surface of the face). The portrait may only show the cardholder with headgear if the cardholder is a member of a religion requiring the wearing thereof and provided that the headgear does not present as an obstruction or present a shadow and render the portrait inadequate for the identification of the cardholder. Jurisdictions that incorporate FR biometric technology may wish to ensure eyeglasses are removed to aid in consistent identification of the credential holder.

Depth of field: A full-face frontal pose shall be in focus from the crown (top of the hair) to the chin and from the nose to the ears.

Orientation: The crown (top of the hair) shall be nearest the top edge of Zone III as defined in the AAMVA’s DL/ID Standards and Secure Design Principles, e.g., the crown to chin orientation covering the longest dimension defined for Zone III).

Face size: The crown-to-chin portion of the full-face frontal pose shall be 70% to 80% of the longest dimension defined for Zone III,* maintaining the aspect ratio between the crown-to-chin and ear-to-ear details of the face of the cardholder.

Lighting: Adequate and uniform illumination shall be used to capture the full-face frontal pose, that is, appropriate illumination techniques and illumination shall be used to achieve natural skin tones (and to avoid any color cast) and a high level of detail and minimize shadows, hot spots, and reflections (e.g., those caused by eye glasses).

Background: A uniform light blue color or white background shall be used to provide a contrast to the face and hair. Note: Preference is for uniform light blue color, such as Pantone 277. Although the specific Pantone color is not a requirement, a uniform light blue color or white background is a requirement.

Centering: The full-face frontal pose shall be centered.

Additional guidelines: The following items summarize additional image guidelines for images captured for use in FR.

- Minimum dot per inch (DPI) is based on having 64 pixels between the centers of the eyes within the photo. For legacy photos used for DL/IDs, 72 DPI is a practical minimum because of the small image size.
- JPEG and PNG formats are most commonly used for secure credential issuance.
- The face substantially fills the frame of the image.
  - Optimum is chin to hairline being 80% of the height of the image.
- Scaling up the image does not improve the results.
- Minimum overall image resolution of 128 x 128 pixels
  - Maximum overall image resolution of 1024 x 1024 pixels
  - Images can be color or gray scale.
Forward-facing pose
– Face fully visible; avoid hair in face area

Neutral expression
– Helps matching against other images with non-neutral expression

Avoid eyeglasses.
– Glare affects enrollment.
– Heavy glasses affect comparison.

Avoid headwear when possible.
– When headgear is allowed, the chin, ears, and forehead must be visible.

Hey general rule: If something blocks the pupils of the eyes, FR results will be inaccurate.
– Operators should be trained on what constitutes a good image. In addition, they should be trained to detect evasive behavior (a deliberate nonconformant presentation). For example, a nonfrontal pose might be an attempt to evade a duplicate license check.

4.5 Image Compression
For efficiency of data storage, facial images are often compressed, with most FR systems following one of the JPEG standards developed by the Joint Photographic Experts Group (JPEG). Compression methods used in FR are called “lossy” because data are discarded or lost. The degree of compression can be adjusted to an optimal level that minimizes the amount of data retained while not harming the FR system’s matching accuracy. More information on the history of JPEG and the various versions available can be found at www.jpeg.org.

Retained facial images should have a target size of 40 KB for a 640 x 480 token image. Compression should be performed on the source image and not recompressed.

4.6 Search Engine Technology
Biometric search engines provide comparison results that FR solutions use for daily batch screening operations and interactive investigation tools. For screening of credential issuance, the biometric search engine is typically composed of several services that manage interactions with the biometric algorithms. These services include:

- Batch processing services that accept photos from the agency and move them through enrollment and search operations
- Enrollment services that transform the photo into a biometric template and store the image within the database to be used for identification and verification matching
- Matching services that leverage biometric algorithms to perform identification and verification functions
- Application processing services that manage overall processing, exception handing, monitoring, and so on

Algorithms
Facial recognition algorithms are computer instructions that generally perform the following three functions:

- Image processing: Could include image enhancement or checking the quality of the image against a predetermined standard.
- Feature extraction: Process that identifies the points of interest (features) in the digital image that are relevant to the matching process. These features are then extracted, and a mathematical representation of the image is generated.
Matching: Process of comparing multiple facial representations. The result of the matching process is a similarity score, which is then compared with the threshold value to determine a match or no-match decision.

It is important to note that FR algorithms are proprietary and unique to each vendor and may include additional functions as well as different methods and techniques.

Identification and Verification

The utility of biometric comparison systems can be fundamentally described by two basic concepts, identification and verification. Identification is the process of searching for a biometric match of a given probe image within a gallery of images. Verification is the process of comparing one image with one other image, with the expectation that those two images will match biometrically. The remainder of this section describes the technology and applications that give investigators the necessary tools to perform these identification and verification operations as a reliable component in carrying out their daily investigative work.

NIST Testing Perspective

Biometric algorithms are the focus of a series of NIST evaluations of accuracy and performance. These tests offer some insight into algorithm support for DL/ID screening; however, agencies must evaluate other criteria such as product maturity, extensibility, scalability, and cost to assess how well the entire solution fits within their overall business operations.

Facial recognition algorithms can be used to verify a claimed identity (e.g., for credential reissuance) or to identify someone (e.g., to find an applicant using an assumed name). In the latter case, an algorithm will return a candidate list that enumerates hypothesized identities for a search sample. FI algorithms can be set up to be used in two distinct modes. The first, investigational mode, assumes the existence of a workforce of human face examiners who are manually adjudicating images on candidate lists to resolve false matches. In the second, identification mode, the algorithm is set up with a high threshold to give very short candidate lists and a small chance that a nonmatching candidate is returned. Stringent thresholds make false matches rare but at a cost of elevated miss rates. The most accurate investigational algorithms are not the most accurate identification algorithms.

NIST testing concluded that the most accurate FR algorithm, the chance of identifying the unknown subject (at rank 1) in a database of 1.6 million criminal records is about 92%. This figure depends critically on the image quality achieved during photographic capture. Higher quality—which can be obtained with improved lighting, cameras, subject cooperation, and photographer training—will yield much improved accuracy. On the other hand, NIST showed that, in the investigational mode, identification accuracy reduces as the enrolled population size grows, although the rate of accuracy reduction is quite slow and decreases linearly with the logarithm of the population size.

When the most accurate algorithm is used in an investigational mode to provide trained examiners with the top 50 ranked candidates, 97% of searches will yield the correct identity in a fixed population of 1.6 million subjects. In cases when the top 200 candidates are searched, the correct match is present 97.5% of the
Uniformly sufficient lighting is, however, the most important aspect in capturing a quality portrait image. Harsh lighting from above or from the side or a lack of lighting can cause diminished performance. As with professional photography, sufficient ambient lighting is just as important to the quality of the resulting portrait image as is the lighting provided by the camera’s flash.

**Analyst or Examiner Workstations**

Effective FR relies as much on human factors and experience as the technology performing automated comparisons. Ultimately, an experienced examiner will make the final “match/no-match” determination using manual and visual analysis.

The examiner should be provided a well-lit, ergonomic workspace. This will decrease fatigue over the course of a shift. Workstation displays should be glare resistant and of sufficient size, and aspect ratio, to support the side-by-side display of two full-size portrait images along with a useful set of comparison controls or other inputs or visual tools provided by the image comparison software.

Display resolution, aspect ratio, and diagonal size all typically work together to define the viewable size of a computer monitor. Other factors, such as color depth, refresh rate, brightness, and contrast, each plays a factor in the usability of the monitor but are more related to subjective human factors and may involve the video card capabilities. However, for the purposes of this activity, the primary interest is the geometry of the screen and the utility of displaying side-by-side images within the context of the image comparison application or tool.

Screen resolution plays a role in the total amount of information that can be viewed but must always be considered in context of the application(s) in use and how each presents information. Typically, a display resolution lower than 1280 in the horizontal direction, time. The hit rate increases roughly linearly with the log of the number of candidates inspected.

In identification mode, when high thresholds are used, an increase in the population size will usually lead to more false matches, and this in turn will necessitate an increase in threshold. Some systems are able to automatically adjust thresholds to maintain low false match rates as the enrolled population grows. In all cases, a secondary (human) adjudication process is necessary to verify that the top-rank hit is indeed that hypothesized by the system. The adjudicator will be able to consider other “case” information to assess whether the system has found a fraudulent claimant or has returned a false match.

### 4.7 Devices and Equipment

The heart of FR is software based. It is important to recognize that equipment for the user to interact with the system is crucial. Following are some considerations for configuring equipment in various environments.

**Cameras and Lighting**

One of the benefits of using a facial image as the biometric is that unlike a fingerprint, acquisition of the biometric image is unobtrusive and can be easily acquired using a commercially available digital camera. Selecting an appropriate digital camera and related lighting and background equipment is an important consideration.

Portrait composition, and to some degree lighting, are discussed in other areas of this chapter. Uniformly sufficient lighting is, however, the most important aspect in capturing a quality portrait image. Harsh lighting from above or from the side or a lack of lighting can cause diminished performance. As with professional photography, sufficient ambient lighting is just as important to the quality of the resulting portrait image as is the lighting provided by the camera’s flash.
and 900 in the vertical direction, should be avoided. For example, a 19” to 23” diagonal, 16:10 (1.6:1) aspect ratio widescreen computer display capable of displaying 1440 x 900 pixels will satisfy these criteria and is commonly available today. By comparison, some older 16:10 displays were offered at 1280 x 800, and some newer “Windows 8, HD Ready, HDTV 720p/1808i” displays are 16:9 but only 1366 x 768 and simply do not provide enough vertical resolution to avoid constant scrolling of the screen by the user.

No specific FR-related requirements are made on the workstation personal computer (PC). Except in some increasingly rare cases, all FR comparison computations are performed in the back office. However, some application vendors choose to perform FR verification (1:1) comparisons locally on the workstation PC, but these calculations are easily managed by a modern dual-core processor-based PC.

**Tools Available to Verify Identities**

There are a number of commercially available tools to assist analysts and investigators in confirming the matching results. A few examples include:

- **Detailed zooming:** Allows users to zoom in close to a specific facial feature on two images simultaneously. If users needed to compare ear shape or lip structure closely, this tool will help with the review.

- **Split screen layer:** Used to align two images and see how facial features line up. For example, using split screen will take half of the probe image face and align it with the other half of the target image face. Users can drag the face side by side to examine how the eyes, lips, and nose line up.

- **Image overlay:** Provides the option to take the target image and overlay or superimpose the image over the probe. Users can drag a slider bar to swap from probe to target and review similar facial features.

- **Color adjustment and removal:** Provides the ability to remove color from the image making it black and white.

- **Image rotation:** Provides the ability to rotate facial images by 180 degrees, a proven method for enabling the analyst to concentrate on key facial characteristics, when comparing two facial images.

- **Additional tools:** Other tools may be included in an analyst workstation. Be sure to obtain a comprehensive listing of the tools available before making a final purchasing decision.

### 4.8 Networks, Bandwidth, and Communication

Two areas of network performance are typically considered in supporting an FR system: the front office (examiner workstations) network and the back office network where the FR comparison array nodes communicate with their controller.

Office bandwidth, estimated at 200 to 300 kilobytes-per-second (KBps) per user, should be sufficient for normal workstation use. For the back office, a dedicated network is optimal between the FR system’s controlling server and its local database server (via one network card) and the controlling server and the array of comparison node computers (via a second network card). Incoming comparison and enrollment requests from relying systems normally arrive on yet another (third) network interface to the controlling server. All of these back office servers can usually achieve the desired performance over standard gigabit Ethernet interfaces.

Network and bandwidth speed may depend on external factors such as network latency over wireless broadband networks. Remote field users using commercial wireless networks may sometimes experience a slow return of the image gallery after the
network requirements for an FR system. It is therefore recommended that before selecting and implementing an FR system, IT professionals are engaged early in the decision making process so that a careful assessment on system requirements is performed and appropriate standards followed.

probe image is submitted because of being connected to older 2G and 3G technologies. 4G technology has advanced to the point where network speed is equivalent to a Wi-Fi or wired network. It is important to note that this document does not attempt to replace or define IT architecture or
Training that includes information on a multitude of topics for various levels of staff and management of the motor vehicle agency that uses FR technology should be developed and delivered. Additional training for external users, external partners, and those involved in prosecution is beneficial to complete the educational process that is necessary to deploy a complete and highly successful FR program. As technology in FR continuously develops, so should the training.

Classroom training provided by SMEs is recommended over online or other training methods. SMEs can be part of the jurisdiction’s staff, the vendor team, or a combination of the two. Training should involve examples and actual case studies in which FR has proven to add to successful subject verification and case closures. The training regimen should also involve examples of challenges in the use of FR and what could or could not occur if poor quality images are used.

**Training Matrix: Who Should Be Trained, and What They Should Be Trained On**

<table>
<thead>
<tr>
<th>Training</th>
<th>Field Office Staff</th>
<th>Analyst or Investigative Analyst</th>
<th>Investigator</th>
<th>Administrator</th>
<th>IT Operations</th>
<th>IT Support</th>
<th>External Users</th>
<th>External Partners</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limitations of Technology</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ethical Use and Privacy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Processes and Procedures</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Access and Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Usage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comparing Faces</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Specialized Facial Comparison Training</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Case Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Photo Requirements</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Biometric Technology</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Systems and Software</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Refresher Training</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


**Limitations of Technology**

Facial recognition identity comparisons do not provide explicit yes-or-no results. The results are “probable matches” that need to be reviewed and investigated by a qualified staff member to make a determination. This training provides an introduction to technology limits for FR.

Training should emphasize that FR is an investigative tool that allows the investigator to potentially identify a subject via photo image capture and image gallery development. This is not an absolute when attempting to identify an individual; it is simply another tool to aid in the identification and subsequent verification of a subject. Several challenges that detract from a quality image capture include the angle in which the subject’s face was captured, lighting, clarity, sunglasses, or a low-pulled cap. These are only some of the variables that affect the strength of a photograph.

In the end, trainers should ensure users understand that they must make the determination that the subject in question is indeed the subject located within the image array produced from the established dataset. This should not be based solely on the believed match of the captured image and generated image gallery but as part of the overall evidentiary collection gathered for the purpose of verifying an unknown subject. The collective investigative process leads to a final determination, not the presence or absence of a potential match by itself.

**Ethical Use and Privacy**

An FR system contains highly sensitive personal information; therefore, is surrounded with special rules regarding its use and disclosure of PII. Ensuring that all involved with using and managing the system understand those rules is essential to the continuation of a successful FR program.

It is recommended that this portion of the training should include but not be limited to the following information:

- Data contained within the FR system must be maintained according to provisions of laws, regulations, and agency policies and should be protected from unauthorized access, use, and disclosure.
- Resources are to be used exclusively for the agency’s business unless otherwise approved.
- Authorized users may access, use, and disclose information only when necessary to perform work assigned by a supervisor to accomplish the agency’s mission and objectives.
- Information contained in the FR system should not be accessed or used for personal reasons.
- Authorized users should not process their own personal transactions or transactions involving friends, family members, colleagues, or anyone known to them without prior disclosure and authorization from a supervisor. A supervisor must be notified immediately if a transaction involves any possible conflict of interest.
- Information from the FR files or databases may be disclosed only to individuals who have been authorized to receive it through the appropriate agency procedures.
- False, misleading, or incomplete data should not be deliberately entered or deleted.
- Unauthorized action may not be deliberately taken that would cause the interruption of electronic data processing services or the destruction or alteration of data files or software.

Training should include possible ramifications for violations of ethics and privacy policies.
Processes and Procedures
Training for the processes and procedures specific to your jurisdiction should be tailored to each user group. For example, investigators—whether internal or external to the agency—should have training based on system use but not necessarily on systems and software. The training may come from either a train-the-trainer setting or directly from the vendor providing the FR solution.

User Access and Security
It is important that users and managers understand the basics of the security protocols in place that limit access to the FR system. Securing the system is fundamental to the protection of the PII contained in the system. Training should help users understand user access and security policies, for example, that deliberately sharing use of an account or password is prohibited.

Application Usage
Application usage training should consist of everything from accessing the system to adjudicating cases reported by the system. The FR system vendor may be a valuable resource in providing application usage training, so it is important to include training services in the Request for Proposal (RFP) process.

Comparing Faces
Training for examining an image and the individual’s facial characteristics is an important topic to cover with the appropriate users. FR-related training programs are available for a jurisdiction to provide this type of training, and it is recommended that these will enhance the skills. The AAMVA’s Fraudulent Detection and Remediation (FDR) program is an excellent resource to augment an FR training program.

Specialized Facial Comparison Training
The Federal Bureau of Investigation, CJIS Training and Advisory Process Unit, is one source of independent training to assist jurisdictions. For information, contact biometric_training@leo.gov.

Case Management
Training should provide guidelines for managing cases that includes the use of FR and the supporting evidence it can provide. A multistep process is often used to review and adjudicate probable matches, ensuring that cases are managed efficiently. Potential training topics include investigation process overview, case components, case phases and dispositions, and tracking and reporting.

Photo Requirements
The strength of an FR program is fundamentally reliant on the proper capture and enrollment of the facial images. To ensure maximum enrollment success, adequate training on photo capture is of paramount importance. For identifying the image quality factors that may be part of this training, refer to Chapter 4: Technology, Image Capture subsection.

Biometric Technology
Training should include an overview of what a biometric is and why FR is considered a biometric. Distinguishable features such as those described in Chapter 4, Section 4.1 provide fundamental information that should be included in this training.

Systems and Software
Facial recognition systems involve multiple applications operating across several servers that may be interfaced with multiple agency systems, including record databases, operations monitoring, network access and security, and DL/ID document issuance. Training should provide knowledge and details required to support and manage daily operation of the systems.
Refresher Training

For most users, refresher training should occur at least annually, if not more frequently. However, the frequency for each user type and the training content will differ based on level of program usage and technical expertise needed. Three training components that should be conducted annually are the limitations of the FR technology, the ethical use of the system, and user access and security. Changes to program policy and operations should be included in training as part of implementation.

Refresher training provides updates, examples of positive investigative outcomes, various uses of FR, and perhaps a renewed confidence in the program as a whole. The importance of providing end users current and useful updates or enhancements in an FR program is paramount in continuous development of a beneficial image dataset and subsequently, positive investigative outcomes.

Prosecutor Training

In addition to the training identified in this chapter, it is essential that prosecutors are educated on the fundamentals of FR technology and how it is used as part of the DMV credential issuance process, as well as system capabilities and limitations.

Prosecutors, in particular, should understand the limitations on the information an analyst can provide when testifying. Case law of relevance to FR that prosecutors should be familiar with includes Supreme Court rulings on scientific evidence such as Daubert v. Merrell Dow Pharmaceutical, Inc., 1993; Frye v. United States, 1963; and Alberta v. Hutterian Brethren of Wilson Colony.
The privacy of the DMV customer and the protection of personal information must be paramount. Privacy advocates have expressed concerns with the use of FR and some believe that images may be used to infringe upon civil liberties and other constitutionally protected rights of law abiding citizens. They believe that government agencies may be using facial images to track their every move, infringe on their right to free speech, and to violate other constitutionally protected rights. Advocates further argue that FR can be used not only to identify an individual, but also to unearth other personal data—such as other photos featuring the individual, blog posts, social networking profiles, Internet behavior, travel patterns, and so on. Unfortunately, many crime shows only serve to fuel this perception.

Although biometric matching itself raises privacy concerns, most privacy risk actually comes from associated data sharing. Many types of sensitive customer data might be received from or shared with other agencies, under various criteria. The collecting agency has primary responsibility for shared records. The export of DMV-collected customer data should be carefully controlled.

Given the value of FR software to DMVs and law enforcement, it is imperative that DMVs address the privacy concerns of our citizens. The following are offered as best practices:

- DMVs operating an FR program should develop strict policies on both acceptable and prohibitive uses of facial images. Policies should clearly outline the administrative, civil and criminal consequences for inappropriate use.

- Internal and external users should be required to sign statement of ethics, confidentiality agreements, or Memorandums of Understanding, as appropriate. See Appendix C and D for sample MOU and Application for Requesting an FR Comparison.

- Implement an audit program of the operation of FR processes to ensure compliance with privacy policies and usage guidelines. While internal audits may be sufficient, an audit by an outside entity is recommended.

**Privacy in the United States**

The Driver Privacy Protection Act (DPPA or Act) of 1994 governs the manner in which U.S. DMVs may release personal information regarding holders of DLs and defines penalties for misuse by agencies and individuals. Congress passed this Act as an amendment to the Violent Crime Control and Law Enforcement Act after it was learned that criminals were obtaining and/or accessing personal information from DMVs and using it to carry out violent crimes. In essence, DMVs are prohibited from knowingly disclosing and/or making available personal information outside the parameters of the Act. The DPPA defines personal information that identifies an individual, such as a photograph, social security number, driver identification number, name, address (not their zip code), phone number and any medical or disability related information. Relative to facial images, the DPPA designates an individual’s photograph or image (as well as one’s social security number and medical and disability information) as “highly restricted personal information”.

* 18 U.S.C.A. Section 2721
Privacy in Canada

In Canada, an extensive privacy framework was developed, beginning with the 1978 passage of the *Canadian Human Rights Act* which covers the use of personal information by the federal public sector, followed by the passage in 1983 of the federal *Privacy Act*, and similar provincial and territorial legislation. For example, in Ontario, the *Freedom of Information and Protection of Privacy Act (FIPPA)* focuses on the public sector at the provincial level. The role of the Information and Privacy Commissioner (IPC) at both the federal and provincial levels is set out in the privacy legislation, and generally the IPC acts independently of government to uphold and promote open government and the protection of personal privacy.

While jurisdictional law may not infringe on the federal protection afforded by the DPPA, many jurisdictions have imposed further restrictions on the use and dissemination of facial images.

There currently are no comprehensive U.S. privacy laws that specifically address biometric data. However, other federal statutes that include requirements for protecting personal information include:


- **Cyber Privacy Fortification Act** ([http://www.gpo.gov/fdsys/pkg/BILLS-113hr1121ih/content-detail.html](http://www.gpo.gov/fdsys/pkg/BILLS-113hr1121ih/content-detail.html))

The security of PII must be of supreme priority to prevent data breaches. Agencies must develop comprehensive policies and procedures for protecting the confidentiality of PII, including FR data.
**Facial Image Access and Dataset Sharing**

A strong working relationship between motor vehicle agencies and law enforcement is essential to public safety, homeland security, and identity protection. Sharing of FR data can play an important role in meeting local, state, and federal public safety goals. It can reduce costs for administering public services by providing efficiencies in demonstrating constituent identity and in detecting suspicious activity.

There are many benefits to shared access. One of the most important is the establishment and maintenance of a strong relationship between law enforcement and the DMV. This is particularly important in jurisdictions in which the DMV does not have a dedicated investigations unit to handle fraud. Cooperation between the two entities needs to exist to assist and facilitate with the identification, arrest, and prosecution of criminals.

There are numerous questions surrounding the issue of allowing law enforcement to have access to DMV-owned FR resources. Should access be direct or indirect? Should a particular threshold exist for access? How is access controlled and documented? How much access should be allowed? Are there privacy considerations that need to be addressed? Each jurisdiction must follow its own legislation and policy in sharing data.

Sharing of information allows government to be more efficient in fighting crime and protecting identities. The sharing of FR technology can serve as a proactive, early intervention, and preventive crime-fighting measure. It provides an opportunity for sharing resources and data to enable motor vehicle agencies to enhance the DL enrollment process and for law enforcement to expand their investigative resources. When properly implemented, the technology can assist all government agencies in preventing fraud from evolving and escalating.

A myriad of options, from simple to complex, are available for sharing FR technology. Options range from providing a service that offers facial recognition comparison requests and incorporating criminal images into the DL database to fully integrating the DL and criminal image databases and jointly using the FR technology for DL and criminal identification enrollment processes.

An effective tool to combat the criminal element is through legislation and subsequent MOUs allowing interjurisdictional FR access to image databases. From a motor vehicle perspective, full integration of the DL and criminal identification enrollment processes provides another level of opportunity to reduce fraud and identify theft. Integration increases the likelihood of identifying fraud attempts during credential issuance because some applicants may have a criminal history linked to their true identity.

**Additional Uses of Facial Recognition**

Facial recognition technology provides opportunities for development and expansion of services including:

- Identification of criminal suspects
- Identification of deceased, injured, or incapacitated individuals
- Identification of prison inmates or visitors
- Identification and protection of victims during catastrophic events
- Identification and regulation of individuals subject to sex offender registry requirements
- Creation of photo lineups
- Reducing entitlement and benefit fraud

**Types of Shared Personally Identifiable Information**

Data elements that may be shared with approved external entities include photographs, biographic and demographic information, and biometrically determined links between records. Although guidance may exist for the sharing of photographs and biographic records, two biometric-specific considerations need to be evaluated.

First, a potential link between two identities is a new piece of data, with different implications in different contexts. For example, whereas a link within a DMV database implies a clerical error or fraudulent activity, a link between a DMV record and a law enforcement record implies that the customer had a previous law enforcement contact. Jurisdictions should ensure that only authorized individuals or entities have access to such information. Second, photo-matching tools may return false matches, which necessitates the need to make PII data available to authorized investigators. Because of this, it may be necessary to modify existing privacy protection policies.

When considering the release of data, jurisdictions must take care to protect intentionally disguised identities such as undercover law enforcement officers and those in witness protection programs. Such data should not be released to outside entities and should be accessible by only authorized DMV employees.

Potential sharing arrangements that can be established are illustrated in the following chart.

<table>
<thead>
<tr>
<th>Data Shared</th>
<th>Lookup Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>In</td>
<td>Out</td>
</tr>
<tr>
<td>Import of another agency’s photographs, for anti-fraud investigations (e.g., Department of Corrections dataset)</td>
<td>Bio, Photo</td>
</tr>
<tr>
<td>Import of another agency’s photographs, to support the agency’s investigations (e.g., watch lists, warrants)</td>
<td>Bio, Photo</td>
</tr>
<tr>
<td>PII records returned to other agencies based on a biographic query using text matching or an ID# lookup</td>
<td>Bio</td>
</tr>
<tr>
<td>PII records returned to other agencies based on a combined biographic lookup and biometric verification</td>
<td>Bio, Photo</td>
</tr>
<tr>
<td>Match/no-match decision returned to other agencies based on biographic lookup and biometric verification</td>
<td>Bio, Photo</td>
</tr>
<tr>
<td>PII records returned to other agencies based on submitted nonconsensual still (e.g., law enforcement investigation)</td>
<td>Photo</td>
</tr>
</tbody>
</table>
Establishing a Memorandum of Understanding: A Critical Juncture

When entering into a partnership of data sharing, an MOU should be executed to ensure responsibilities and expectations are established. The MOU should not retract from the FR process; however, a clear understanding and agreement of the process and protocols is essential to establishing and maintaining a mutually successful partnership. An example of an MOU can be found in Appendix C.

Jurisdictions that elect to share services, such as FR comparison requests, may elect a less formal partnership process than an MOU. An application for requesting an FR comparison may be used as documentation and for informing the requestor of the allowed use of the returned results. An example of an application form can be found in Appendix D.

Security and Access for Database and Records

Jurisdictions must retain the public’s trust by reaffirming their commitment that personal information will be kept safe and secure when information is shared. Enacting strict policies regarding the development and usage of an FR program is essential.

As discussed in Chapter 6, PII should be protected against unauthorized access and accidental disclosure. A clear policy should be established that governs both DMV personnel granted privileges to access records and any external organizations with which records may be shared. The system must provide protections from physical and signal-related intrusions and unauthorized attempts to exploit the system.

Aside from the threat of unauthorized external users accessing the system, risks are associated with insider misuse or fraudulent activity by collusion that could result in record theft, data alteration, data removal, or inappropriate creation of bogus records. Appropriate measures must be taken to ensure the integrity and security of records maintained by the DMV.

Facial Recognition Program Authorization

Specific statutory or regulatory authority differs in each jurisdiction. Jurisdictions may have specific or implied authority for the use of FR technology, but others may have specific prohibitions against its use or sharing of images.

Before the implementation of FR technology, a thorough review of jurisdictional regulations and statutes is recommended. Jurisdictions with a prohibition should consider amending current language to provide the needed authorization. Gaining legislative and public support is paramount to the implementation and successful continuation of an FR program. Trust in the validity of the FR program, quality image enrollment, stringent FR search parameters, and controlled information release practices will enhance an FR program’s chance of support, success, and continued growth. Deviation from these protocols invites speculation, suspicion, and the perception of misuse.

“Bio” indicates biographic data (e.g., name, date of birth, address).

“Photo” indicates photograph data.

“Match” indicates knowledge that two different records are linked to the same person.

“1:1 Biographic” indicates a lookup of specific records by unique name or identification number.

“1:N Biographic” indicates a query using partial biographic information.

“1:1 Photo” indicates verification of a photo against a stored photo for a specific, uniquely identified record.

“1:N Photo” indicates a biometric search against a large number of stored records.
A successful approach to combating threats includes a layered security strategy, which should address both physical and logical threats. Advances in technologies used for intrusions necessitate a careful and well-thought-out design of each system component. Effective measures to protect against information security threats should be planned in advance. Security design considerations should be inherent in components that house PII data because these contain the most sensitive and valuable data.

**Security Standards and Guidelines**

The NIST sets security standards for most U.S. government agencies. NIST publications include both Federal Information Processing Standards (FIPS) and guidelines, known as Special Publications (SPs). These documents are publicly available and may be useful to DMVs in developing their security and access control policies and procedures.

Examples of NIST security standards include the following:

- **FIPS 200**, *Minimum Security Requirements for Federal Information and Information Systems*
- **FIPS 199**, *Standards for Security Categorization of Federal Information and Information Systems*
- **FIPS 197**, *Advanced Encryption Standard (AES)*
- **FIPS 191**, *Guideline for The Analysis of Local Area Network Security*
- **FIPS 190**, *Guideline for the Use of Advanced Authentication Technology Alternatives*

Special Publications from NIST include:

- **SP 800-130**, *A Framework for Designing Cryptographic Key Management Systems*
- **SP 800-128**, *Guide for Security-Focused Configuration Management of Information Systems*

- **SP 800-127**, *Guide to Securing WiMAX Wireless Communications*
- **SP 800-125**, *Guide to Security for Full Virtualization Technologies*
- **SP 800-124**, *Guidelines for Managing and Securing Mobile Devices in the Enterprise*
- **SP 800-115**, *Technical Guide to Information Security Testing and Assessment*
- **SP 800-97**, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*
- **SP 800-77**, *Guide to IPsec VPNs*

The International Organization for Standardization (ISO) has published ISO/IEC 24745, an international standard that provides guidance for the protection of biometric information under various requirements for confidentiality, integrity, and renewability and revocability during storage and transfer. The standard also provides requirements and guidelines for the secure and privacy-compliant management and processing of biometric information. This standard addresses:

The AAMVA’s Digital Image Access and Exchange (DIA) program, currently used by 23 jurisdictions, has provided the groundwork for improved customer service and support, enhanced public safety and security and has provided a mechanism for further reducing the incidence of driver’s license fraud. The DIA provides an opportunity for jurisdictions to electronically transfer driver’s license images from one jurisdiction to another for comparison purposes using FR. Jurisdictions gain value in their fight against fraud by possessing this capability. The continued use and expansion of DIA to additional jurisdictions will further enhance the value of FR technology.
Analysis of the threats to and countermeasures inherent in a biometric and biometric system application models

Security requirements for secure binding between a biometric reference and an identity reference

Biometric system application models with different scenarios for the storage of biometric references and comparison

Guidance on the protection of an individual’s privacy during the processing of biometric information

ISO/IEC 24745 can be purchased from the ISO’s website at www.iso.org.

Jurisdictions should follow appropriate Information Security and Information Assurance standards such as:

- Security and Privacy Controls for Federal Information Systems and Organizations: NIST SP 800-53
- FBI Criminal Justice Information Services (CJIS) Security Policy (CJISD-ITS-DOC-08140-5.1) provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI data.
Stakeholders should be identified early in the preplanning stages and encouraged to participate in the development of laws, policies, and procedures. Their involvement guarantees a voice to express their interest and concerns. Identifying the correct stakeholders can prevent unforeseen pitfalls and provide for a much better end product. Stakeholders with a legitimate interest in the responsible use of FR technology and the safeguarding of citizens’ privacy will guarantee the balance for this technology to flourish.

Collaboration and Partnerships

Facial recognition technology provides the opportunity to maximize the integrity of the credential issuance process and to provide protection to citizens from fraudulent criminal actions. Another use of FR technology within a jurisdiction to be considered is its use in assisting law enforcement partners.

Expanding partnerships with other agencies enhances investigative success and expands the ability to identify individuals who in the past may have been unknown. Partnership is about working together and sharing resources. This can only be accomplished through established policies, mutual understanding of use, and continuous communication. Sharing fraud results between stakeholders provides valuable information to all involved often resulting in identification of fraud that may otherwise go undetected. Partnerships should be developed with stakeholders within the jurisdiction, as well as cross-jurisdictionally.

It is recommended that any FR system implemented within a jurisdiction have the capability to perform searches of the image database at the request of a system user. The recommended searches include the ability to use an existing image on the database or to introduce an image from an outside source to search for possible matches. Searches may be performed by DMV staff, or access to the system may be granted to law enforcement agencies. These actions enhance the jurisdiction’s ability to locate and investigate potential fraud and provide an opportunity to assist law enforcement partners with their existing investigative processes.

Examples of Successful Jurisdictional Partnerships

The Nebraska DMV entered into a partnership with the Nebraska Commission on Law Enforcement and Criminal Justice to share facial images. The law enforcement agencies provide images of their jail booking photos, which are loaded into the DMV’s FR system. Comparisons with these images are completed on a daily basis. Matches are investigated by either the DMV or the law enforcement agency, depending on the circumstance. Authorized law enforcement agencies are able to access the FR database for criminal investigation purposes. As a result of these partnerships, fraud is detected on a daily basis.

The Washington Department of Licensing (DOL) and the Washington State Patrol (WSP) formed a partnership for investigating of potential FR matches. Before the partnership, the DOL, having no sworn investigators, was limited to taking administrative actions against individuals with multiple identities. The agencies realized that without conducting criminal investigations and pursuing prosecution, offending individuals could continue their fraudulent practices in other jurisdictions. The WSP offered investigative assistance, which has led to numerous investigations, arrests, and prosecutions.
An Example of a Successful Cross-Jurisdictional Partnership

The Interstate Fraud Prevention Initiative, a CDL pilot project between the New Jersey Motor Vehicle Commission and the New York Division of Motor Vehicles, was implemented to identify individuals who held CDLs in more than one jurisdiction. The project provided for an interstate sharing of CDL data and images to complete an FR-driven interstate scrub. Both jurisdictions uncovered clear cases of identity-related crime and cases of individuals who had a suspended CDL in one state and procured a valid CDL in the other state under fraudulent circumstances. The actual numbers, percentages, and the extrapolated degree of the problem are still being analyzed. The initiative provided proof that interjurisdiction license and identity fraud exists and that FR technology is an effective tool for detecting fraud.

To learn more about jurisdiction’s successes with FR programs, please see Chapter 9.

Public Education and Outreach

Open and transparent communication is necessary for a jurisdiction to gain not only acceptance but also confidence that the program has been established to protect both individuals and the public. Outreach and education is an important and effective method for constructively influencing public perception on a jurisdiction’s use of an FR program. A positive public perception is essential in the continued use, growth, and understanding of the true nature and benefit of an FR program. There are two public outreach approaches to consider when implementing an FR program: a high-profile, proactive campaign or a lower profile approach.

A high-profile campaign is the proactive sharing of information about how the program works, benefits, timelines, and other pertinent information. When using this approach, communication should be released when the program is implemented.
and throughout the life of the program. A low-profile campaign is more passive and is mostly reactionary through responses to media and public inquiries. Even when a low-profile campaign is used, communications with stakeholders remain important.

Messaging should focus on the positive facts such as that FR is essential in verifying identity and ensuring people are who they claim to be. This technology prevents people from defrauding DMVs and protects the identities of law-abiding citizens. FR technology protects innocent citizens from having their identities used by others for DL/ID purposes. Without this technology the public is more vulnerable because criminals can potentially visit as many different DMV offices as they wish and obtain DL/IDs under different identities in the same state. FR provides the government an additional identity protection tool for safeguarding citizens’ personal information.

Communications Strategy
A carefully thought-out communications strategy will ensure that outreach goals are achieved. A key decision is to determine whether you are going to pursue a high- or low-profile communications approach. This decision will provide the foundation for building a strategy that should include objectives, key messages, target groups, potential issues and mitigation preparation, tactics and rollout plan, budget, resources and roles, and evaluation approach. When attempting to initially reach a broad audience in an unsolicited manner, consider professional assistance.

Periodic publication of success stories will strengthen program credibility with the public and show progress throughout the program’s life and can help agencies educate, promote, and garner support. Achievements and success during the early development stages reinforce the benefits to the public of this technology and provide information to stakeholders. Key factors to consider when selecting a success story are the audience, timing, and goal. When selecting a story, consider whether it illustrates the problem and highlights the solution the program provides. If properly promoted, success stories can also deter criminals.

Stakeholder Communications
A communication plan should be developed to educate stakeholders. The plan should be tailored for the audience. For example, when presenting to prosecutors, include a demonstration of the FR platform, presenting the steps an investigator follows with image collection, dataset query, image gallery development, and subject selection and identity. In this example, the objective is for prosecutors to obtain an understanding of FR technology and how it is used as an investigative tool.

The success of an FR program depends on the ability to assure individuals that their personal information is secure and used only for lawful purposes.

Stakeholders
Successful FR programs are built by identifying and engaging stakeholders. Examples of FR stakeholders include:

- Governors and ministers
- Legislators
- Agency directors
- State, local, and federal law enforcement agencies
- Correctional institutions
- Prosecutors
myths about FR and educate communities of interest of the benefits of using FR to deter and detect fraud. Delivering an effective outreach and education program will educate, engage, and enable stakeholders to understand how the FR program contributes to the integrity of the credential issuance process.

- Judiciary: attorney general, public defender’s offices, presiding judges and magistrates
- Entitlement, public health, and benefit-oriented agencies

Openly sharing information provides transparency and builds trust. It is important to continually dispel
Facial recognition programs provide a number of benefits. The following stories are examples of experiences and successes with jurisdictional FR programs.

**Unknown Decedent Identified**

After a woman’s body, with no identification found on her person, was pulled from the river, police unsuccessfully attempted to identify her using fingerprints. With no apparently matching missing person’s records to assist them, police turned to the motor vehicle database’s FR technology to try to identify the deceased. An image of the deceased’s face was run through Alberta’s image repository, and a possible match surfaced. After extensive human analysis of specific parts of the face, information was passed along to the police, allowing the victim to be identified. Her family could then be located and notified without having to do a public appeal for assistance.

**Sibling Identity Theft Unveiled**

Mark Clayton Mahovlich, whose DL was cancelled in 2009, visited an Insurance Corporation of British Columbia office in February 2010 to apply for an identity card in the name of his brother Michael, who had lived in the United States for the previous 20 years. Mahovlich had a birth certificate and CareCard in his brother’s name but no photo ID. The use of FR allowed the identification and prevention of attempted fraud.

**Veterinarian Impostor Located**

The Delaware State Police’s License and Gaming Unit requested the DMV Fraud Unit assist in identifying an individual who was posing as a veterinarian for the horse racing tracks. His actions resulted in the deaths of a number of horses. A comparison of his image through the DMV’s FR system resulted in a match, which gave authorities the information necessary to locate and arrest the individual.

**Check Fraud Scheme Uncovered**

Twenty-four fraudulent DLs were found in a trashcan in Marion County, Florida, and turned in to the Ocala Police Department. The use of FR provided for the identification of the individuals whose images appeared on the documents. It was determined that the counterfeit DLs were used in a check fraud scheme.

**A Murderer in Hiding Caught**

John Robert Jones was convicted in 1974 of murdering a fellow soldier at Fort Dix, New Jersey. After three years in prison, Jones escaped and was on the run for more than 37 years under an assumed identity. He was listed as one of the Army’s top 15 most wanted fugitives. The U.S. Marshall’s Office submitted a photograph of Jones for comparison in the Florida DMV’s FR system. A match with an image on a DL that Jones had fraudulently acquired in 1981 was returned. Jones was subsequently apprehended, and his fingerprints confirmed he was indeed the wanted fugitive.

**Forced Labor Traffickers Arrested**

The Kansas DMV’s FR system triggered an investigation that evolved into the largest forced labor-trafficking case in the United States and the first time the Racketeer Influenced and Corrupt
Organizations Act (RICO) was used in a human-trafficking case. Twelve defendants, including eight Uzbekistan nationals, were charged with crimes that included aggravated identity theft, money laundering, forced labor trafficking, mail fraud, visa fraud, and harboring illegal aliens. Members of the criminal enterprise used the identities of foreign nationals getting ready to depart the United States to apply for DLs. They used the assumed identities to register and fraudulently operate businesses across the United States. The businesses established under the assumed identities enabled the criminal enterprise to defraud multiple federal agencies by arranging for foreign workers to enter the United States under false pretenses and overstay their visas. The fraudulently obtained DLs allowed members of the criminal enterprise to conceal their true identity and proceeds of their illicit activities. The ring leader and several of his conspirators were eventually identified by the Kansas DMV’s FR software after the individuals returned to the DL office to apply for licenses under their true identities. The initial FR matches allowed investigators to link the criminal enterprise to their true identities, which ultimately led to criminal convictions.

**Social Service Assistance Rendered**

Orange County Deputies were called to a scene involving a woman with a mental condition. The woman was in need of medical treatment and was unable to provide the deputies with her identity. Her image was entered into an FR program, and she was identified. With her identification, medical records were located, and she received the appropriate medical treatment.

**Social Media Aids in Identification**

Pinellas County Sheriff’s Office Detectives were attempting to identify an unknown woman involved in prostitution by using social media sites. Detectives were able to capture an image from the woman’s website and enter it into the agency’s FR program. An image query and subsequent developed image gallery proved successful when queried against the mug shot dataset, and identification was made.

**Benefit and Bankruptcy Fraud Detected**

Angela Richardson, previously known as Angela Williams, was convicted after having her dual identity scheme uncovered through the use of FR in the credential issuing process. The investigation found that Williams applied for a new Social Security number, alleging she was the victim of fraud, which allowed her to create a second identity using her married name and the new Social Security number in the DMV database. She continued to renew both licenses for a number of years until Nebraska’s implementation of FR. Richardson, a homeowner who was employed full time, applied for and received thousands of benefit dollars as an unemployed mother, including rental assistance. In addition, she filed bankruptcy twice within a five-year period using the dual identities, allowing her to forego thousands of dollars of debt. Richardson was sentenced to five years’ probation and ordered to pay $16,255 restitution.

**School Bus Driver with Narcotics Conviction Arrested**

A New York City school bus driver, who had been previously deported after a narcotics conviction, was identified through the use of FR technology. The driver was licensed and working as a CDL school bus driver in New York State under one name, date of birth, and Social Security number. He also had a nondriver ID under another name and date of birth, which had multiple open suspensions for unpaid tickets, as well as narcotics convictions and suspensions of his DL privileges for narcotics transactions. The subject was arrested under multiple felony charges and is no longer operating a school bus.
Driver with Four Records and Multiple Suspensions Identified

Through the use of FR, a New York driver was identified and arrested on numerous felony charges for using multiple identities to obtain state issued credentials. The driver held a DL under one name, date of birth, and Social Security number and a second DL under another name and date of birth that had been revoked since 2003 for a driving while intoxicated (DWI) conviction. He also had a third DL under a different name and date of birth that was suspended for an unresolved DWI arrest and six unpaid moving violations fines. He had a fourth record with yet a different name and date of birth that was created for a court-ordered suspension after the subject was arrested. His records have been combined, and his DL privileges have been revoked.
Appendix A  Facial Recognition Survey Results

Following are the Facial Recognition questions asked in a recent AAMVA membership survey.

1. Do you have a facial recognition (FR) program? If so, when was the program implemented?

2. Did you complete a scrub of your data prior to full implementation?

3. What action do you take when it is determined through FR that a person has fraudulently applied for a driver license or ID card?

4. Who is your facial recognition vendor?

5. Do you use FR internally for anything other than credential issuance?

6. Do you share images or allow access to your FR database with other entities?

7. Do you require a specific number of identities before a criminal or administrative investigation is initiated?

8. Do you have an investigative unit within your agency? If yes, do you have fully sworn officers possessing powers of arrest? If no investigative unit, do you have an arrangement (formal or informal) with your state police/highway patrol to conduct criminal investigations?

Full survey results with detailed jurisdiction answers can be found in the American Association of Motor Vehicle Administrators knowledge bank at http://www.aamva.org/survey/web/knowledge-bank.aspx

The map on page 52 shows, at a glance, the jurisdictional adoption of FR.
Use of Facial Recognition Among AAMVA Jurisdictions

*Michigan State Police Use FR

Appendix A: Facial Recognition Survey Results
I. Authority – The Department is authorized to implement a facial recognition system for the protection and validation of identities associated with driver licenses, driving permits and identification cards issued by the Department.

II. System Capabilities – The facial recognition system administered by the Department:

a. Must be capable of highly-accurate facial recognition matching processes; and

b. Should comply with the most recent, applicable standards as established by the American Association of Motor Vehicle Administrators.

III. Limitations on Use –

a. The Department may utilize the facial recognition system in:

   i. Validating and protecting the identity of an applicant for, or current holder of, a driver license, driving permit, or identification card; or

   ii. Making determinations on whether an applicant or person has previously been issued a driver’s license, permit or identification card under a different identity; or

   iii. The investigation and/or prosecution of any driver license, driving permit or identification card related fraud

b. Results from the facial recognition system shall not be made available for public inspection or copying, but may be disclosed only:

   i. By court order;

   ii. To criminal justice agencies for the purposes of conducting criminal investigations, missing persons investigations, or identifying unidentified persons;

   iii. To a federal government agency (other than a criminal justice agency) if specifically authorized by law; or

   iv. To a federal, state or local government agency for use in carrying out its functions if it has been determined that the subject of the results has committed a prohibited practice or criminal offense as determined by state law. Such offenses shall include but not be limited to:

      1. Sale or delivery of a stolen driver license or identification card;

      2. Manufacture, sale, or delivery of a forged, fictitious, counterfeit, fraudulently altered or unlawfully issued driver license or identification card;
3. Manufacture, sale, or delivery of a blank driver license or identification card, except under the direction of the Department;

4. Display or possess any fictitious or fraudulently altered driver license or identification card;

5. Lending or knowingly permitting the use of one’s driver license or identification card to or by any other person;

6. Display or representing as one’s own any driver license or identification card not issued to oneself;

7. Willfully failing or refusing to surrender to the Department upon its lawful demand any driver license or identification card that has been suspended, revoked or canceled;

8. Use of a fictitious name in any application for a driver license or identification card or to knowingly make a false statement to conceal a material fact or otherwise commit a fraud in any such application; or

9. Permitting any unlawful use of a driver license or identification card issued to oneself; and

10. Any other driver license, driving permit or identification card related criminal offense(s).

IV. Notification of Use

a. Upon implementation of the facial recognition system, the Department shall provide notice of the facial recognition system in use. Notice shall include information on:

   i. A description of how the facial recognition system works;

   ii. Reasons the Department is employing the facial recognition system;

   iii. Ways in which the Department may use the results from the facial recognition system;

   iv. How an investigation could be conducted based on results from the facial recognition system; and

   v. A person’s right to appeal any licensing determinations made as a result of use of the facial recognition system.

b. The Department shall provide information on the facial recognition system by:

   i. Posting notices in driver licensing locations; and/or

   ii. Making general written information regarding the facial recognition system available to all applicants at driver licensing locations and on the Department’s Web site.

V. Data Storage and Security – The facial recognition system, including personal identifying information therein, must conform with the appropriate security safeguards as mandated by state law, regulation, and procedures.
MEMORANDUM OF UNDERSTANDING
between the
NEBRASKA DEPARTMENT OF CORRECTIONS
and the
NEBRASKA DEPARTMENT OF MOTOR VEHICLES

I. Parties
This Memorandum of Understanding (MOU) is an agreement between the Nebraska Department of Corrections (DCS), and the Nebraska Department of Motor Vehicles (DMV), hereinafter the Parties.

II. Purpose
This MOU is intended to enhance law enforcement and the working relationship between the DCS and the DMV Driver and Vehicle Records Division to assist those individuals who are victims of identity theft and for investigation of criminal activity using images and signatures stored in facial recognition system, hereinafter FRS. The purpose of this MOU is to specify the terms and conditions for DCS access of the FRS to carry out functions of DCS. The MOU will also document the agreed responsibilities and functions of the Parties with respect to enhancing the use of the DMV FRS photo repository by adding photographs from the DCS mug shot repository. Integrating DCS mug shots into FRS will enhance the DMV’s ability to ensure that the individuals presenting themselves to the DMV have not been previously identified as another person. Authorized employees of the DCS and the DMV will carry out the requirements of the MOU.

III. Legal Authority
The statutes provided for in this MOU include, but are not limited to, the following:

Nebraska Revised Statute § 60-484.02;
Nebraska Revised Statutes §60-2901 through 60-2912;
Title 18, U.S.C. Section 2721 (b)(1);

This MOU shall be interpreted to incorporate any amendments to the above statutes by the Nebraska Legislature as may be applicable during the term of the MOU.
IV. Implementation

A. DCS:

1. Agrees to restrict the access to the DMV FRS images to one employee of the DCS and to provide the DMV with the name, address, and contact information for this employee. Access to and use of images and signatures of individuals stored in DMV databases shall be used solely to carry out the purposes of this MOU as assigned by the DMV to DCS pursuant to the terms and conditions of this MOU. Any access, disclosure, or use of any image or signature for any other purpose beyond the terms and conditions of this MOU is prohibited and shall be considered a breach of the MOU.

2. Agrees to make no facial recognition comparison request except for a case being investigated and/or prosecuted in a criminal manner.

3. Understands that the FRS results provided by the DMV are to assist in furthering an ongoing investigation or criminal matter and cannot be used as the sole reason for arrest or action.

4. Agrees to adhere to the requirements of Neb. Rev. Stat. §60-484.02 and §60-2901 through 60-2912 and agrees that no employee, contractor, or agent of DCS shall allow disclosure of images and signatures except to federal, state or local law enforcement agencies or a certified law enforcement officer employed in an investigative position by a federal, state, or local agency for the purpose of carrying out the functions of the agency or assisting another agency in carrying out its functions or as otherwise may be authorized by action of the Nebraska Legislature.

5. Extract an initial historical file from their database of available photos. It will also implement a nightly extract and transmission process to provide new photos and relevant demographics to DMV for incorporation into the facial recognition database.

6. Agrees to enforce all applicable laws and security protocols for handling and processing of images and signatures accessed pursuant to this MOU to prevent any access, use, or disclosure other than as provided in this MOU.

B. DMV agrees to:

1. Provide one FRS user ID and password to be used to access images and signatures in the FRS for the sole use of the identified employee of DCS.

2. Provide DCS with access to FRS and the available DMV images and signatures subject to the conditions of this MOU.

3. Provide DCS with the names, addresses, and telephone numbers of contact persons within the DMV regarding any questions or problems which may arise in connection with the FRS.

4. Ensure that only authorized personnel will handle data provided by DCS.

5. Provide DCS training and assistance necessary to use FRS.
V. Privacy and Security

A. The information involved in the MOU may identify U.S. persons, whose information is protected by the Privacy Act of 1974. DCS will ensure that all such information will be handled lawfully. Conversely, DCS is assured that DMV will comply with all privacy and disclosure laws.

B. For purposes of this MOU, personally identifiable information (PII) is defined as information which can be used to distinguish or trace an individual’s identity, including any personal information which is linked to a specific individual. The parties will review and make appropriate changes, if any, to their privacy compliance documents, in advance of the implementation of this MOU to ensure that privacy risks are appropriately mitigated and the scope and routine uses of applicable system of records notices permit the collection, maintenance, and sharing of PII as set forth in this MOU. Each party that discloses PII is responsible for making reasonable efforts to ensure that the information disclosed is accurate, complete, timely, and relevant.

C. Each party shall be responsible for the safeguarding of any equipment used by it to access records and shall limit access to authorized users. Each party will immediately report to the other party each instance in which information received from the other party is used, disclosed, or accessed in an unauthorized manner.

D. DMV will ensure user account and authorities granted to the FRS are maintained in a current and secure status.

VI. Effective Date and Term of the MOU

This MOU is effective upon the date the authorized representatives of both parties have signed and will continue in effect until terminated.

VII. Modification.

This MOU may be modified in writing signed by the authorized representatives of both parties.

VIII. Costs

DMV and DCS will each be responsible for costs incurred by the respective agency in furtherance of this MOU.

IX. Termination

This MOU may be terminated by either party upon 30 days prior written notice to the other party. DMV may terminate this MOU without prior notice if deemed necessary because of a requirement of law or policy, upon a determination by DMV that there has been a breach of this MOU, upon a determination by DMV that there has been a breach of system integrity or security by DCS, upon a failure by DCS to comply with established procedures or legal requirements, or for reasons of government necessity.

Nothing in this MOU is intended, or should be construed, to create any right or benefit, substantive or procedural, enforceable at law by any third party against the State of Nebraska, its agencies, officers, or employees or against DMV or DCS or employees or officers of DMV or DCS.

The foregoing constitutes the full agreement on this subject between the DCS and the DMV.

The undersigned represent that they are authorized to enter into this MOU on behalf of the DCS and the DMV, respectively.
Nebraska uses this form in instances when a law enforcement agency has not signed an MOU with the DMV and is requesting an FR comparison be completed.

### Appendix D  Sample Application for Requesting a Facial Recognition Comparison

<table>
<thead>
<tr>
<th><strong>APPLICATION FOR RELEASE OF DIGITAL IMAGE/SIGNATURE</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LAW ENFORCEMENT USE ONLY</strong></td>
</tr>
</tbody>
</table>

If filing this request in person, be prepared to furnish us with proof of identification. If filing this request through the mail or by fax, your signature must be notarized or the request will be returned to you unprocessed.

No officer, employee, agent, or contractor of the Department of Motor Vehicles or law enforcement officer will release a digital image or a digital signature unless the requestor is one of the following (please indicate the applicable exemption):

- a federal, state, local law enforcement agency,
- a certified law enforcement officer employed in an investigative position by a local, state or federal agency,
- a driver licensing agency of another state for the purpose of carrying out the functions of the agency upon the verification of the identity of the person requesting the release of the information and the verification of the purpose of the requestor in requesting the release.

Any requestor that knowingly discloses or permits disclosure of a digital image or digital signature will be guilty of a Class 1 misdemeanor and will be, at the discretion of the appropriate official, removed from office or discharged.

**FORM MUST BE COMPLETED IN FULL**

<table>
<thead>
<tr>
<th><strong>PLEASE PRINT</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name (as it appears on driver’s license):</strong></td>
</tr>
<tr>
<td><strong>Date of Birth: ___________________ Nebraska Driver’s License Number ___________________</strong></td>
</tr>
</tbody>
</table>

**Name and Date of Birth OR Name and Nebraska Driver’s license Number must be supplied before a record check can be done.**

<table>
<thead>
<tr>
<th><strong>Please Print Your Name:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Agency Name:</strong></td>
</tr>
<tr>
<td><strong>Address:</strong></td>
</tr>
<tr>
<td><strong>City, State, Zip:</strong></td>
</tr>
<tr>
<td><strong>Phone Number ( ) Email:</strong></td>
</tr>
</tbody>
</table>

Under penalty of law, the undersigned certifies that the information requested will be used as authorized by the Uniform Motor Vehicle Records Disclosure Act. The undersigned hereby acknowledges that this request is made with the understanding that any person requesting disclosure of sensitive personal information to the Department of Motor Vehicles who misrepresents his or her identity, misrepresents the purpose for which the information requested will be used, or otherwise makes a false statement on the application shall be guilty of a Class I misdemeanor.

| **Signature:** ___________________ **Date:** ___________________ |

(Signature must be notarized below if filing this request through the mail or by fax.)

| **State of: ___________________ **County of: ___________________** |

The foregoing signature of the requestor was acknowledged before me this _______ day of __________

<table>
<thead>
<tr>
<th><strong>Notary or Designated County Official</strong></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Submit this application to:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Nebraska Department of Motor Vehicles</td>
</tr>
<tr>
<td>Driver and Vehicle Records Division</td>
</tr>
<tr>
<td>301 Centennial Mall South</td>
</tr>
<tr>
<td>PO Box 94789</td>
</tr>
<tr>
<td>Lincoln, NE 68509-4789</td>
</tr>
<tr>
<td>(402) 471-3918</td>
</tr>
<tr>
<td>Fax: (402) 471-8694</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>DMV Use Only</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Date:</strong> ___________________</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Employee Releasing Image/Signature</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Supervisor Approval</strong></td>
</tr>
</tbody>
</table>

*Revised 6/2011*
Appendix E  Working Group Roster

CHAIR

Mr. George Theobald
Director, Program Management Office
Georgia Department of Driver Services
2206 East View Parkway
Conyers, GA 30013
(678) 413-8876 | gtheobald@dds.ga.gov

VICE CHAIR

Ms. Betty Johnson
Administrator
Nebraska Department of Motor Vehicles
Department of Motor Vehicles
P.O. Box 94789
Lincoln, NE 68509-4789
(402) 471-3909 | betty.johnson@nebraska.gov

MEMBERS

Ms. Catherine Brooks
Project Manager, Fraud Prevention and Business Integrity Office
Ontario Ministry of Transportation
1201 Wilson Avenue
Downsview, ON M3M 1J8
(416) 235-3877 | catherine.brooks@ontario.ca

Mr. Gord Bryant
Coordinator, Document Verification & Facial Recognition
Service Alberta
Special Investigations Unit
810-600 6 Avenue SW
Calgary, AB T2P 0S5
(403) 355-4885 | gord.bryant@gov.ab.ca

Mr. Dave Coleman
Director
IBG, A Novetta Solutions Company
7921 Jones Branch Drive
McLean, VA 22102
(571) 282-3000 | dcoleman@novetta.com

Mr. Thomas Flarity
Director of Security and Investigations
New Jersey Motor Vehicle Commission
225 East State Street—6 East
Trenton, NJ 08666
(609) 984-5279 | thomas.flarity@dot.state.nj.us

Ms. Sydney Roberts
Chief Deputy Director, Department of Police
Illinois Office of the Secretary of State
110 East Adams Street
Springfield, IL 62701
(217) 785-0846 | sroberts@ilsos.net

Ms. JoAnna Shanafelt
Investigator III/Acting Administrator
Washington Department of Licensing
1125 Washington Street, SE
P.O. Box 9020
Olympia, WA 98501
(360) 902-3715 | jshanafelt@dol.wa.gov

Mr. Kenneth Shock
Chief of Fraud Unit
Delaware Division of Motor Vehicles
P.O. Box 698
Dover, DE 19903
(302) 744-2544 | kenneth.shock@state.de.us
Major Sean Jowell  
Pinellas County Sheriff’s Office  
Support Services  
14400 49th Street, N  
Clearwater FL 33762  
(727) 582-6248 | sjowell@pcsonet.com

Major Ryan Burchnell (and Major Steve Williams)*  
Chief Technology Officer  
Florida Department of Highway Safety & Motor Vehicles  
2900 Apalachee Parkway, MS22  
Room A418H  
Tallahassee, FL 32399-0514  
(850) 617-2391 | ryanburchnell@flhsmv.gov  
* Major Williams retired midproject and was replaced by Major Burchnell.

TECHNICAL ADVISORS

Mr. John Drago  
Chief Inspector  
U.S. Department of Justice  
P.O. Box 745  
New York, NY 10008  
(212) 791-9089 | John.Drago@usdoj.gov

Ms. Trudy Ford  
Supervisory Management and Program Specialist  
Federal Bureau of Investigation  
FACE Services Unit  
1000 Custer Hollow Road  
Clarksburg, WV 26306  
(304) 625-4760 | trudy.ford@ic.fbi.gov

Mr. Walter Hamilton  
Senior Consultant  
Identification Technology Partners, Inc.  
3235 Bluff Blvd.  
Holiday, FL 34691  
(727) 938-2704 | whamilton@idtp.com

Mr. Mike Neumann  
Solutions Manager  
Gemalto  
9442 Capital of Texas Highway North  
Building 2, Suite 400  
Austin, TX 78759  
(512) 257-3926 | mike.neumann@gemalto.com

Mr. Kevin O’Leary  
Senior Product Manager  
MorphoTrust USA, a Safran Group company  
296 Concord Road  
Billerica, MA 01821-0000  
(508) 423-6945 | koleary@morphotrust.com

Mr. Douglas Sprouse  
Management and Program Analyst  
Federal Bureau of Investigation  
FACE Services Unit  
1000 Custer Hollow Road  
Clarksburg, WV 26306  
(304) 625-2111 | douglas.sprouse@ic.fbi.gov

STAFF LIAISONS

Mr. Brian Ursino  
Director, Law Enforcement  
American Association of Motor Vehicle Administrators  
P. O. Box 16629  
Seattle, WA 98116  
(703) 350-5103 | bursino@aamva.org

Mr. Geoffrey Slagle  
Director, Identity Management  
American Association of Motor Vehicle Administrators  
4301 Wilson Boulevard  
Suite 400  
Arlington, VA 22203-0000  
(703) 342-7459 | gslack@aamva.org

Ms. Sheila Prior  
Regional Director, Regions III & IV  
American Association of Motor Vehicle Administrators  
10800 North 101 Street  
Scottsdale, AZ 85260  
(480) 275-4584 | sprior@aamva.org