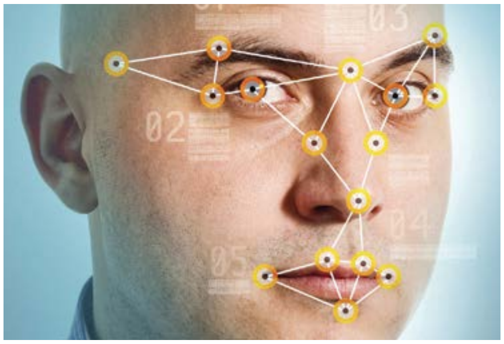
AAMVA

American Association of
Motor Vehicle Administrators



Facial Recognition Program
Best Practices

Edition 2

December 2019

DRIVER STANDING COMMITTEE & LAW ENFORCEMENT STANDING COMMITTEE
FACIAL RECOGNITION WORKING GROUP

Cover photo credits: ©Thinkstockphotos.com (“Face Detection” by stevanovicigor, “Eye with binary code” by Vladimir Arndt/iStock, and “Profile with Code” by Dimitris Kolyris)

Contents

Executive Summary

AAMVA originally published a *Facial Recognition Best Practices Guide* in 2015.The Law Enforcement Standing Committee recommended, and the AAMVA Board approved, a 2019 Facial Recognition Working Group (hereinafter referred to as the *Working Group*) to update the Guide to ensure the content and recommended best practices were based on the most up-to-date information.

Customer privacy and the protection of personal information is paramount and should be consistent with the laws of the jurisdiction. Although biometric matching itself raises privacy concerns for some, the use of the technology actually helps protect people's privacy and personal identities. Moreover, it is a basic tenet that potential matches from Facial Recognition should generate human examination and no other action, such as an arrest or corrective action, should be taken solely on the basis of a FR result.

It is a basic tenet that potential matches from Facial Recognition should generate human examination and no other action, such as an arrest or corrective action, should be taken solely on the basis of a FR result.

Identity fraud and identity theft are continuing problems. According to the 2018 Javelin Strategy & Research Identity Fraud Study, the number of identity fraud victims increased to 15.4 million U.S. consumers, costing $16.8 Billion in 2017. Unfortunately, a portion of identity fraud and theft begins, or is continued, through the credential issuing authority of each jurisdiction (this term is used throughout the document because not all issuing agencies are known by "Department of Motor Vehicles" or "DMV").

When Indiana DMV first started using FR, the state found a resident with 146 different identities. This individual was running a check-kiting scheme across multiple states. Indiana worked with law enforcement to determine what the individual's true identity was, and they were able to locate and arrest him in Nebraska.

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. Chapter One contains a map depicting FR use in North America. 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 use by the credential issuing authority 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. Even in cases when a fraudster had previous success obtaining a fraudulent credential, FR improves the credential issuing authority's ability to detect that fraud through image comparison analysis and investigation, often leading to arrest.

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

The importance of gaining stakeholder support for an FR program cannot be overemphasized. Two recent surveys indicated the majority of the public approves of appropriate FR use by government agencies (Brookings Institute, September 2018; Center for Data Innovation, January 2019).

This document was written for all credential issuing authorities, whether or not they currently use 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 programs are 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 A.

New Jersey conducted a multistate Commercial Driver License (CDL)/Facial Recognition pilot with New York and identified a CDL driver who had his CDL revoked for four DWI convictions. The subject had purchased a new identity from an individual incarcerated in Puerto Rico and used it to obtain a valid CDL in New York. When an arrest warrant was obtained, it was found that the same false identity was used to obtain Class D DLs in the States of Florida, Connecticut, and Massachusetts. The subject was arrested and charged with multiple felonies.

The Kansas Department of Motor Vehicles' (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.

After providing an overview of FR, this document provides chapters on technology; program development and enhancement; operations; training; privacy; access and sharing of images; stakeholders, collaboration, and outreach; and success stories. FR programs should include a strong privacy component and are best developed in consultation with general counsel to address privacy, access, and use.

This document contains a total of 12 Best Practice recommendations throughout the aforementioned chapters.

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 within the parameters of strictly controlled access.

To continue and increase public acceptance, strategic communication and outreach sharing 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.

Terms and Definitions

Algorithm A facial recognition algorithm is an equation created from the combination of measurements from key points on the face.

Biometric Match A determination that two samples correspond to the same source based on some level of computer-evaluated similarity. Does not inherently imply that the probe and candidate are the same person.

Biometric Template When an image of a person's face is turned into a digital record through a (usually a commercial secret and proprietary) process of biometric feature extraction that will be used for comparison.

Biometrics A physiological or behavioral characteristic that attempts to uniquely identify an individual.

Cleanse (also *Deduplication* and *Scrub*) A quality assurance and fraud detection process undertaken to identify duplicate information in a biometric system. This is achieved when images are biometrically matched against every other typically in conjunction with biographical and other data, and a matching threshold is used to identify duplicates.

Comparison The observation of two or more faces to determine the existence of discrepancies, dissimilarities, or similarities.

Credential A driver's license, identification card, permit, or other identity document issued by an issuing authority.

Enhance In the context of facial identification, a tool, technique or process of improving the visibility of facial detail to assist searching and comparison of faces. Best practice is to preserve originals and follow a non-destructive process, noting all steps.

Enroll The act of capturing a facial image, creating a template, and entering the template into a facial recognition gallery.

Evaluation Ascertaining the value of dissimilarities and similarities between two facial images.

Examiner An individual who has received training in the face recognition system and its features.

Face Recognition (FR)
In automated systems: The automated searching of a facial image in a biometric database (one-to-many, 1:N), typically resulting in a group of facial images ranked by computer-evaluated similarity.
By humans: The mental process by which an observer identifies a person as being one she or he has seen before.

Facial Identification (FI) The manual examination of the differences and similarities between two facial images or a live subject and a facial image (one-to-one, 1:1, one-to-record, 1:R) for the purpose of determining if they represent the same person.

Facial Image Electronic image–based representation of the portrait of a person.

False Positive When one or more candidates are not matches with the probe. Examples include twins or people that look similar to the probe.

Feature Extraction 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.

Gallery A repository of enrolled images within the facial recognition database that supports separation of driver license/identity credential faces from other enrolled images (e.g., watch list, unknown individuals, department of corrections) Galleries enable data separation between agencies and daily screening operations.

Identity Within a biometric system, the collective set of biographic data, images, and templates assigned to one person.

Image (Portrait) Photograph of a person which includes the full head, with all hair in most cases, as well as the neck and the tops of the shoulders.

Leads (also known as *Candidates*) An automated list of possible matches governed by a threshold within an image database.

Match Score An automated score indicating the similarity between two or more images or templates.

Matching The process of comparing a probe facial template with a previously stored template.

No Match A negative result from a face recognition search in which the probe image was determined not to be sufficiently similar to or resemble any of the reference image or image templates contained in an image repository.

One-to-Many (1:N) Face Image Comparison The process whereby a probe image from one subject is compared with the features of reference images contained in an image repository, generally resulting in a list of the most likely candidate images.

One-to-One (1:1) Face Image Comparison The process whereby a probe image from one subject is compared with a most likely candidate image that is also from one subject. See *Comparison*.

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

Personally Identifiable Information (PII) 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, biometric records, and any other information that is linked or linkable to an individual.

Pose The orientation of the face with respect to the camera. Common poses are frontal and profile.

Probe The facial image or template searched against the gallery in a facial recognition system.

Resolution The act, process, or capability of distinguishing between two separate but adjacent elements of detail in an image. Resolution normally has three components: spatial (e.g., pixels per inch), spectral (e.g., number of colors), and radiometric (e.g., number of shades).

System Bias (1) Errors repeatedly introduced through automation (e.g., errors in template generation or comparison). (2) Errors repeatedly introduced through operational practices in an organization or unit (e.g., improper lighting or camera position guidance).

Template A set of biometric measurement data prepared by a facial recognition system from a facial image.

Threshold A match score where a decision boundary exists, typically being a specific known value in a biometric system.

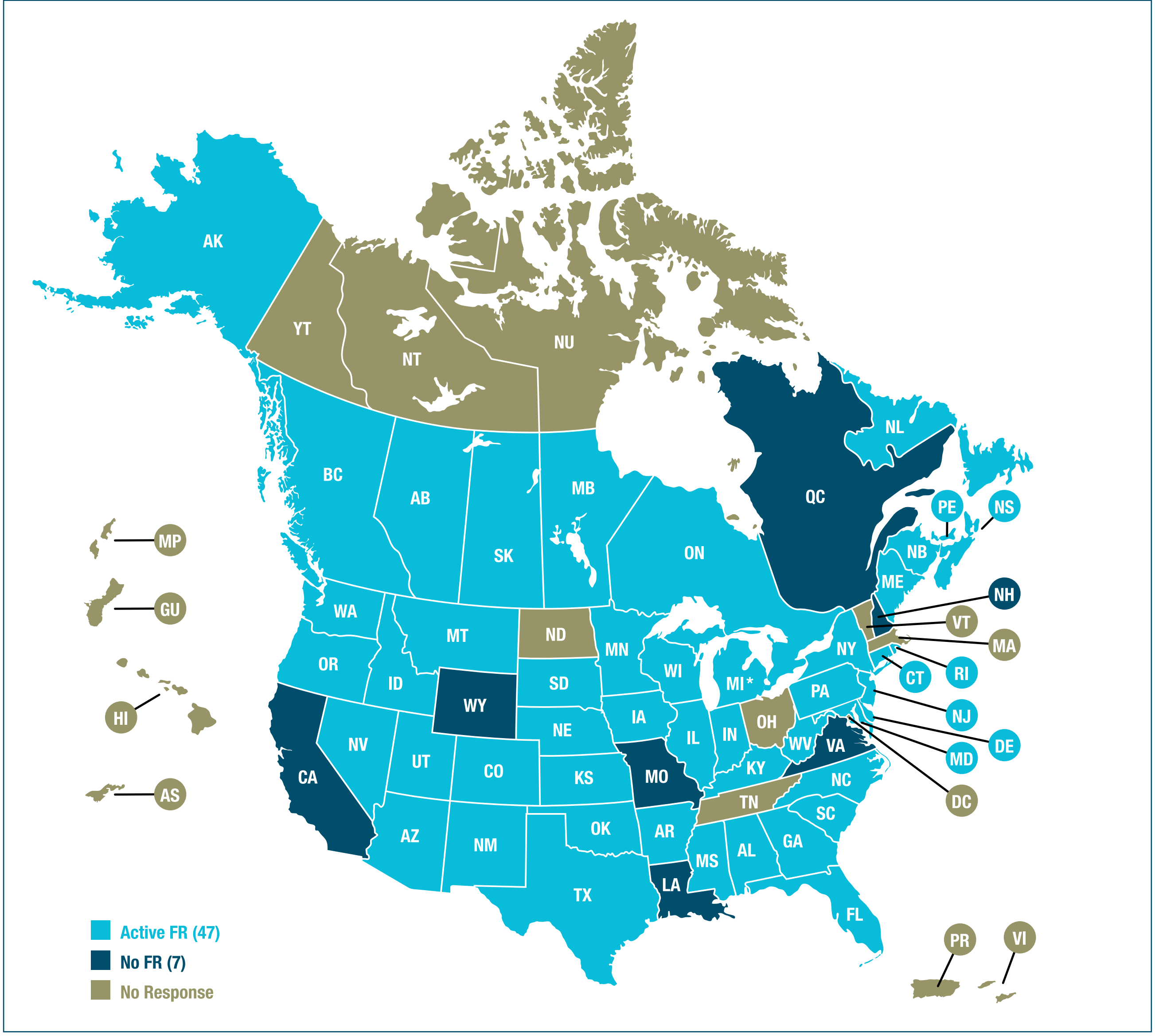
Watch List In the context of facial identification, a selection of persons enrolled in a facial recognition system that allows a probe to be matched against only a selection of the overall system face holdings.

Chapter 1 An Overview of Facial Recognition

Facial recognition (FR) is a fraud prevention, fraud detection, business integrity, and risk mitigation tool used by the majority of U.S. and Canadian credential issuing authorities. 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, which may trigger intervention by an examiner to investigate the possibility.

The Working Group conducted a survey in which 54 of 69 AAMVA jurisdictions replied either through direct reply or telephone follow-up (78% response rate). Of the 54 respondents, 47 reported

Use of Facial Recognition Among AAMVA Jurisdictions



implementing some form of FR technology in their credential issuing agency.

1.1 How the Technology Works

What is Facial Recognition?

A facial recognition system is a technology capable of identifying or verifying a person's identity from a digital image or a video frame by converting the image to a template. The template is then compared with other templated images. Facial recognition is also described as a biometric artificial intelligence (AI) based application that can assist in identifying a person.

In the context of credential issuing authorities, facial recognition is composed of web-based applications, business workflows, and biometric search engine technology aligned with daily credential issuance processes. In addition, the technology aids government agencies with investigating potential fraud and resolving ongoing cases.

1.2 The Business Case for Using Facial Recognition

A core responsibility of the credential issuing authority is to ensure that each 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 genuine (frequently stolen) or counterfeit breeder documents to obtain a genuine credential or other document that contains false information. *Identity theft* occurs when someone uses the personal identifying information of another individual. According to the Federal Trade Commission, identity theft is a leading consumer crime in the United States, costing consumers billions of dollars in a single year.

Facial recognition assists credential issuing authorities in identifying suspicious activities, including:

1. An individual holding more than one credential under different names (identity fraud or multiple fictitious identities)
2. Different individuals holding a common identity and credential number (identity theft)
3. Clerical or data errors, such as attaching a photo to the wrong driver record
4. Patterns of clerical error that may indicate collusion or internal fraud

Internal Fraud

Depending on the FR system capabilities, some jurisdictions are able to detect not only the individuals committing the fraud but also the office and operators who processed their transactions. If an issuing authority 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 its transactions to determine whether there is a concern that requires further review.

For more detailed information on fighting fraud, see the American Association of Motor Vehicle Administrators' Best Practices for the Deterrence and Detection of Fraud*, March 2015.*

Clerical and Systematic Errors

A clerical error is the inadvertent creation of two or more records for the same person. FR helps identify when multiple records are created in error. It also identifies when the wrong image is captured on a new or existing record. FR functionality can be used to detect offices and operators who process a high number of errors and enhances overall system integrity.

Systematic problems can occur when an image is applied to the wrong record. For example, when data migration occurs, a photo could be applied to an incorrect record.

1.3 Benefits of Using a Facial Recognition System

Benefits include, but are not limited to, improving highway safety, reducing benefit fraud, and reducing financial fraud activities. FR also helps communities recover after natural disasters and provides invaluable assistance to law enforcement.

Highway Safety

The primary purpose of a driver's license credential is to verify that an individual has met the requirements to drive legally and safely. One intended use of an FR system is to prevent individuals who lose their driving privileges from committing fraud to obtain another driver's license credential in order to continue driving.

To illustrate the correlation between individuals holding multiple records and highway safety, the New York State (NYS) Department of Motor Vehicles conducted an evaluation of the driving records for everyone identified with multiple licenses via facial recognition. The results from the analyses of 2018 data supports the findings from the 2012 analyses, indicating that drivers with multiple license records pose a serious traffic safety risk. In 2018, of the more than 9,200 cases involving drivers with multiple license records:

- 52% had no valid license associated with any of their multiple records.
- 21% had been convicted of unlicensed operation compared with 8% of all NYS licensed drivers.
- 4% had been convicted of impaired driving compared with 2% of all NYS licensed drivers.
- 15% had been convicted of a cell phone violation compared with 9% of all NYS licensed drivers.
- 29% had been convicted of a seat belt violation compared with 21% of all NYS licensed drivers.
- 26% had accumulated six or more points on their license record within an 18-month period compared with 11% of all NYS licensed drivers.

In 2018, of the more than 9,200 cases involving drivers with multiple license records, 52% had no valid license associated with any of their multiple records.

As illustrated by the NYS example, FR programs can provide an important tool for 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.

Reducing Benefits or Financial Fraud

Benefit fraud is the willful misrepresentation of a material fact on a petition or application to gain a benefit. A fraudster who obtains a credential in a false identity now possesses a document that may be used to obtain benefits he or she is not entitled to.

Similar to benefits fraud, financial fraud involves the use of a false identity to commit fraudulent financial transactions. Common victims of financial fraud activities include banks, retail stores, and insurance companies.

According to the 2018 Javelin Strategy & Research Identity Fraud Study, the number of identity fraud victims increased to 15.4 million U.S. consumers, costing $16.8 billion in 2017.

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.

Several jurisdictions are using FR to quickly identify and verify identities for individuals involved in natural disasters who have lost their original identification and breeder documents. FR greatly enhances the identification of victims of a disaster such as tornadoes, fires, and floods, 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.

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 credential issuing authorities FR systems, within the parameters set by legislation and agency policies and procedures. These systems may be used to aid in criminal investigations and other assistance activities such as helping to identify missing persons, find most-wanted persons, and combat human trafficking, to name a few.

> *Several jurisdictions are using FR to quickly identify and verify identities for individuals involved in natural disasters who have lost their original identification and breeder documents.*

The search of counterfeit document factories and labs frequently results in dozens, if not hundreds, of images of people who need to be identified to be notified of potential fraud against them. It is common for suspect images found on counterfeit identification to be run through a credential issuing authority's image database.

As provided by law, the Florida Department of Highway Safety and Motor Vehicles (HSMV) provides digital images in response to law enforcement agency requests. The Pinellas County Sherriff's Office (PCSO) in Florida, a leader in bringing FR technology into mainstream law enforcement use, receives HSMV images in accordance with a Memorandum of Understanding. In addition to receiving images from other sources, including the Department of Corrections and other law enforcement agencies, PCSO has equipped patrol vehicles with the equipment necessary to do on-the-spot FR verification and identification. What follows is a success story using PCSO's FR system as provided by PCSO: On February 11, 2019, an armed robbery occurred in Hillsborough County, Florida. During the robbery, a detailed suspect photograph was obtained by Hillsborough County Sheriff's Office (HCSO). HCSO sent out an alert requesting assistance in identifying the suspect. An FR query was conducted using the suspect's photograph. A potential match was found and the subject was arrested within 23 hours of the robbery.

See Chapter 9 for more FR success stories.

Chapter 2 Technology

This chapter provides summary detail of a facial recognition (FR) system, including external aspects such as the quality of images captured during the enrollment process.

FR systems are generally operated within an agency information technology (IT) environment with multiple modules or components. The components include, but are not limited to:

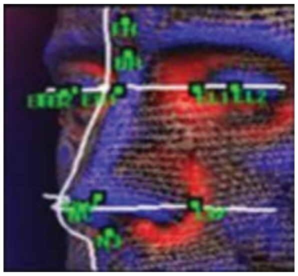
- Workflow management supporting the daily comparisons and results presentation to examiners
- Applications software used by examiners
- FR search engine services executing comparisons and generating match results
- Database services to store images, templates and results

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.

2.1 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 verification and identification.

FR 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.



FR 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
- Shape of the cheekbones
- Dimensions of the mouth
- Length of the jaw line

These features are measured to 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.

FR 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. Technology is advancing quickly, and there are several emerging approaches, such as three-dimensional (3D) modeling, that may overcome some of the current limitations with the systems.

As with other biometrics, the accuracy of FR implementations varies greatly across the industry. Absent other performance or economic parameters, user agencies should be aware of the variability and apply the most current system and software available.

FR use is not limited to governmental institutions. There is extensive development in the private sector that focuses on smartphone applications for use in social media, gaming, and targeted marketing. For example, social media uses FR software to help automate user tagging in photographs.

Performance Factors

System match performance is contingent upon the baseline algorithms of the system to drive following factors:

- Verification
- Identification
- Image quality
- Accuracy
- Time elapsed between captured images or aging[1]
- [*] Using consistent camera type
- Gallery size

Similarity Scoring

FR screening produces a similarity score for each comparison, identification, or verification. A numerical threshold, configured individually for the solution and image database, defines the level at which human review and follow-on adjudication will occur. FR applications may provide the option to display or review the similarity scores between the probe image and the associated candidates. The actual scores may vary between vendors and algorithm versions. As a result, the scores should not be compared with one another.

Recommendation 2.1.1: Similarity scores should not be used during initial review as an investigative tool, or decision point.

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.

Recommendation 2.1.2: Vendors provide a work queue to load images for manual enrollment.

Search Engine Technology

Biometric search engines provide comparison results that FR systems 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

[*] P. Grother, et al. *Report on the Evaluation of 2D Still-Image Face Recognition Algorithms*, NIST Interagency Report 7709, August 2011. See http://www.nist.gov/itl/iad/ig/mbe.cfm

- 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

2.2 Standards

Standardization of the image capture (or photo) is vital to FR accuracy. Standardized image capture facilitates interchange of the biometric data themselves and enables interoperability of FR systems. 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. 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.

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.

Data Elements	Mandatory	Recommended
Credential Number	■	
Unique Identifier	■	
Credential Type (DL, ID, DPC, EDL)	■	
First Name	■	
Middle Name	■	
Last Name	■	
Suffix		■
Address		■
City		■
State		■
Zip		■
Date of Birth	■	
Height		■
Weight		■
Eye Color		■
Hair Color		■
Sex		
Image Capture Date	■	
Capture Operator		■
Capture Machine Name or Capture Station	■	

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

A few of the key standards include:

- 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 driver's licenses).

- 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 standards in a direction that facilitates growth, advancement, and interoperability.

The Organization of Scientific Area Committees (OSAC) Subcommittee on Facial Identification (SFI), and the Facial Identification Scientific Work Group (FSWIG)[‡] are involved in gathering and disseminating accurate information regarding the proper application of facial identification (FI) and FR methodologies and technologies. OSAC SFI and FISWG 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 and FISWG is to develop consensus standards, guidelines, and best practices for the discipline of image-based comparisons of human features, primarily the 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 and FISWG seek to leverage constituency group and stakeholder knowledge to produce guidelines and position statements and to 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 and FISWG are 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).

[†] NIST Special Publication 500-290.

[‡] The OSAC Committee on Facial Identification. https://www.fiswg.org

NIST Testing Perspective

The National Institute of Standards and Technology (NIST) publishes test results showing the comparative performance of FR algorithms and contrasting against previously measured performance.[§] For example, the NIST report shows that for the four developers who submitted algorithms to NIST in 2010 and 2013, accuracy improved in all cases.

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 1:N search remains poorly quantified.

2.3 Image Capture Guidelines

Good image captures that support credential issuance also support FR. AAMVA's DL/ID Standards and Secure Design Principles provide guidance to issuing authorities for obtaining optimal image capture, and they can be applied in other controlled environments where an agency captures still images.

Pose: The image should 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).

Depth of field: A full-face frontal pose should 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) should 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 should 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 should be used to capture the full-face frontal pose, that is, appropriate illumination techniques and illumination should 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 eyeglasses).

Background: A uniform light blue color or white background should be used to provide contrast to the face and hair. Note: There is a 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 should be centered.

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

- 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.

[§] P. Grother and M. Ngan. Face Recognition Vendor Test: Performance of Face Identification Algorithms. *NIST Interagency Report 8009.* https://www.nist.gov/publications/face-recognition-vendor-test-frvt-performance-face-identification-algorithms-nist-ir

[¶] Personal Identification—AAMVA North American Standard—DL/ID Card Design–A.7.8.1–Portrait

- 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 the face area
- Neutral expression
  - Helps matching against other images with non-neutral expressions
- Avoid eyeglasses.
  - Glare affects enrollment
  - Heavy glasses affect comparison
- Avoid headwear when possible.
  - When headgear is allowed, the chin, ears, and forehead should be visible.
- A 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 non-conformant presentation). For example, a non-frontal pose might be an attempt to evade a duplicate license check.

2.4 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. A JPEG image, if saved more than once, compresses images so much that it can change the photo dramatically. Therefore, user agencies should consider using Portable Network Graphic (PNG) or Bitmap (BMP) formats because they do not compress the original image.

Stored image captures 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.

2.5 Devices, Equipment, and Software

Following are some considerations for configuring equipment in various environments.

Cameras and Lighting During Image Capture

One of the benefits of using a facial image as the biometric is that the image capture is unobtrusive and can be easily acquired using a commercially available digital camera. Selecting an appropriate digital camera and background equipment is important.

Uniformly sufficient lighting is the most important aspect in capturing a quality 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 image as the lighting provided by the camera's flash.

Analyst or Examiner Workstations

The examiner should be provided a well-lit, ergonomic workspace. Standing workstations should be considered. 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 images along with a useful set of comparison controls or other inputs or visual tools provided by the image comparison software. Use of multiple monitors by each examiner can improve the effectiveness and efficiency of the image review process.

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, play 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 should 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 and 900 in the vertical direction should be avoided.

Application Tools Available to Verify Identities

There are a number of commercially available software tools to assist examiners in confirming the matching results. User agencies should consult with their vendor to determine the desired capabilities of their suite of tools. Examples include, but are not limited to:

- **Detailed zooming:** Allows users to zoom in close to a specific facial feature on two images simultaneously. For example, 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

2.6 Networks, Bandwidth, and Communication

This document does not attempt to replace or define IT architecture or 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 of system requirements is performed and appropriate standards are followed, including future operation and maintenance requirements.

2.7 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.

The 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.
- **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. 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.

Chapter 3 Program Development and Enhancement

For jurisdictions considering implementing or enhancing a facial recognition (FR) program, this chapter can be used as a blueprint to assist in development of an effective program or as a benchmark document to identify opportunities for program improvement. A program mission statement that concisely describes what the program is meant to accomplish and why should 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, implementation, and maintenance.

3.1 Program Development

Items that may be included in developing a comprehensive FR program plan include:

- Legislative considerations
- Identification of a project lead
- Request for information (RFI)
- Request for proposal (RFP)
- Budget considerations
- Policy development

Legislative Considerations

Before pursuing legislation (if authorizing legislation is needed), 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 needing or seeking to amend current legislation, AAMVA has developed model legislation (see Appendix A). This model legislation is not intended to fit the exact needs of every jurisdiction. Rather, it is intended to provide a foundation of 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, including law enforcement and prosecutors (see Chapter 8).

Project Lead

A project lead should be identified during initial planning to ensure a person is involved in every aspect from program development through deployment and implementation. Some general project management experience would be beneficial.

Request for Information

An RFI allows a jurisdiction to conduct research to determine specific needs and find out how vendors may be able to meet those needs. When a detailed RFI is completed, the jurisdiction should be confident that when they complete an RFP, they have all the information included that will adequately fulfill their FR program requirements.

Request for Proposal

An RFP is a document that government agencies create to outline the requirements for a specific project. Agencies use the RFP process to solicit bids from qualified vendors and identify which vendor might be the best qualified to complete the project.

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:

- **Technology acquisition costs:** These are the costs involved with procuring and installing the facial recognition system.
- **Staffing costs:** These are costs associated with training, daily screening, and investigation efforts.
- **Operation costs:** These are ongoing technical costs required to maintain the technology and operate the computer systems
  - Infrastructure (network, data storage, hosting, and data recovery, as well as hardware and software updates)
- **Administration costs:** These are costs involving record changes and management, citizen correspondence, hearings, and so on.

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

Policy Development

Every jurisdiction that has an FR system should have an FR policy. The policy should:

- Define the system objectives.
- Provide a set of ground rules for how to handle day-to-day operations.
- Guide the system users on the appropriate and efficient use of the system.
- Outline who can access the system.
- Describe how to handle requests from other agencies.
- Describe how to handle exception processing.

(See Appendix B for sample policies.)

3.2 Project Planning

The project plan is an approved document used to guide both project execution and project control. It should include, at a minimum, the timeline, requirements, risks, and data conversion.

Timeline

The project lead should provide a clear vision broken into stages, each with measurable goals. The vision should include the required tasks and the responsibilities for each team member.

Requirements

The importance of developing comprehensive requirements is key to the success of deploying and operating an FR system that meets the jurisdiction's objectives and deliverables. Business, functional, and technical requirements should be clearly identified and documented. The long-term reliability of an FR system depends on having a maintenance plan. Depending on contract terms, systems maintenance may be required by the vendor, or it may be managed by the jurisdiction's information technology (IT) staff. A jurisdiction should take maintenance and upgrade options into consideration when developing a maintenance plan for current and future budget cycles.

Licensing and the need for additional storage as the image database increases in size are functions and costs that should be reviewed on a regular basis.

Risks

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

Data Conversion

Current data should 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.

3.3 Implementation

Implementation, sometimes referred to as project execution, typically defines the activities related to building and customizing software and building the IT infrastructure.

Software Development and Delivery

Often an FR product selected during procurement will not meet all of an agency's needs right out of the box without some level of customization. As with other application development projects, adhering to a mature software development life cycle (SDLC) will ensure the delivered application meets quality, performance, and business expectations while having a manageable cost of ownership over the total life of the system. The U.S. Department of Justice guidelines* define a comprehensive SDLC methodology that has become the de facto standard for many government organizations.

Information Technology Infrastructure

The complexity and effort required to build the IT infrastructure will vary greatly based on the size of the program, the state of technology available in the marketplace, and system performance requirements. Information in Chapter 4 of this document introduces some of the FR technology factors that qualified IT staff will need to consider when designing and building an FR system's IT infrastructure.

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.

3.4 Deployment Options

When deploying an FR program, jurisdictions should determine the option that best meets their needs (i.e., piloting, phasing, or immediate full system deployment).

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.

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 the system may have on its users 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 4, Section 4.3, for more information on setting a threshold).

A second 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.

* http://www.justice.gov/archive/jmd/irm/lifecycle/table.htm

A third pilot approach is a 1:N pilot. This involves loading a portion of your system images for a mini-scrub. This allows you to evaluate the quality of images within your system, lighting, and other problems that may be encountered in different offices. This approach also allows staff to become familiar with how the system works and identify changes they want or need.

Phased Deployment

A phased approach is an option for agencies that choose to deploy FR in stages (i.e., a regional deployment approach). Choosing to phase in FR can determine workload and aid in adjusting parameters as deployment continues jurisdiction-wide. This approach can allow for a scrubbing of legacy images on a gradual basis, thereby incrementally identifying the number of matches requiring investigatory follow-up.

Immediate Full System Deployment

A full system deployment offers immediate program-wide benefits. The impact to employee workload and 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.

Chapter 4 Operations

The use and operation of a facial recognition (FR) system broadly includes the legacy cleanse, staffing, and processes. It is a basic tenet that potential matches from facial recognition should generate human examination and no other action, such as an arrest or corrective action, should be taken solely on the basis of a FR result.

4.1 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 one-to-many (1:N) identification for images uploaded from the credential issuing agency's database. 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 (identification) and one-to-many (1:R; 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

Below are the pros and cons of a full versus a partial scrub.

Scrub Type	Pro	Con
Full	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.	A complete system cleanse will require more resources as there will be a greater number of results that may need to be adjudicated. Many cases may be beyond the statute of limitations for criminal or administrative action.
Partial	A partial cleanse will give the jurisdiction a smaller number of results and will require fewer resources during implementation. Case results will likely fall within statute of limitations for criminal or administrative action.	A partial cleanse will only identify fraud from the cleanse start date to present. Any fraud before the start of the cleanse date will not be detected. The database will not be completely cleaned up, and errors will not be corrected.

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

Recommendation 4.1.1: Perform a full scrub.

Recommendation 4.1.2: Jurisdictions should consider contacting other agencies that have implemented an FR program to gather information and lessons learned on their experiences in handling scrub results.

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:** Perform an FR identification search of each image against all other images.
- **System-generated results:** Select highest probability for further investigation.

When the scrub is completed, the jurisdiction should analyze the scrub results. Users should then use facial identification to determine the presence of a false positive, clerical error, or fraud, and appropriate action should be taken. Procedures should be developed or updated to address the errors and the analysis of cases to determine if other criminal activities have occurred. 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 should be addressed to clean up the image system and may require corrective or investigative action.

- **False positive:** When one or more candidates are not matches with the probe.
- **Clerical error:**

  – 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.
- F**raud:**

  – A person intentionally using different identities (real or fictitious)

  – Multiple persons using the same identity

4.2 Staffing Considerations

The selection and training of examiners for specific job functions and charging them with the appropriate FR responsibilities. See the AAMVA's *Best Practices for the Deterrence and Detection of Fraud* for information on staffing a fraud unit.

Staffing considerations include, but are not limited to:

- Staffing should be sufficient to handle processes as defined in 4.3.
- Staff who are responsible for reviewing potential cases should have other duties to avoid burnout.
- Staff assigned to FR units should have diverse backgrounds.
- FR system users should have appropriate level of access based on their job responsibilities.

4.3 Processes

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 credential (see AAMVA's DL/ID Standard and Secure Card Design Principles).

Central issuance process recommendations:

Recommendation 4.3.1: Capture and enroll an image of applicants any time they visit a credential issuing authority for a transaction.

Recommendation 4.3.2: At the time of application. perform a 1:1 FR comparison upon capture of new image to the most recently captured image for that record.

Recommendation 4.3.3: Review daily leads before final credential issuance.

Recommendation 4.3.4: Perform a second-level review of the lead when fraud is suspected.

Although central issuance is the preferred (best practice) issuance method, jurisdictions that have over the counter issuance processes should follow these recommendations:

Recommendation 4.3.5: Complete a full scrub of all images in the legacy system.

Recommendation 4.3.6: Complete a 1:1 comparison at the time of application. Deny issuance of the credential if images do not match.

Recommendation 4.3.7: For initial issuance, complete a 1:N of the newly enrolled images before production of the credential. If a potential match is identified, deny issuance and advise that the credential cannot be issued at this time. If 1:N cannot be done at time of application, then complete a 1:N 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 be or were not processed as part of the scrub or daily operation. Examples of exceptions include restricted photos; user test images; and images that cannot be systematically enrolled because of a disfiguration, eye patch, and so on.

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.

Setting a Threshold

When developing an FR program, jurisdictions should determine the threshold at which potential matches should be generated. Different thresholds may be needed for 1:N and 1:R.

The threshold directly impacts the number of leads received for manual review. Jurisdictions should work with their vendor to set the threshold to balance the workload requirements with the potential fraud that may be identified.

> *The threshold directly impacts the number of leads received for manual review. Jurisdictions should work with their vendor to set the threshold to 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.

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.

Watch List

Jurisdictions may have an investigation when they have an image of a person but are unsure of the true identity. The person may appear at a credential issuing agency in the future and obtain a credential in a new identity unbeknown to the investigator and that agency. By using a watch list, the existing image can be templated and stored in the facial recognition system. This template can then be checked through the facial recognition system on a regular basis in an attempt to locate a potential match. Staff examining potential matches would be alerted to this during a future review thereby assisting in identifying the unknown person.

4.4 Reporting and Trending

Statistics regarding the number of applicants processed, the number of leads, and the number of records of potential fraud should be recorded. Statistics should be reviewed to determine if the program's goals and objectives are being met. Most FR products designed for users already include several predefined reports. Additional reports may also be desired.

Operational Reports

Operational reports allow the jurisdiction to monitor operations and to ensure credentials 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
- **Audit report:** lists images processed by the 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 may be sent to advise the applicant that her or his credential cannot be issued until she or he returns to an office for a photo retake.

Analytical Reports

Analytical reports are used strategically by management to make long-term decisions and manage staff activity. The analytical reports defined for FR should provide measurements of key performance objectives. Examples include, but are not limited to:

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

Audit

Jurisdictions should ensure that audits are conducted regularly. The process may require the ability to retrieve a chronology of events (history) for any image request that enters FR. It includes the history for any activity related to the record, such as any notes recorded, searches completed on the record, and so on.

Chapter 5 Training

Training that includes information on a multitude of topics for various levels of staff and management of the agency should be developed and delivered. Additional training for external users, partners, and those involved in prosecution is beneficial to complete the educational process that is necessary to deploy a successful facial recognition (FR) program. As technology in FR continuously develops, so should the training.

Classroom training provided by subject matter experts is recommended over online or other training methods. 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

Training	Field Office Staff	Analyst or Investigative Analyst	Examiner	Facial Recognition or Investigative Manager	Information Technology Operations and Support	External Users	External Partners
Limitations of Technology	■	■	■	■	■	■	■
Ethical Use and Privacy	■	■	■	■	■	■	■
Processes and Procedures	■	■	■	■	■	■	■
User Access and Security	■*	■	■	■	■	■	
Application Usage	■*	■	■	■	■*	■	
Facial identification	■	■	■	■		■	■
Specialized facial identification training		■	■	■		■	■*
Case management		■	■	■			■*
Photo requirements	■	■	■	■	■	■	■
Biometric technology	■*	■	■	■		■	■
Systems and software				■	■		
Refresher training	■	■	■	■	■	■	■

**If applicable.*

Limitations of Technology

FR comparisons do not provide explicit yes-or-no results. The results are "probable matches" that need to have a facial identification examination completed 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 quality of a photograph.

In the end, trainers should ensure examiners understand that they should 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.

> *FR comparisons do not provide explicit yes-or-no results. The results are "probable matches" that need to have a facial identification examination completed by a qualified staff member to make a determination.*

> *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.*

5.1 Ethical Use and Privacy

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

Training curricula should include but not be limited to the following:

- Data contained within the FR system should 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 accomplish the agency's mission and objectives.
- Information contained in the FR system may 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 should be notified immediately if a transaction involves any possible conflict of interest. The agency vendors may be able to provide an automated process.

- 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.
- Possible ramifications for violations of ethics and privacy policies should be established.

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.

5.2 Application Usage

Application usage training should consist of everything from accessing the system to adjudicating cases reported by the system.

Processes and Procedures

Training for the processes and procedures are jurisdiction specific and 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.

Facial Identification

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 Identification Training

The Federal Bureau of Investigation, Criminal Justice Information Services (CJIS) Biometric Training Team, is one source of independent training to assist jurisdictions. The Federal Bureau of Investigation (FBI) may also provide on-site training. The FBI CJIS Face Comparison and Identification Training may be requested by sending a formal written request on your agency letterhead, signed by your supervisor or superior, via email as an attachment to biometric_training@leo.gov. Explain the reasons your agency could benefit from the training and be sure to include your agency's ORI number (qualifying agency identifier issued by the FBI). These classes are free of charge but require a minimum of 15 students. This class is also offered several times a year at the FBI CJIS Division Complex, in Clarksburg, WV.

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 reporting. The agency vendor may provide additional training resources.

Prosecutor Training

It is essential that prosecutors are educated on the fundamentals of FR technology and how it is used as part of the credential issuance process, as well as system capabilities and limitations. Prosecutors should understand the limitations on the information an examiner can provide when testifying and that FR is only an investigative tool. Other elements of the criminal justice system may also request training.

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 2.3, Image Capture Guidelines.

5.3 Refresher Training

Refresher training provides updates, examples of positive investigative outcomes, and various uses of FR and should occur at least annually, if not more frequently. Changes to program policy and operations should also be included in refresher training. Three training components that should be conducted annually are:

- The limitations of the FR technology
- Ethical use of the system
- User access and security

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.

Chapter 6 Privacy

Customer privacy and the protection of personal information is paramount and should be consistent with the laws of the jurisdiction. Although biometric matching itself raises privacy concerns for some, the use of the technology actually helps protect people's privacy and personal identity.

Security and Access for Database and Records; Protecting Against Unauthorized Use

It is critical to have a policy that strictly controls who can access data for what purpose and that establishes specific limitations along with periodic audits to ensure adherence. The data contained within the facial recognition system must be maintained in accordance with established policy and must be protected from unauthorized access, use, and disclosure. Jurisdictions must have a uniform policy in place regarding the appropriate use and access of facial recognition. Appendix B provides an example of a jurisdiction facial recognition (FR) program policy.

It is critical to have a policy that strictly controls who can access data for what purpose and that establishes specific limitations along with periodic audits to ensure adherence.

Jurisdictions should 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. Personal identifying information (PII) should be protected against unauthorized access and accidental disclosure. A policy should be established that governs both personnel granted privileges to access records and any external organizations with which records may be shared.

Aside from the threat of unauthorized external use, 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 fraudulent records. Appropriate measures should be taken to ensure the integrity and security of records maintained by the credential issuing authority.

A successful approach to combating threats includes a layered security strategy, which should address both physical and remote threats. Advances in technologies used for intrusions necessitate a careful and well-thought-out design of each system component. For example, new software will alert if you attempt to transmit any PII information. If continued, it will alert the information security officer. 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 they contain the most sensitive and valuable data.

6.1 Data Breach

A data breach occurs when stored information is accessed or leaked by unauthorized individuals. It is extremely important to have layers of security in place to protect the PII that is in the FR system.

The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence when (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for a purpose other than authorized purposes. An entity's response to a data breach may be addressed in state law or agency policy. This may include incidents such as:

The security of PII must be a priority to prevent data breaches. Agencies should develop comprehensive policies and procedures for protecting the confidentiality of PII, including FR data.

- Theft or loss of digital media—including computer tapes, hard drives, or laptop computers containing such media—upon which such information is stored unencrypted
- Posting such information on the internet
- Unauthorized employee access to certain information
- Moving information to a computer otherwise accessible from the internet without proper information security precautions
- Intentional or unintentional transfer of information to a system that is not completely open but is not
- Appropriately or formally accredited for security at the approved level, such as unencrypted e-mail
- Transfer of information to the information systems of a possibly hostile agency or environment where it may be exposed to more intensive decryption techniques

Having a security protocol in place will help the recovery process if PII is compromised. The protocol varies by jurisdiction, but the first step after an identified data breach is alerting the customer in a timely manner and allowing him or her to take the necessary steps to protect his or her identity. There are services that are not specific to any one jurisdiction that can be offered to the customers for free by contacting the three major credit reporting agencies (Equifax, TransUnion, and Experian). Providing actions for the customer to take can alleviate the stress and further protect the identities of those affected.

6.2 Privacy in the United States

The Driver Privacy Protection Act (DPPA) of 1994 governs the manner in which credential issuing authorities may release personal information and defines penalties for misuse by agencies and individuals. Congress passed the DPPA as an amendment to the Violent Crime Control and Law Enforcement Act after it was learned that criminals were obtaining and accessing personal information from credential issuing authorities and using it to carry out violent crimes. In essence, credential issuing agencies are prohibited from knowingly disclosing or making available personal information outside the parameters of the DPPA. The DPPA defines personal information that identifies an individual, such as a photograph, Social Security number, driver identification number, name, address (not 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."

Although 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, there are some federal statutes, such as the Cyber Privacy Fortification Act, that include requirements for protecting personal information.

In June 2019, The United States Government Accountability Office (GAO) published written testimony before the Committee on Oversight and Reform, House of Representatives on Facial

Recognition Technology. The GAO testimony outlined how the Department of Justice and Federal Bureau of Investigation have taken some actions to response to previous GAO recommendations to ensure privacy and accuracy. Additional work remains on this front, and efforts continue.

6.3 Privacy in Canada

Every Canadian province and territory has its own laws that apply to provincial government agencies and their handling of personal information. Some provinces have private-sector privacy laws that have been deemed "substantially similar" to the national Personal Information Protection and Electronic Documents Act (PIPEDA). In this case, the private-sector privacy laws may apply instead of PIPEDA. Each province and territory has an Information and Privacy Commissioner (IPC) or similar body that is responsible for oversight and enforcing provincial access and privacy laws.

For more information, contact the Office of the Privacy Commissioner of Canada. This office also has contact information for the commissioner or ombudsperson responsible for overseeing provincial and territorial privacy legislation.

Chapter 7 Access and Sharing of Images

Facial Image Access and Dataset Sharing

There are numerous questions surrounding the issue of allowing law enforcement to have access to credential issuing authority–owned facial recognition (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? Each jurisdiction should answer these questions in accordance with its own laws and policies.

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 credential issuing authority. This is particularly important in jurisdictions that do not have a dedicated investigations unit to handle fraud. Cooperation between the two is important to facilitate the identification, arrest, and prosecution of criminals. Sharing of information allows government to be more efficient and proactive in fighting fraud and protecting identities.

Types of Shared Personal Identifying 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:

- 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 credential issuing authority's database implies a clerical error or fraudulent activity, a link between that record and a law enforcement record implies that the customer had a previous law enforcement contact. Jurisdictions should ensure only authorized individuals or entities have access to such information.

- Photo-matching tools may return false matches, which necessitates the need to make personal identifying information data available to authorized examiners. Because of this, it may be necessary to modify existing privacy protection policies.

Establishing a Memorandum of Understanding

When entering into a data sharing partnership, a Memorandum of Understanding (MOU) should be executed to ensure responsibilities and expectations are established. A clear understanding and agreement of the process and protocols is essential to establishing and maintaining a mutually successful partnership. MOU examples can be found in Appendix C. Development of MOU(s) should involve the agency's legal counsel to address the many issues surrounding the sharing of data.

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 E.

When considering data-sharing partnerships with law enforcement that provide for image comparisons, foundational information about how FR technology functions, its intended uses, and operating principles is imperative. Toward this end, Appendix D contains a document titled *Guiding Principles for Law Enforcement's Use of Facial Recognition Technology*. This document was created jointly by the International Association of Chiefs of Police (IACP) CJIS Committee. IACP Criminal Justice Information Services (CJIS) Committee and the IJIS Institute and is intended for law enforcement executives. This document provides a high-level explanation of FR technology and identifies principles for proper use by law enforcement. This is an example of providing proper educational information that clearly establishes public and user expectations regarding the use of facial recognition technology.

Recommendation 7.1.1: Motor vehicle administrations entering into an MOU with a partner law enforcement agency or providing FR comparison results should include the *Guiding Principles for Law Enforcement's Use of Facial Recognition Technology* document narrative (or reference to the document) as part of the MOU or FR comparison request results.

Security Standards and Guidelines

The National Institute of Standards and Technology (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 credential issuing authorities 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 800-137, An Introduction to Information Security Continuous Monitoring (ISCM)*
- *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 800-100, Information Security Handbook: A Guide for Managers*
- *SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*
- *SP 800-77, Guide to IPsec VPNs*
- *SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations*
- *SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems*

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:

- 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 CJIS Security Policy (CJISD-ITS-DOC-08140-5.1) provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of criminal justice information data.

Chapter 8 Stakeholders, Collaboration, and Outreach

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 the vast range of interests and concerns with a facial recognition (FR) program. Partnerships should be developed with stakeholders within the jurisdiction, as well as cross-jurisdictionally.

8.1 Examples of Successful Jurisdictional Partnerships

The Nebraska Criminal Justice Information Services (NCJIS) 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 credential issuing authority 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) have an established partnership for investigating potential FR matches with possible criminal predicate. When the Washington DOL finds probable identity theft, they refer the matter to the WSP for follow-up criminal investigation.

To learn more about jurisdictional successes with FR programs, please see Chapter 9.

8.2 Public Education and Outreach

Outreach and education is an important and effective method for gaining public acceptance. Open and transparent communication is necessary for a jurisdiction to build confidence that the program has been established to protect the public. There are two public outreach approaches to consider when implementing an FR program: a high- or low-profile campaign.

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 recent Brookings Institute national survey (2018), also cited in Chapter 1, indicates that 75% of Americans believe the federal government should not strictly limit the use of facial biometrics technology.

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 how this technology can prevent people from defrauding credential issuing authorities and protects identities. 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; 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. Consider whether the story illustrates the problem and highlights the solution the program provides. If properly promoted, success stories can also deter criminals.

Stakeholder Communications

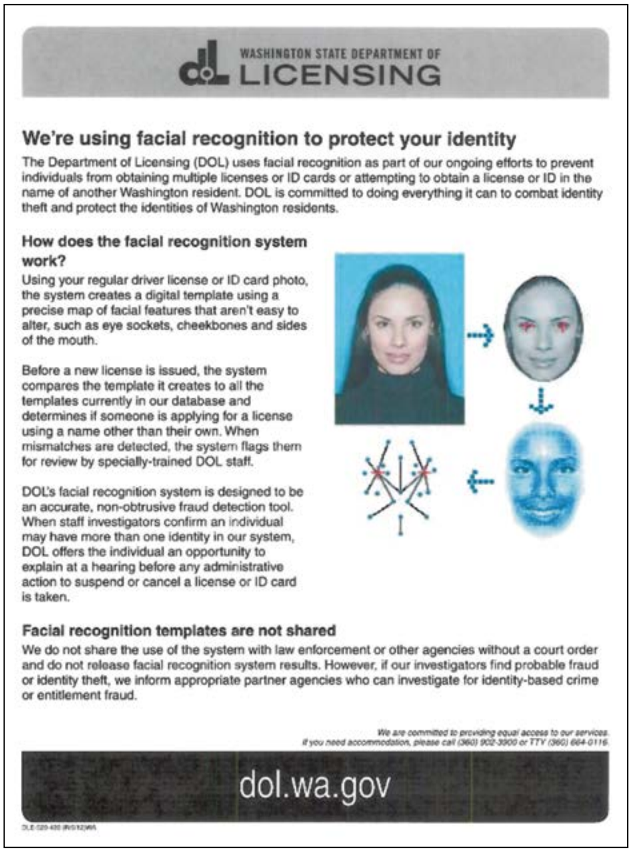
A communication plan should be developed to educate stakeholders. The plan should be tailored for the audience. For example, when presenting to prosecutors, include a demonstration of the FR platform, presenting the steps an examiner follows with image collection, dataset query, image gallery development, 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.

Stakeholders

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

- Governors and ministers
- Other jurisdictions
- Legislators
- Agency directors
- State, local, and federal law enforcement agencies
- Correctional institutions
- Prosecutors
- Judiciary: attorney general, public defender's offices, presiding judges and magistrates
- Public health and benefit-oriented agencies
- General public

The Washington DOL uses posters such as this in their office lobbies to educate the importance FR plays in protecting individual identities.



WASHINGTON STATE DEPARTMENT OF
LICENSING

We're using facial recognition to protect your identity

The Department of Licensing (DOL) uses facial recognition as part of our ongoing efforts to prevent individuals from obtaining multiple licenses or ID cards or attempting to obtain a license or ID in the name of another Washington resident. DOL is committed to doing everything it can to combat identity theft and protect the identities of Washington residents.

How does the facial recognition system work?

Using your regular driver license or ID card photo, the system creates a digital template using a precise map of facial features that aren't easy to alter, such as eye sockets, cheekbones and sides of the mouth.

Before a new license is issued, the system compares the template it creates to all the templates currently in our database and determines if someone is applying for a license using a name other than their own. When mismatches are detected, the system flags them for review by specially-trained DOL staff.

DOL's facial recognition system is designed to be an accurate, non-obtrusive fraud detection tool. When staff investigators confirm an individual may have more than one identity in our system, DOL offers the individual an opportunity to explain at a hearing before any administrative action to suspend or cancel a license or ID card is taken.

Facial recognition templates are not shared

We do not share the use of the system with law enforcement or other agencies without a court order and do not release facial recognition system results. However, if our investigators find probable fraud or identity theft, we inform appropriate partner agencies who can investigate for identity-based crime or entitlement fraud.

We are committed to providing equal access to our services.
If you need accommodation, please call (360) 902-3900 or TTY (360) 664-0116.

dol.wa.gov

DLE-520-400 (R/5/12)WA

Open communication provides transparency and builds trust. It is important to continually dispel 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 and enhances highway safety.

Chapter 9 Success Stories

Facial recognition (FR) programs provide a number of benefits. Following are seven stories that serve as a small sample of experiences and successes with jurisdictional FR programs.

Highway Safety Impact

A New York City taxi driver was identified via a daily FR match to have two New York State (NYS) driver's licenses (DLs). One was valid that he had renewed the day before; the other was revoked for failure to respond after being arrested for driving while intoxicated (DWI). When a criminal history search was conducted as part of the case preparation, it revealed that the subject had been previously arrested multiple times using a total of six different names and dates of births (DOBs) and a variety of DLs from the northeast states. Overall, the subject had 268 open suspensions in NYS for unpaid moving violations, two separate revocations, and $30,000 in unpaid judgements.

Fugitive Who Escaped from Prison 41 Years Earlier Arrested

In 2014, Ronald Carnes applied for an Iowa DL. In 1973, Carnes had walked away from a North Carolina Correctional Institution where he was serving a 15- to 20-year sentence for armed robbery. After serving three years of his sentence, he escaped and began a new life living under multiple identities and working various jobs around the country. No one suspected who he really was until 2014, when he applied for a DL at an Iowa Department of Transportation Driver's License Office. FR identified Ronald Carnes as possibly both Ronald and Bill Cox. An investigation commenced by the Iowa Department of Transportation's Bureau of Investigation & Identity Protection. After a search of Carnes' home turned up evidence of the crime, Carnes was arrested and sent back to North Carolina to complete his original sentence.

Forced Labor Traffickers Arrested

The Kansas Department of Motor Vehicles' (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 ringleader and several of his conspirators were eventually identified by the Kansas DMV's FR system after the individual's returned to the DL office to apply for DLs 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.

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 Nebraska DMV database. She continued to renew both DLs 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.

Multistate Commercial Driver' License *Fraud*

New Jersey conducted a multistate Commercial Driver License (CDL)/FR pilot with New York and identified a CDL driver who had his CDL revoked for four DWI convictions. The subject had purchased a new identity from an individual incarcerated in Puerto Rico and used it to obtain a valid CDL in New York. The subject continued to use the new identity to operate trucks registered under his original identity and gathered and paid a variety of moving violations. When an arrest warrant was obtained, it was found that the same false identity was used to obtain Class D DLs in the States of Florida, Connecticut, and Massachusetts. The subject was arrested and charged with multiple felonies. To resolve the other records, New York officials contacted the other jurisdictions and then issued a permissive revocation for fraud that flagged the identity to prevent any new activity.

Taxi Driver Fraud Foiled by Facial Recognition

When NYS DMV had the Institute of Traffic Safety examine the driving records of "for-hire taxi drivers" who had been identified with FR, they found a trend in the New York City metro region. Instead of obtaining a second license, many licensed taxi drivers obtained a non-driver ID card using a different name, DOB, and verified Social Security number. The "clean" DL was used for registration and insurance purposes, and the non-driver ID was presented for traffic stops. For the majority of the stops, the driver was cited for operating without a license and operating without a "for-hire" license, and an infraction for the initial offense was never issued. The study identified many drivers who used this scam over an 8- to 10-year period. After it was identified, it was passed along to the New York Police Department, and they quickly addressed the issue through enforcement.

One Person; 146 Identities

When Indiana DMV first started using FR, the state found a resident with 146 different identities. This individual was running a check-kiting scheme across multiple states. Indiana worked with law enforcement to determine what the individual's true identity was, and they were able to locate and arrest him in Nebraska.

Appendix A Model Legislation

Many jurisdictions have successfully implemented FR technology without enabling legislation by using existing laws or administrative codes. Jurisdictions seeking to pursue enabling or strengthen existing legislation may consider some or all of the following model legislation:

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 should meet the Best Practices 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 credential 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 authorized purposes ;

    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 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, should conform to the appropriate security safeguards as mandated by state law, regulation, and procedures.

Appendix B Sample Policies

The Bureau of Justice Assistance (BJA) has Facial Recognition Policy Development Template (December 2017) that jurisdictions can use as a guide for developing or updating their agency policies as they desire. The document can be found at www.ncirc.gov.

What follows is a sample policy provided by the Arizona Department of Transportation:

I. Purpose

This policy provides uniform guidance regarding the appropriate use of facial recognition. Facial Recognition is a technology designed to perform an initial search for candidates as a foundation for manual comparison/identification analysis to uncover potential fraudulent activity such as identity theft, internal/occupational fraud within the Division of Motor Vehicles (DMV) credential data base while maintaining compliance with (**list appropriate statutes**). This technology can be a valuable investigative tool to support the investigative efforts of law enforcement and public safety agencies both within and outside (state name).

II. General Policy Statement

A. The (**agency name**) hereby be referred to as "division" is responsible for investigating and taking appropriate action to prevent or rectify Identity Theft, Credential Fraud or Clerical Errors with the DMV credential data base. Facial recognition is designed to identify suspicious activities, include, but not limited to:

a. An individual holding more than one credential under multiple names;

b. Multiple (differing) individuals holding a common identity and credential number

c. Clerical or data entry errors that, for example, result in the attachment of a photo to the wrong driver record or the creation of multiple records for the same customer (combined records).

d. A pattern of truncations completed by a Customer Service Representative that may indicate internal fraud.

B. An added potential internal use may include searching for misuse of credentials, as part of a law enforcement pre-employment background investigation.

C. (**agency name**) may also fulfill outside law enforcement agency requests for image comparisons of the following persons:

a. Subjects suspected of having committed a crime or who law enforcement may suspect is about to commit a crime

b. Subjects involved in activities determined to be a potential threat to public safety

c. Subjects sought as part of a criminal investigation or an intelligence-gathering effort

d. Applicants for a government of law enforcement security clearance

e. Subjects for whom a warrant has been issued

f. Subjects suspected of benefit fraud

g. Individuals labeled as missing person

III. Definitions

IV. Responsibilities

A. Level 1 reviewer is responsible for reviewing and completing a facial comparison on DMV photographs to identify potential fraud and submit questionable images for a second level review

B. Level 2 reviewer is responsible for final review of questionable images than assigning potentially fraudulent records to investigator

C. Investigator is responsible for reviewing potentially fraudulent records, scheduling and conducting interview with customers and forwarding recommendations to the appropriate departments for action

D. Legal is responsible for conducting hearings when applicable

V. Access Requests

(**If applicable for per your State requirements**) All requests for external identification results require the completion and submittal of Facial Recognition Form and the attached investigative photograph. Such request must be submitted by an authorized law enforcement agency or a governmental non-criminal justice agency involved in the identification of searching for missing persons or actively involved investigation of fraud. No personal identifying information obtained through the use of facial recognition shall be disseminated to members of the general public or to the news media with the following exceptions:

A. Public Safety Organization – When a law enforcement agency supervisor or an official prosecutor in the jurisdiction determines that an individual poses a threat of substantial harm to the public, then facial images and relevant identifying information may be released to the public.

B. A determination that the "public safety organization" exception applies should be documented in writing by the (**Title of administrator**).

C. The release of facial images and identifying information should be limited to information that could reasonably protect the public from harm, as determined from the information submitted by the requesting law enforcement agency.

D. Limit the total number of facial images provided to an authorized requestor by performing sufficient comparison necessary to refine the results.

VI. Retention Requirements

A. Internal Requirements – (**agency name**) Facial Recognition staff will maintain a log of all transactions made via the facial recognition system in accordance with established retention schedules. A copy of the query and the query response (to include facial images or gallery results) will be retained in the (**storage place**).

B. System Report – Capabilities of running ad hoc or established reports on individual queries in accordance with established retention schedules.

VII. Data Provision Requirements

(**If hosted – agency name/vendor name**) shall maintain full control and ownership of the facial recognition system (hardware) and associated data and, for that reason, is responsible for the quality and accuracy of facial images and information provided to the authorized requestors. In order to maintain the integrity of the process, (**agency name**) Facial Recognition staff shall:

A. Make determinations that result in the provision of an image or gallery of images that resemble the subject of a submitted image (request for comparison) within a specified threshold (level or degree of similarity). Circumstances may dictate a limitation on facial images provided.

B. As part of the review process, facial images provided shall be ranked or sorted. Such sorting serves to confirm that an image analysis has been conducted.

VIII. Process

A. General Information

1. Privacy, Security and Ethics

a. The data contained within the Facial Recognition system must be maintained in accordance with established policy and is protected from unauthorized access, use and disclosure

b. Authorized users may access, use, and disclose information only when necessary to perform work assigned to them in support of agency objectives.

c. Information contained in the Facial Recognition system shall not be accessed for any reasons that are personal to the requestor, user or any person making the query.

d. Authorized users shall not process personal transactions or those involving individuals known to them in accordance with (insert division policy/statute/procedures). A supervisor should be notified immediately if a transaction involves a possible conflict of interest or personal use, and the appropriate log entry shall be completed.

e. Information from Facial Recognition files may be disclosed to individuals only on a “need to know” basis. The individuals who receive such information should be approved/authorized to receive such information. Appropriate procedures should be followed in providing documenting such receipt of the information. Appropriate procedures should be followed in providing and documenting such receipt of the information.

f. Every reasonable effort shall be made to ensure misleading or incomplete data will not be entered, shared, disseminated or deleted.

g. Unauthorized actions that might cause the interruption of electronic data processing services or the destruction or alteration of data files or software are strictly prohibited.

h. If a user becomes aware of or witnesses an ethical or policy violation, such information should be immediately reported to their immediate supervisor.

B. Operation

1. Operating Standards Requirements

The (**Title of Administrator**) will be establishing and maintaining standards through the development of desk procedures (standardized work processes) is critical to ensure consistency and standardization in the process.

2. User Requirements

a. Only authorized personnel who have completed (**identify required training/certification**) shall have access to the Facial Recognition system.

b. Authorization is managed by the designated (**Title of Administrator**) who work within the (**insert agency name**).

C. User Access and Security

Facial Recognition presents risks that must be addressed to safeguard vital information assets. Access and usage should be dictated by and consistent with business needs and legal and contractual restrictions. Individuals subject to this policy are responsible to exercise good judgment regarding the use of the Facial Recognition system.

a. Use of the system shall not circumvent administrative control in place as defined within this policy.

b. A User shall not attempt to gain or provide unauthorized access to data.

c. System use shall be identified through auditing and other detection capabilities that include, but are not limited to, detection accounts, general usage, session logs, and enrolled devices.

d. Misrepresentation of identity for any reason is strictly prohibited. The sharing, disclosure, appropriation, unauthorized entry, posting or passing around of logon IDs or passwords for any reason is strictly prohibited. All employees are required to take reasonable steps to safeguard their assigned logon IDs and passwords. All employees are required to immediately report to the (**Title of appropriate party**) any known or suspected breaches of logon ID and password security.

e. All access and use is to be contemporaneously logged and is subject to audit in accordance with (**list appropriate statutes, procedures, and orders**).

f. An audit system usage history by individual users may be conducted at any time and without notice to validate compliance with internal policies or as part of a (Internal and/or Professional

Standards investigation). All authorized users should agree to these terms and conditions and should further agree that they have no individual expectation of privacy as to their login or use of the Facial Recognition system, or as to any information which they may search for, locate, retrieve or retain from accessing such database.

D. Training

All individuals using facial recognition software shall be fully trained in its proper use through a combination of classroom and online training that covers the following topics:

a. Face Comparison

b. Ethical Use and Privacy

c. User Access and Security

d. Technology – system and software, including limitation

e. Application Usage

f. Refresher Training

IX. Audit Process

A. External Audit

An Audit log that includes both a requestor query and the response provided. The audit log shall be maintained by the Facial Recognition staff. The log shall contain the following information:

a. The agency requesting facial recognition information

b. The date the transaction occurred

c. An assigned case number and date of image capture that uniquely identifies the facial images transmitted in response to the query (or a notation that no facial images were available and/or provided).

B. Internal Audit

The internal reporting mechanism will provide any/all information pertaining to facial recognition through a query process that will identify user or transaction history.

Appendix C Sample Memoranda (or Letter) of Understanding

Below are three samples. The first is an intrastate Memorandum of Understanding (MOU) between Nebraska Department of Corrections and the Nebraska Department of Motor Vehicles (DMV). The second is and interstate MOU between Iowa's Motor Vehicle Division, the Nebraska DMV, the Illinois Driver Services Department, and the South Dakota Department of Public Safety. The third sample is between the states of Connecticut and New York.

SAMPLE 1

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);

Uniform Motor Vehicle Disclosure Act, under Title 250 Nebraska Administrative Code Chapter 2-Rules and Regulations Governing Requests for and Release of Personal Information Contained in Motor Vehicle Records Pursuant to the Uniform Motor Vehicle Records Disclosure Act (UMVRDA)

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.

SAMPLE 2

Memorandum of Understanding Among
The Iowa Department of Transportation Motor Vehicle Division; The Nebraska Department of Motor Vehicles; The Illinois Secretary of State Driver Services Department; and The South Dakota Department of Public Safety Driver Licensing Program
Regarding Multi-State CDL Image Verification

12-27-2017

The State of Iowa, Department of Transportation Motor Vehicle Division; the State of

Nebraska Department of Motor Vehicles; the Illinois Secretary of State Driver Services Department; and the South Dakota Department of Public Safety Driver Licensing Program (hereinafter the "Parties"), acknowledge that:

- The Parties are responsible for fully identifying each applicant for a driver's license and identification card to ensure the goal of one person/one identity/one license;
- The Parties are required under 49 C.F.R. Part 383 of FMCSA Regulations to "prohibit a commercial motor vehicle driver from having more than one commercial motor vehicle driver's license;"
- The Parties utilize facial recognition technology to ensure an applicant does not hold a DL/ID in their state under another identity, to help confirm and protect individual identities, to prevent fraud, and to help save lives;
- The Parties currently do not have the capability to verify or run an automated interstate
- Facial match check in multiple states, which would help prevent individuals from obtaining commercial driver's licenses (CDLs) in different or assumed names;
- The Parties wish to perform cross-jurisdictional facial recognition searches of CDL applicant/driver photos in facial recognition databases across jurisdictional boundaries to reduce applicant fraud in connection with CDL issuance.

The Parties agree and understand as follows:

Article 1 – Problem Definition

1. Individuals cross state lines to obtain credentials for illegal and inappropriate uses such as: avoiding child support obligations, carrying out criminal activities related to identity theft, bank and credit fraud, and/or insurance fraud, obtaining licenses when their license had been revoked by their home jurisdiction and facilitating terrorism.
2. Identity fraud across state lines using altered or different identities remains pervasive, despite all actions already taken to deter or defeat it, and states are challenged to address this type of fraud.
3. There is a high public safety risk from those who commit fraud to obtain CDLs, especially from those individuals who may continue to drive commercial vehicles after having been revoked or suspended, and those transporting hazardous materials.

Article 2 – Purpose and Scope

1. The Parties have an interest in performing cross jurisdictional facial recognition searches and have asked MorphoTrust, USA to develop and implement a facial recognition program (hereinafter "Program") among the states, giving each the opportunity to execute and evaluate the processes, procedures, and protocols necessary for them to conduct cross jurisdictional facial recognition searches.
2. Facial Recognition information shared pursuant to this Memorandum of Understanding (hereinafter "MOU") shall be automatic and electronic and shall not expose any Parties' information to additional individuals outside a Party's normal course of business, unless a possible match is found. If a possible match is found, only authorized individuals from the initiating and responding Parties will be able to access the information in order to determine whether fraud is being attempted.
3. The Parties have an interest in mutual support and collaboration among their investigators when potential fraud cases are identified.
4. This MOU may be expanded in the future to include other States that utilize facial recognition technology and would benefit from cross-jurisdiction facial recognition matching to reduce fraud and save lives. Such expansion shall only occur upon the agreement of all Parties to this MOU, shall be in writing via an addition of the proposed Party to this MOU, and upon proper execution shall nullify and void any prior MOUs.
5. The images and data provided from one Party to another Party under this MOU shall be used solely for the purposes set forth in this MOU and shall not be disclosed to a third party except for use in a criminal prosecution, or as otherwise required by law.

Article 3 – Benefits

1. The following are the benefits to be realized by each Party for successful Program implementation:
   a. Improved Highway Safety
   b. Increased Integrity of Licensing Process
   c. Reduced Fraud and Identity Theft

d. Improved Agency Perception
e. Enhanced Case Development/Prosecution
f. Cost Containment/Reduction

Article 4 – Execution Steps

1. The Parties shall provide technical support to assist MorphoTrust, USA in the execution of this Program.

2. Iowa State University In-Trans Office shall coordinate data collection in collaboration with the Parties and provide evaluation and analysis of the Program. The Parties shall cooperate with In-Trans for providing data collection in compliance with privacy laws.

Article 5 – Methodology/Approach

1. Each Party shall, at agreed upon intervals, pull their most recent and archived applicant images and biographical information for CDL applicants in their State and run it against the entire image database of all Parties.

2. The Party receiving the request shall automatically under the Program's technology return to the initiating Party a folio of any potential matches for adjudication.

3. The initiating Party shall adjudicate potential matches and shall notify the responding Party of outcomes for each potential match.

4. Parties shall collaborate to optimize the processes, procedures, and protocols necessary to adjudicate matches from the other jurisdictions.

Article 6 – Funding

1. The Iowa Department of Transportation secured grant number FM-CDL-0216-15-01-00 through the Federal Motor Carrier Safety Administration to provide payment for the costs for the participating States, excluding the South Dakota, Department of Public Safety, Driver Licensing Program, to make the necessary connections to participate in this program. The total amount of this grant is $2,215,000.00 (Two million two hundred fifteen thousand dollars).

2. Costs incurred by MorphoTrust, USA for this project, except for those costs incurred by the South Dakota, Department of Public Safety; Driver Licensing Program, shall be billed to the Iowa Department of Transportation as provided for in the Proposal from MorphoTrust, USA. The Iowa Department of Transportation shall pay said costs with the funds obtained through grant FM-CDL-0216-15-01-00. In no event shall the Iowa Department of Transportation be liable or responsible for payment of any costs in excess of the total grant amount of $2,215,000.00 (Two million two hundred fifteen thousand dollars), or for those costs or liabilities incurred by the South Dakota, Department of Public Safety, Driver Licensing Program.

3. It is understood and acknowledged by the Parties that they shall provide the necessary internal resources to fulfill their responsibilities for the Program.

4. The State of Nebraska, Department of Motor Vehicles, the Illinois Secretary of State, Driver Services Department, and the South Dakota, Department of Public Safety, Driver Licensing Program all

understand and acknowledge that Iowa Department of Transportation is the recipient of grant number FM-CDL-0216-15-01-00. The State of Nebraska, Department of Motor Vehicles, the Illinois Secretary of State, Driver Services Department, and the South Dakota, Department of Public Safety, Driver Licensing Program have reviewed the grant agreement (FM-CDL-0216-15-01-00) and agree to cooperate and assist Iowa Department of Transportation in any way necessary to allow Iowa Department of Transportation to fully comply with the terms and conditions of said agreement and agree that such cooperation and assistance is a requirement of their continued participation in this program.

5. It is further understood that the South Dakota, Department of Public Safety, Driver Licensing Program Vehicles has secured the necessary funds to participate in the Program and understand and affirmatively acknowledges that no form of remuneration shall be provided by the Iowa Department of Transportation or any affiliates, subordinates, or partners.

Article 7 – Limitations of Liability

1. The Iowa Department of Transportation Motor Vehicle Division shall hold harmless all parties to this MOU, and his, her, its, or their agents, officers, heirs, assigns, and employees of and from any all damages, claims, penalties, debts owed, or any other form of liability arising from or related to the Iowa Department of Transportation Motor Vehicle Division's service, performance, errors, acts, or omissions incurred as a result of their participation in the program.

2. The Nebraska Department of Motor Vehicles shall hold harmless all parties to this MOU, and his, her, its, or their agents, officers, heirs, assigns, and employees of and from any all damages, claims, penalties, debts owed, or any other form of liability arising from or related to the Nebraska Department of Motor Vehicles' service, performance, errors, acts, or omissions incurred as a result of their participation in the program.

3. The Illinois Secretary of State Driver Services Department shall hold harmless all parties to this MOU, and his, her, its, or their agents, officers, heirs, assigns, and employees of and from any all damages, claims, penalties, debts owed, or any other form of liability arising from or related to the Illinois Secretary of State Driver Services Department's service, performance, errors, acts, or omissions incurred as a result of their participation in the program.

4. The South Dakota Department of Public Safety Driver Licensing Program hereby agrees that it shall be responsible for any and all damages, claims, penalties, debts owed, or any other forms of liability incurred as the result of the South Dakota Department of Public Safety Driver Licensing Program's service, performance, errors, acts, or omissions incurred as a result of their participation in the program.

5. The Parties are individually and separately liable and responsible for any liabilities or maintenance of their respective systematic components after the conclusion of the Program.

Article 8 – Length of MOU and Removal of Party

1. Any Party may remove itself from this MOU by giving a notice of intention to do so to all other signatories to this MOU not less than 30 days from the date of the notice. Such removal has no effect on MOU or Program as to the remaining Parties.

2. A Party may be removed as a result of a material failure to reasonably and substantively collaborate over the processes, procedure, and protocols necessary to effectuating this MOU. Such removal shall only occur after a failure to so collaborate and Notice of Removal signed by all of the other participating Parties. Such removal shall be effective 15 days after the receipt of the properly executed Notice of Removal by the Party to be removed.
3. This MOU shall remain in force until all of the participating Parties mutually decide to end it. Such mutual termination of this MOU shall only occur after a Mutual Notice of MOU Termination is signed by all of the participating Parties. Such termination shall be effective 15 days after all Parties execute such Mutual Notice of Termination of MOU and deliver the same, in good faith, to all participating parties.

WHEREAS an authorized representative for each respective Party hereby and forthwith, fully and wholly acknowledges, understand and agrees to all of the terms, conditions and stipulations in this MOU by executing below:

State of Iowa, Department of Transportation, Motor Vehicle Division

Authorized Signature and Title Date

State of Nebraska, Department of Motor Vehicles

Authorized Signature and Title Date

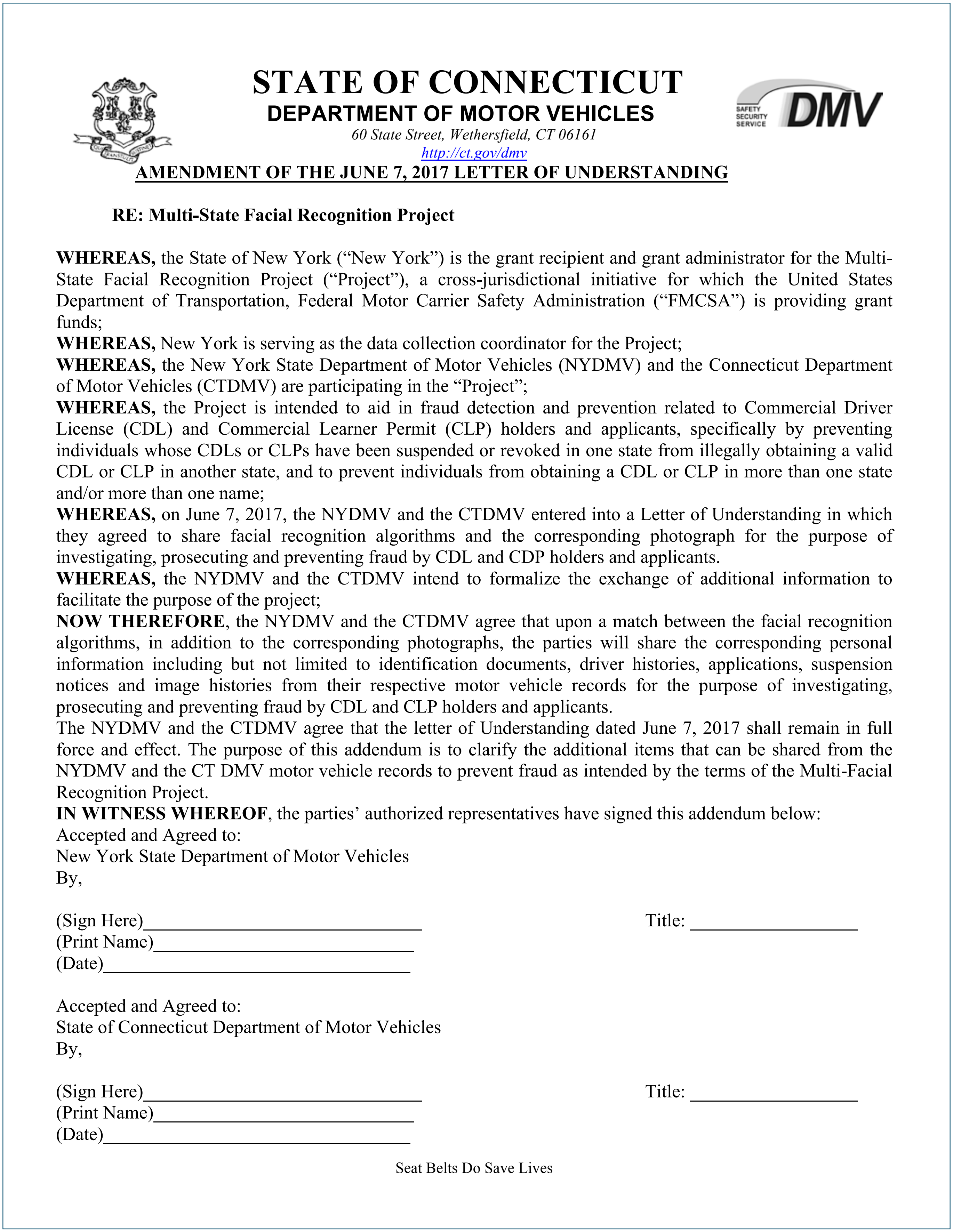
State of Illinois, Secretary of State's Office, Driver Services Department

Authorized Signature and Title Date

State of South Dakota, Department of Public Safety, Driver Licensing Program

Authorized Signature and Title Date

SAMPLE 3



STATE OF CONNECTICUT

DEPARTMENT OF MOTOR VEHICLES

60 State Street, Wethersfield, CT 06161
http://ct.gov/dmv

AMENDMENT OF THE JUNE 7, 2017 LETTER OF UNDERSTANDING

RE: Multi-State Facial Recognition Project

WHEREAS, the State of New York ("New York") is the grant recipient and grant administrator for the Multi-State Facial Recognition Project ("Project"), a cross-jurisdictional initiative for which the United States Department of Transportation, Federal Motor Carrier Safety Administration ("FMCSA") is providing grant funds;

WHEREAS, New York is serving as the data collection coordinator for the Project;

WHEREAS, the New York State Department of Motor Vehicles (NYDMV) and the Connecticut Department of Motor Vehicles (CTDMV) are participating in the "Project";

WHEREAS, the Project is intended to aid in fraud detection and prevention related to Commercial Driver License (CDL) and Commercial Learner Permit (CLP) holders and applicants, specifically by preventing individuals whose CDLs or CLPs have been suspended or revoked in one state from illegally obtaining a valid CDL or CLP in another state, and to prevent individuals from obtaining a CDL or CLP in more than one state and/or more than one name;

WHEREAS, on June 7, 2017, the NYDMV and the CTDMV entered into a Letter of Understanding in which they agreed to share facial recognition algorithms and the corresponding photograph for the purpose of investigating, prosecuting and preventing fraud by CDL and CDP holders and applicants.

WHEREAS, the NYDMV and the CTDMV intend to formalize the exchange of additional information to facilitate the purpose of the project;

NOW THEREFORE, the NYDMV and the CTDMV agree that upon a match between the facial recognition algorithms, in addition to the corresponding photographs, the parties will share the corresponding personal information including but not limited to identification documents, driver histories, applications, suspension notices and image histories from their respective motor vehicle records for the purpose of investigating, prosecuting and preventing fraud by CDL and CLP holders and applicants.

The NYDMV and the CTDMV agree that the letter of Understanding dated June 7, 2017 shall remain in full force and effect. The purpose of this addendum is to clarify the additional items that can be shared from the NYDMV and the CT DMV motor vehicle records to prevent fraud as intended by the terms of the Multi-Facial Recognition Project.

IN WITNESS WHEREOF, the parties' authorized representatives have signed this addendum below:

Accepted and Agreed to:
New York State Department of Motor Vehicles
By,

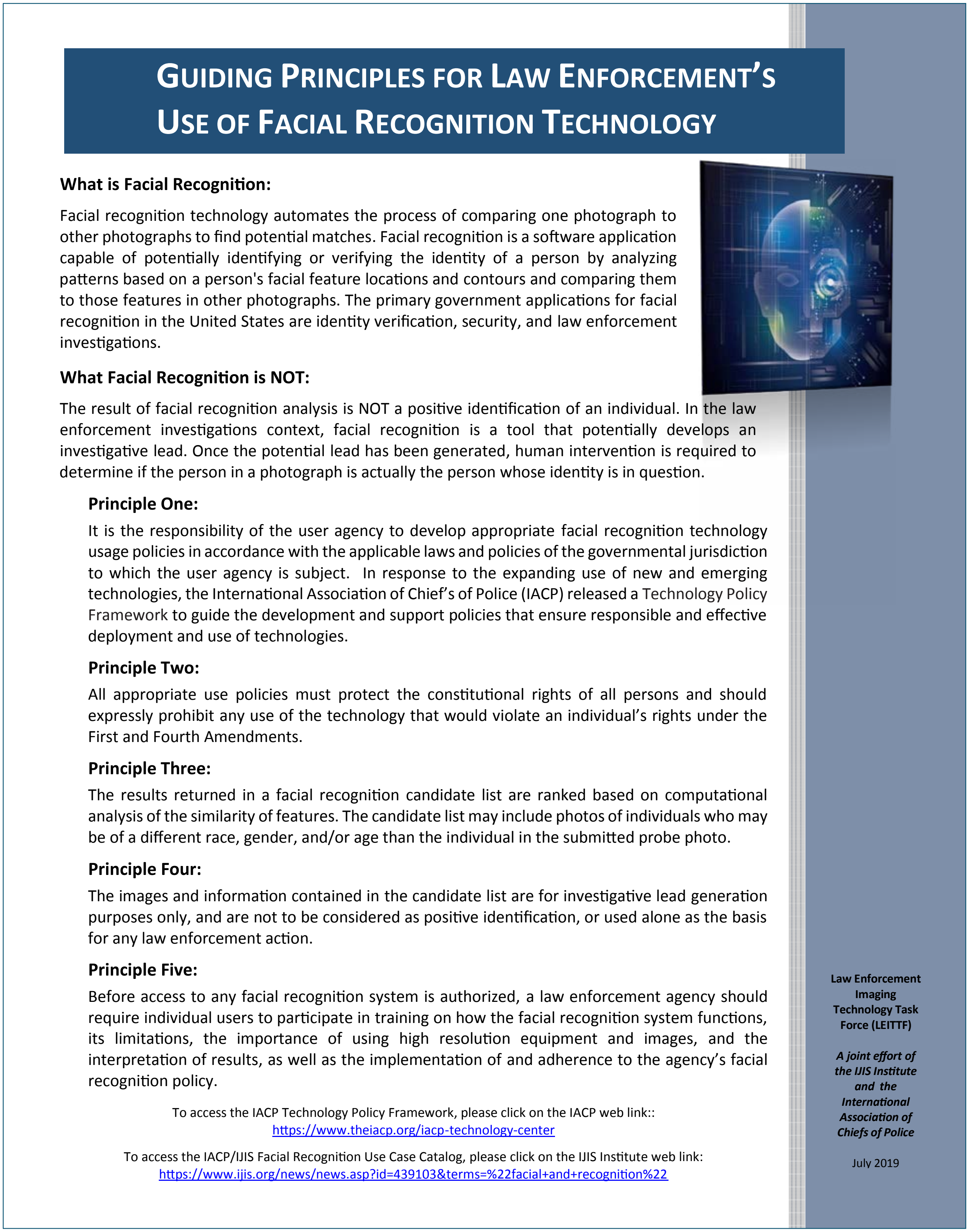
(Sign Here)______________________________ Title: __________________
(Print Name)____________________________
(Date)_________________________________

Accepted and Agreed to:
State of Connecticut Department of Motor Vehicles
By,

(Sign Here)______________________________ Title: __________________
(Print Name)____________________________
(Date)_________________________________

Seat Belts Do Save Lives

Appendix D Guiding Principles for Law Enforcement's Use of Facial Recognition Technology



Guiding Principles for Law Enforcement's Use of Facial Recognition Technology

What is Facial Recognition:

Facial recognition technology automates the process of comparing one photograph to other photographs to find potential matches. Facial recognition is a software application capable of potentially identifying or verifying the identity of a person by analyzing patterns based on a person's facial feature locations and contours and comparing them to those features in other photographs. The primary government applications for facial recognition in the United States are identity verification, security, and law enforcement investigations.

What Facial Recognition is NOT:

The result of facial recognition analysis is NOT a positive identification of an individual. In the law enforcement investigations context, facial recognition is a tool that potentially develops an investigative lead. Once the potential lead has been generated, human intervention is required to determine if the person in a photograph is actually the person whose identity is in question.

Principle One:

It is the responsibility of the user agency to develop appropriate facial recognition technology usage policies in accordance with the applicable laws and policies of the governmental jurisdiction to which the user agency is subject. In response to the expanding use of new and emerging technologies, the International Association of Chief's of Police (IACP) released a Technology Policy Framework to guide the development and support policies that ensure responsible and effective deployment and use of technologies.

Principle Two:

All appropriate use policies must protect the constitutional rights of all persons and should expressly prohibit any use of the technology that would violate an individual's rights under the First and Fourth Amendments.

Principle Three:

The results returned in a facial recognition candidate list are ranked based on computational analysis of the similarity of features. The candidate list may include photos of individuals who may be of a different race, gender, and/or age than the individual in the submitted probe photo.

Principle Four:

The images and information contained in the candidate list are for investigative lead generation purposes only, and are not to be considered as positive identification, or used alone as the basis for any law enforcement action.

Principle Five:

Before access to any facial recognition system is authorized, a law enforcement agency should require individual users to participate in training on how the facial recognition system functions, its limitations, the importance of using high resolution equipment and images, and the interpretation of results, as well as the implementation of and adherence to the agency's facial recognition policy.

To access the IACP Technology Policy Framework, please click on the IACP web link::
https://www.theiacp.org/iacp-technology-center

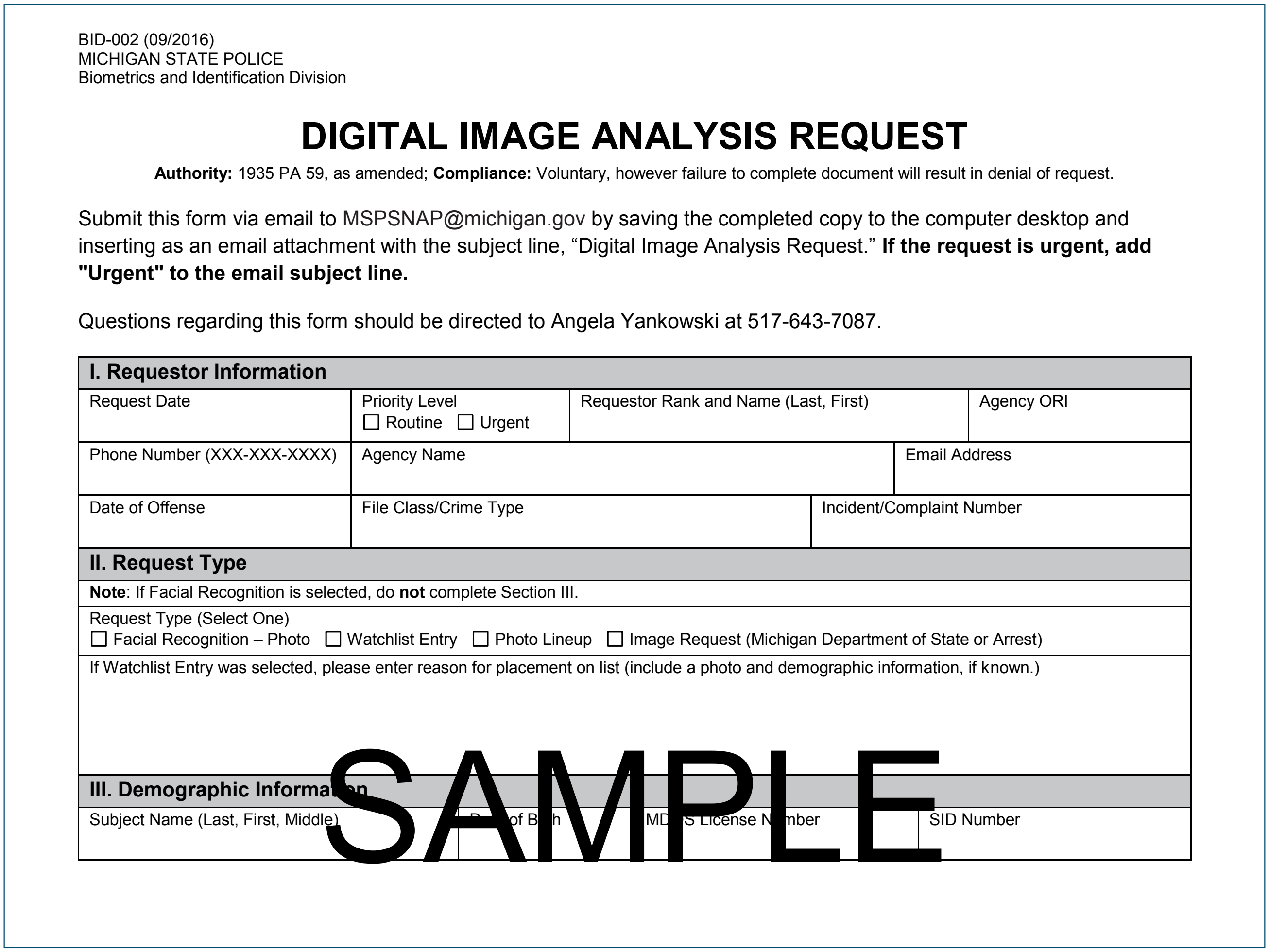
To access the IACP/IJIS Facial Recognition Use Case Catalog, please click on the IJIS Institute web link:
https://www.ijis.org/news/news.asp?id=439103&terms=%22facial+and+recognition%22

Law Enforcement Imaging Technology Task Force (LEITTF)

A joint effort of the IJIS Institute and the International Association of Chiefs of Police

July 2019

Appendix E Sample Applications for Requesting a Facial Recognition Comparison



BID-002 (09/2016)
MICHIGAN STATE POLICE
Biometrics and Identification Division

DIGITAL IMAGE ANALYSIS REQUEST

Authority: 1935 PA 59, as amended; **Compliance:** Voluntary, however failure to complete document will result in denial of request.

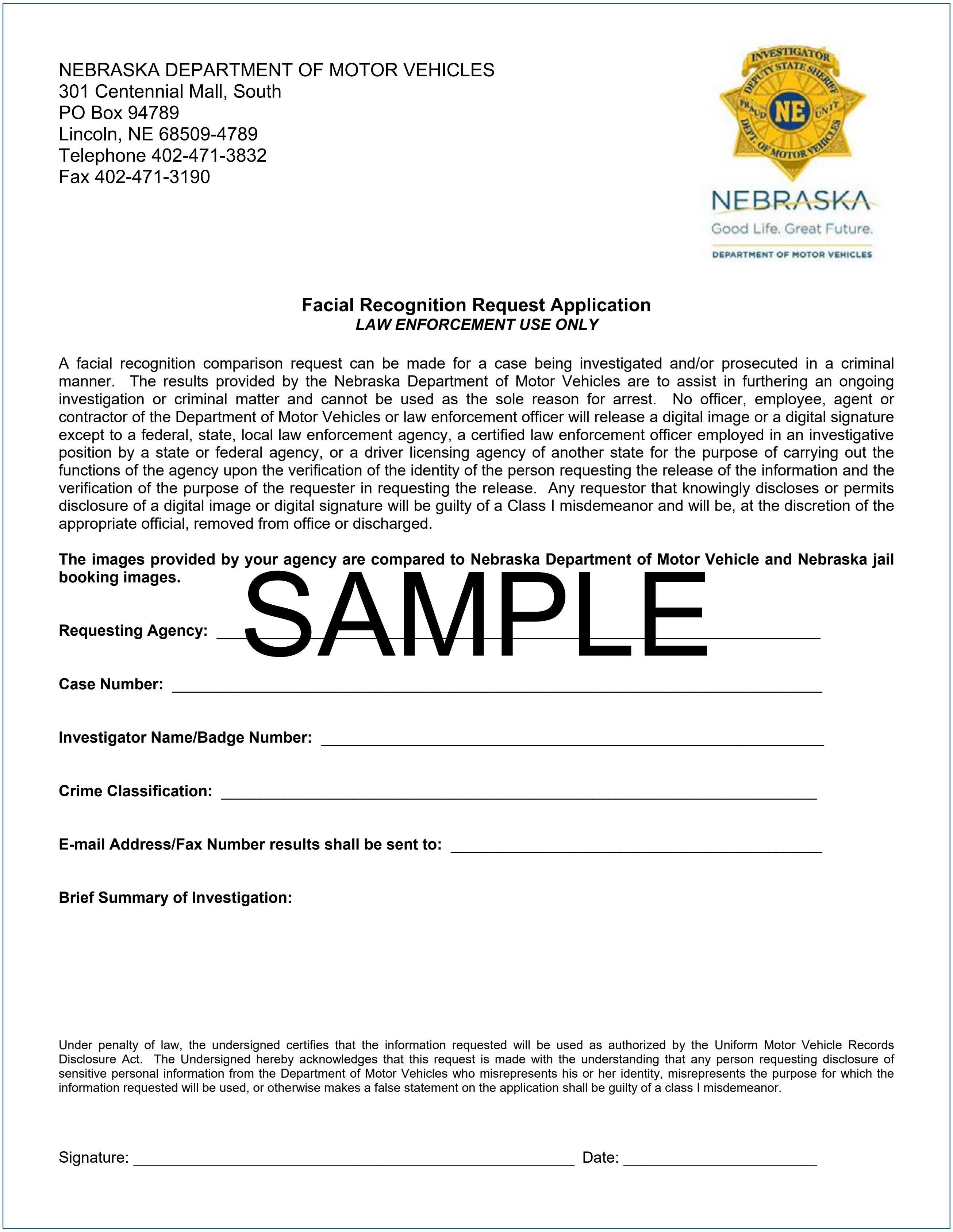
Submit this form via email to MSPSNAP@michigan.gov by saving the completed copy to the computer desktop and inserting as an email attachment with the subject line, “Digital Image Analysis Request.” **If the request is urgent, add "Urgent" to the email subject line.**

Questions regarding this form should be directed to Angela Yankowski at 517-643-7087.

I. Requestor Information			
Request Date	Priority Level ☐ Routine ☐ Urgent	Requestor Rank and Name (Last, First)	Agency ORI
Phone Number (XXX-XXX-XXXX)	Agency Name		Email Address
Date of Offense	File Class/Crime Type		Incident/Complaint Number

II. Request Type
Note: If Facial Recognition is selected, do **not** complete Section III.
Request Type (Select One) ☐ Facial Recognition – Photo ☐ Watchlist Entry ☐ Photo Lineup ☐ Image Request (Michigan Department of State or Arrest)
If Watchlist Entry was selected, please enter reason for placement on list (include a photo and demographic information, if known.)

III. Demographic Information			
Subject Name (Last, First, Middle)	Date of Birth	MDOS License Number	SID Number



NEBRASKA DEPARTMENT OF MOTOR VEHICLES
301 Centennial Mall, South
PO Box 94789
Lincoln, NE 68509-4789
Telephone 402-471-3832
Fax 402-471-3190

Facial Recognition Request Application

LAW ENFORCEMENT USE ONLY

A facial recognition comparison request can be made for a case being investigated and/or prosecuted in a criminal manner. The results provided by the Nebraska Department of Motor Vehicles are to assist in furthering an ongoing investigation or criminal matter and cannot be used as the sole reason for arrest. 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 except to a federal, state, local law enforcement agency, a certified law enforcement officer employed in an investigative position by a state or federal agency, or 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 requester 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 I misdemeanor and will be, at the discretion of the appropriate official, removed from office or discharged.

The images provided by your agency are compared to Nebraska Department of Motor Vehicle and Nebraska jail booking images.

Requesting Agency: ____

Case Number: ____

Investigator Name/Badge Number: ____

Crime Classification: ____

E-mail Address/Fax Number results shall be sent to: ______________________________

Brief Summary of Investigation:

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 from 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: ____________________

Appendix F Listing of Federal Laws[1]

The development of a facial recognition (FR) policy is primarily designed for entity personnel and authorized users to ensure that they are aware of the legal and privacy framework within which they and the entity should operate. If the applicability and requirements of various laws, regulations, or sharing agreements are not spelled out or referenced in an entity's face recognition policy, staff and user accountability is greatly diminished, mistakes are made, privacy violations occur, and the public's (and other agencies') confidence in the ability of the entity to protect face recognition information is compromised. It is important for staff members to know the rules through sound policy and procedure communicated through ongoing training activity.

Three states—Texas[2], Illinois[3], and Washington[4]—have adopted laws regulating commercial use of biometric identifiers gathered through certain types of FR technology. Five state legislatures (as of January 1, 2017)—Alaska[5], Connecticut[6], Massachusetts[7], Montana[8], and New Hampshire[9]—have also introduced bills that would regulate the collection, retention, and use of biometric data. Arizona and Missouri have pending bills regarding student privacy and limitations on the collection of student biometric data without parental consent. Finally, many state laws governing data security and breach response include biometric information in their definitions of covered personal information. For example, North Carolina's Identity Theft Protection Act lists biometric data as an element of identifying information that, in combination with a person's name, constitutes personal information. This law requires any entity conducting business in the state and maintaining personal information of a resident to take reasonable measures to protect the information against unauthorized access.[10]

As of February 2011, there is no U.S. federal law requiring that an individual identify him- or herself during a *Terry*[11] stop, but *Hiibel*[12] held that states may enact such laws, provided the law requires the officer to have reasonable and articulable suspicion of criminal involvement.[13] Twenty-four states have enacted stop and identify laws. Although the *Hiibel* case did not directly involve the deputy's use of biometric technology, the opinion lays the foundation for state legislatures to authorize law enforcement officials to use face recognition systems. Unresolved by *Hiibel* is whether the possible loss of privacy posed by automated face recognition applications is outweighed by improved law enforcement. Nevertheless, many of the privacy issues raised by the intersection of *Hiibel*

[1] This appendix and the information contained in it came from, *Face Recognition Policy Template for State, Local, and Tribal Criminal Intelligence and Investigative Activities*, December 2017.

[2] Capture or Use of Biometric Identifier, Texas Business and Commerce Code §503.001.

[3] Biometric Information Privacy Act, 740 Illinois Compiled Statutes 14.

[4] Biometric Identifiers, Washington House Bill 1493, Chapter 299, effective July 23, 2017.

[5] *Introduced* Collection of Biometric Information, House Bill 72, 2017 Regular Session.

[6] *Introduced* Connecticut House Bill 5522, 2017 Regular Session.

[7] *Introduced* Massachusetts Senate Bill 750, Chapter 93H, Section 1 and 2 2017 Regular Session.

[8] *Introduced* Montana Biometric Information Privacy Act, House Bill 518, 2017 Regular Session.

[9] *Introduced* Biometric Information Privacy Act, New Hampshire House Bill 523, 2017 Regular Session.

[10] Claypoole, Ted, and Stoll, Developing laws address flourishing commercial use of biometric information, Cameron, *Business Law Today*, American Bar Association, May 2016, https://www.americanbar.org/publications/blt/2016/05/08_claypoole.html.

[11] *Terry v. Ohio*, 392 U.S. 1 (1968).

[12] *Hiibel v. Sixth Judicial District Court*, 542 U.S. 177 (2004).

[13] The *Hiibel* Court held, "The principles of *Terry* permit a State to require a suspect to disclose his name in the course of a *Terry* stop."—542 U.S. at 187.

and biometric technologies can be addressed through reasonable controls over how face recognition systems are used in the field and how the data they capture and create will be managed.[14]

The following are synopses of primary federal laws that an entity should review and, when appropriate, consider citing in a face recognition policy to protect face recognition data and any personally identifiable information later associated with the face recognition information. As FR information may be incorporated as one piece of information into a larger case file, the following federal laws may be applicable. The list is arranged in alphabetical order by popular name.

Applicants and Recipients of Immigration Relief Under the Violence Against Women Act of 1994 (VAWA), Public Law 103-322, September 13, 1994, and the Victims of Trafficking and Violence Prevention Act of 2000 (T and U non-immigrant status for victims of trafficking and other serious crimes), Public Law 106-386, Oct. 28, 2000, 8 U.S.C. § 1367, Penalties for Disclosure of Information—The governing statute prohibits the unauthorized disclosure of information about VAWA, T, and U cases to anyone other than an officer or employee of the U.S. Department of Homeland Security, the U.S. Department of Justice, the U.S. Department of State, or parties covered by exception when there is a need to know. This confidentiality provision is commonly referred to as "Section 384" because it originally became law under Section 384 of the Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA) of 1996, which protects the confidentiality of victims of domestic violence, trafficking, and other crimes who have filed for or have been granted immigration relief. 8 U.S.C. § 1367 Information is defined as any information relating to aliens who are seeking or have been approved for non-immigrant or immigrant status as (1) battered spouses, children, or parents under provisions of VAWA; (2) victims of a severe form of human trafficking who generally are cooperating with law enforcement authorities (T non-immigrant status); or (3) aliens who have suffered substantial physical or mental abuse as the result of qualifying criminal activity and have been, are being, or are likely to be helpful in the investigation or prosecution of that activity (U non-immigrant status). This includes information pertaining to qualifying family members who receive derivative T, U, or VAWA status. Because 8 U.S.C. § 1367 applies to any information about a protected individual, this includes records or other information that do not specifically identify the individual as an applicant for or a beneficiary of T non-immigrant status, U non-immigrant status, or relief under VAWA.

Criminal Intelligence Systems Operating Policies, 28 CFR Part 23, Code of Federal Regulations, Title 28, Chapter 1, Part 23—This is a guideline for law enforcement agencies that operate federally funded multijurisdictional criminal intelligence systems. The operating principles of 28 CFR Part 23 provide guidance to law enforcement regarding how to operate criminal intelligence information systems effectively while safeguarding privacy, civil rights, and civil liberties (P/CRCL) during the collection, storage, and dissemination of criminal intelligence information. The regulation governs the intelligence information systems' process, which includes information submission or collection, secure storage, inquiry and search capability, controlled dissemination, and review and purge processes.

Driver's Privacy Protection Act (DPPA) of 1994, 18 U.S.C. 2721 and 2725—18 U.S.C. 2725 (4) defines "highly restricted personal information" **as an individual's photograph or image**, Social Security number, and medical or disability information. 18 U.S.C. 2721(b)(1) states that personal information (as described in 18 U.S.C. 2725(4), above) may be disclosed for use by any government agency, including any court or law enforcement agency, in carrying out

[14] *Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field*, Nlets—The International Justice and Public Safety Network, June 30, 2011.

its functions or any private person or entity acting on behalf of a federal, state, or local agency in carrying out its functions. § 2721-2725 restricts access and prohibits the release of personal information from state motor vehicle records to ensure the privacy of persons whose records have been obtained by that department in connection with a motor vehicle record unless certain criteria are met.

E-Government Act of 2002, Public Law 107–347, 208, 116 Stat. 2899 (2002)—Office of Management and Budget (OMB) (03-22, OMB Memorandum, M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002)—OMB implementing guidance for this act requires federal agencies to perform privacy impact assessments (PIAs) for new information technologies that develop or procure new information technology involving the collection, maintenance, or dissemination of information in identifiable form or that make significant changes to existing information technology that manages information in identifiable form. A PIA is an evaluation of how information in identifiable form is collected, stored, protected, shared, and managed. The purpose of a PIA is to demonstrate that system owners and developers have incorporated Privacy, Civil Rights, Civil Liberties protections throughout the entire life cycle of a system. The act requires an agency to make PIAs publicly available, except when an agency, in its discretion, determines that publication of the PIA would raise security concerns or reveal classified (i.e., national security) or sensitive information. Although this act does not apply to State, Local, Tribal, and Territorial (SLTT) partners, this tool is useful for identifying and mitigating privacy risks and for notifying the public what personal identifying information (PII) the SLTT agency is collecting; why PII is being collected; and how the PII will be collected, used, accessed, shared, safeguarded, and stored.

Enhanced Border Security and Visa Reform Act of 2002, H.R. 3525—In the Enhanced Border Security and Visa Entry Reform Act of 2002, the U.S. Congress mandated the use of biometrics in U.S. visas. This law requires that U.S. embassies and consulates abroad must issue to international visitors, “only machine-readable, tamper-resistant visas and other travel and entry documents that use biometric identifiers.” Additionally, the Homeland Security Council decided that the U.S. standard for biometric screening is 10 fingerprint scans collected at all U.S. embassies and consulates for visa applicants seeking to come to the United States.

Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; 34 CFR Part 99—FERPA governs the disclosure of students’ biometric information, to the extent that it is contained in student records. A student’s biometric record is included in the definition of personally identifiable information and is a type of information that may be included in students’ education records. As such, FERPA prohibits schools from releasing students’ biometric information without parental consent, to the extent that it is contained in students’ education records, with some limited exceptions[15].

Federal Civil Rights laws, 42 U.S.C. § 1983, United States Code, Title 42, Chapter 21, Subchapter I, § 1983—This is a federal statute that allows an individual to sue public officials in federal court for violations of the individual’s civil rights. Civil rights include such things as the Fourth Amendment’s prohibitions against unreasonable search and seizure; violations of privacy rights; and violations of the right to freedom of religion, free speech, and free association. It serves as a deterrent to unlawful collection, use, or sharing of information rather than providing specific authority or a prohibition to the collection, use, or sharing of information.

Federal Records Act, 44 U.S.C. § 3301, United States Code, Title 44, Chapter 33, § 3301—This chapter contains the laws governing disposal of records

[15] Claypoole, Ted, and Stoll, Cameron, Developing laws address flourishing commercial use of biometric information, *Business Law Today,* American Bar Association, May 2016, https://www.americanbar.org/publications/blt/2016/05/08_claypoole.html.

made or received by a federal agency in the normal course of business. It discusses procedures and notices, if required, and the role of the federal archivist. The law applies only to federal agencies, but there may be similar state or local laws applicable to state and local agencies.

Freedom of Information Act (FOIA), 5 U.S.C. § 552, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552—The federal FOIA, enacted in 1966, provides access to federal agency records or information. It does not, however, allow access to state or local government records. Nearly all states have their own public access statutes that provide access to state- and local-agency records. The interaction of federal and state FOIA laws can create complex issues. Federal statutes, in essence, provide a baseline of legal protections for individuals. Although state legislatures may pass laws to supplement these federal guidelines, state laws that interfere with or are contrary to a federal law are pre-empted. By virtue of the Supremacy Clause of the U.S. Constitution (Article VI, Clause 2), federal law may restrict access to records otherwise available pursuant to a state's FOIA by requiring that certain information be kept confidential. Thus, federal confidentiality requirements may supersede a state FOIA statute mandating public disclosure of a record but only when there is a specific federal statute (other than the federal FOIA) that mandates the records be kept confidential. In short, records may be available under one FOIA statute but not pursuant to another.

Health Insurance Portability and Accountability Act (HIPAA) of 1996, 42 U.S.C. § 201, United States Code, Title 42, Chapter 6A, Subchapter I, § 201; Public Law 104-191—HIPAA was enacted to improve the Medicare and Medicaid programs and the efficiency and effectiveness of the nation's health care system by encouraging the development of a national health information system through the establishment of standards and requirements for the electronic transmission of health information. To that end, Congress directed the U.S. Department of Health and Human Services (HHS) to issue safeguards to protect the security and confidentiality of health information. To implement HIPAA's privacy requirements, HHS promulgated regulations setting national privacy standards for health information: the Standards for Privacy of Individually Identifiable Health Information (the "Privacy Rule")—42 U.S.C. §1320d-2; 45 CFR Parts 160, 164 (2003).

HIPAA, Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164, Code of Federal Regulations, Title 45, Parts 160 and 164—This "privacy rule" sets forth national standards for the privacy and security of individually identifiable health information (45 CFR Part 164, Subpart E (2003)). This rule has been described as providing a "federal floor" of safeguards to protect the confidentiality of medical information. State laws that provide stronger privacy protection will continue to apply over and above the federal privacy protection. The general rule under these standards states that a covered entity may not use or disclose protected health information (PHI) except as permitted or required by the rules (45 CFR Part 164.502(a) and §164.103 [defining PHI and use]). The Privacy Rule applies to the following covered entities: (1) a health plan, (2) a health care clearinghouse, and (3) a health care provider who transmits any health information in electronic form in connection with certain transactions (42 U.S.C. §1320d-1(a) (2003); 45 CFR Part 160.102 (2003). Because the privacy rule applies only to a covered entity, a governmental body begins its inquiry by first determining whether it is a covered entity under the Privacy Rule (45 CFR Part 160.103 (2003) [defining health plan, health care clearinghouse, health care provider]). If it is a covered entity, it then looks to the Privacy Rule for a permitted or required disclosure.

Section 164.510(b)(3) permits (but does not require) a health care provider, when a patient is not present or is unable to agree or object to a disclosure due to incapacity or emergency circumstances, to determine whether disclosing a patient's information to the patient's family, friends, or other persons involved in the patient's care, is in the best interests of the patient. When a provider determines that such a disclosure is in the patient's best interests, the provider would be permitted to disclose only the PHI that is directly relevant to the person's involvement in the patient's care.

This permission clearly applies where a patient is unconscious. However, there may be additional situations in which a health care provider believes, based on professional judgment, that the patient does not have the capacity to agree or object to the sharing of PHI at a particular time and that sharing the information is in the best interests of the patient at that time. These may include circumstances in which a patient is has temporary psychosis or is under the influence of drugs or alcohol.

Indian Civil Rights Act of 1968, 25 U.S.C. § 1301 et seq., United States Code, Title 25, Chapter 15, Subchapter I—This act contains definitions of relevant terms and extends certain constitutional rights to Indian tribes exercising powers of self-government.

National Child Protection Act of 1993, Public Law 103-209 (December 20, 1993), 107 Stat. 2490—In each state, an authorized criminal justice agency of the state shall report child abuse crime information to or index child abuse crime information in the national criminal history background check system. A criminal justice agency can satisfy the requirement by reporting or indexing all felony and serious misdemeanor arrests and dispositions. The U.S. Attorney General (AG) is required to publish an annual statistical summary of child abuse crimes. The act requires that 80% of final dispositions be entered in the state databases by December 1998, with steps being taken toward 100% entry.

A 1994 amendment required that the AG—in consultation with federal, state, and local officials, including officials responsible for criminal history record systems, and representatives of public and private care organizations and health, legal, and social welfare organizations—shall develop guidelines for the adoption of appropriate safeguards by care providers and by the state for protecting children, the elderly, and individuals with disabilities from abuse.

National Institute of Standards and Technology (NIST) Special Publication 800-53 (Appendix J) ***Security and Privacy Controls for Federal Information Systems and Organizations*****—**Federal agencies are required to ensure that privacy protections are incorporated into information security planning. To this end, SP 800-53 Rev. 4 features eight families of privacy controls that are based on Fair Information Practice Principles FIPPs. The proliferation of social media, Smart Grid, mobile, and cloud computing as well as the transition from structured to unstructured information and metadata environments have added significant complexities and challenges for federal organizations in safeguarding privacy. These challenges extend well beyond the traditional information technology security view of protecting privacy, which focused primarily on ensuring confidentiality. The use of these standardized privacy controls will provide a more disciplined and structured approach for satisfying federal privacy requirements and demonstrating compliance with those requirements. Like their federal partners, SLTT agencies may use the privacy controls when evaluating their systems, processes, and programs.

Preparing for and Responding to a Breach of Personally Identifiable Information, OMB Memorandum M-17-12 (January 2017)—This memorandum sets forth the policy for federal agencies to prepare for and respond to a breach of PII. It includes a framework for assessing and mitigating the risk of harm to individuals potentially affected by a breach, as well as guidance on whether and how to provide notification and services to those individuals. This memorandum is intended to promote consistency in the way agencies prepare for and respond to a breach by requiring common standards and processes.

Privacy Act of 1974, 5 U.S.C. § 552a, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a—The Privacy Act establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual. The Privacy Act prohibits the disclosure of a record about an individual from a system of records without the written consent of the individual unless the disclosure is pursuant to one of 12 statutory exceptions. The act also provides individuals with a means by which to seek access to and amendment of their records and sets agency record-keeping requirements. In addition, the Privacy Act requires that agencies give the public notice of their systems of records by publication in the *Federal Register*.

Protection of Sensitive Agency Information, Office of Management and Budget Memorandum M-06-16 (June 2006)—This memorandum provides a security checklist from the NIST to protect remote information removed from or accessed from outside an agency's physical location specific to PII. The NIST checklist requires that agencies verify PII in need of protection, confirm the adequacy of organization policy surrounding PII protection, and implement any necessary protections for PII transported or stored off-site or accessed remotely. In addition to the NIST checklist, the memorandum recommends implementing information encryption on all mobile devices, allowing remote access only with two-factor authentication, using timeout functions on devices, and logging all computer-readable information extracts from databases with sensitive information while verifying that each extract has either been erased within 90 days or its use is still required.

Section 210401 of the Violent Crime Control and Law Enforcement Act of 1994, 42 U.S.C. § 14141—This is a federal statute that provides that it shall be unlawful for any governmental authority or its agent to engage in a pattern or practice of conduct by law enforcement officers that violates the Constitution or laws of the United States. It authorizes the AG to bring civil actions to obtain injunctive or declaratory relief to eliminate the unlawful or unconstitutional pattern or practice.

U.S. Constitution, First, Fourth, Fifth, Sixth, and Fourteenth Amendments—The Bill of Rights establishes minimum standards for the protection of the civil rights and civil liberties of persons within the United States. The First Amendment protects religious freedom, freedom of speech, freedom of the press, the right to peaceably assemble, and the right to petition the government for a redress of grievances. The Fourth Amendment protects the people from unreasonable searches and seizures and requires that warrants be issued only upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the individual or things to be seized. The Sixth Amendment establishes the right of an accused individual to a speedy and public trial by an impartial jury, to be informed of the nature and cause of the charges, to confront witnesses, to have compulsory process to obtain witnesses, and to have the assistance of legal counsel. The Fourteenth Amendment addresses citizenship rights and equal protection of the laws. Although the equal protection clause applies explicitly only to state governments, equal protection requirements apply to the federal government through the Fifth Amendment Due Process Clause.

Appendix G Additional Resources

Best Practices Manual for Facial Recognition Comparison
ENFSI-BPM-DI-01
January 2018
www.enfsi.eu

Best Practices Manual for Image and Video Enhancement
ENFSI-BPM-DI-02
June 2018
www.enfsi.eu

IJIS Institute and the International Association of
Chiefs of Police
Law Enforcement Facial Recognition Use Case Catalog
March 2019
https://www.ijis.org

Appendix H Working Group Roster

CHAIR

Owen McShane
Director of Field Investigations
New York Department of Motor Vehicles
Division of Field Investigation

MEMBERS

Charlotte Boyd-Malette
Director, Driver Services
North Carolina Division of Motor Vehicles

Faith Contreras
Facial Recognition Program Administrator
Arizona Department of Transportation

Jennifer Coulson
Digital Image Examiner
Michigan State Police

Ali Danhoff
Assistant Program Director
Indiana Bureau of Motor Vehicles
Credential Management

Eric Ducey
Analyst
Connecticut Department of Motor Vehicles
Document Integrity Unit

Susan Schilz
Compliance, Audit and Fraud Unit Supervisor
Wisconsin Department of Transportation

TECHNICAL ADVISORS

Manuj Gupta
Cyber Security Specialist Manager
Deloitte & Touche

Mr. Kevin O'Leary
Senior Product Manager
IDEMIA

FEDERAL PARTNER

Douglas Hill
Manager, Facial Recognition Program
U.S. Department of State
Bureau of Consular Affairs

AAMVA PROJECT MANAGER

Brian Ursino
Director, Law Enforcement
American Association of Motor Vehicle Administrators
(703) 350-5103 | bursino@aamva.org

AAMVA STAFF

Geoffrey Slagle
Director, Identity Management
American Association of Motor Vehicle Administrators
(703) 342-7459 | gslagle@aamva.org

Paul Steier
Law Enforcement Program Manager
American Association of Motor Vehicle Administrators
(703) 270-8932 | psteier@aamva.org

Mindy Stephens
Manager, Identity Management
American Association of Motor Vehicle Administrators
(571) 201-3472 | mstephens@aamva.org

OUR VISION

Safe drivers
Safe vehicles
Secure identities
Saving lives!

AAMVA

American Association of Motor Vehicle Administrators

4401 Wilson Blvd, Suite 700
Arlington, Virginia 22203
703.522.4200 | **aamva.org**