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.